INMETRO

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA

Boletim de SERVIÇO

EDIÇÃO ESPECIAL

Portaria nº 286, de 19 de maio de 2025

Data de Publicação:

20 de maio de 2025

BOLETIM DE SERVIÇO

EDIÇÃO ESPECIAL

Marcio Andre Oliveira Brito
Presidente do INMETRO

Gildásio Nascimento Rocha
Diretor de Administração e Finanças

Jorge Andre Moreira Medeiros Soares
Coordenador-Geral de Gestão de Pessoas

Rio de Janeiro,20 de maio de 2025.

Publicação eletrônica disponível na intranet produzida mensalmente pela COGEP – Coordenação-Geral de Gestão de Pessoas.

As matérias aqui publicadas deverão ser do conhecimento de todos os servidores de cada unidade do Inmetro.

O Boletim de Serviço impresso encontra-se disponível para consulta no Serviço de Documentação e Informação – Sedin.

Este boletim contém a seguinte seção:
1. Atos do Presidente

Neste número, foram publicadas as matérias encaminhadas Coordenação-Geral de Gestão de Pessoas - Cogep, até a data do fechamento do boletim.

SUMÁRIO

Serviço Público Federal

MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
INSTITUTO NACIONAL DE METROLOGIA , QUALIDADE E TECNOLOGIA - INMETRO

Portaria nº 286, de 19 de maio de 2025.

Estabelece os requisitos mínimos de segurança da informação para utilização segura de *software* e de serviços de computação em nuvem no âmbito do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO)

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO, **SUBSTITUTO**, no exercício da competência que lhe foi outorgada pelo artigo 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, combinado com o disposto no artigo 18, incisos II e III, do Decreto n.º 11.221, de 5 de outubro de 2022 e o art. 12, da Lei nº 9.784, de 29 de janeiro de 1999.

Considerando a **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.

Considerando o que consta no Processo nº 0052600.003137/2025-17, **resolve**:

Art. 1º Aprovar, na forma do anexo único desta Portaria, o Documento Uso seguro de computação em nuvem no âmbito do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO), em conformidade com a Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

Art. 2º A Coordenação-Geral de Tecnologia da Informação (CTINF) da Diretoria de Inovação, Planejamento e Articulação Institucional (DPLAN) do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) deverá adotar, monitorar e garantir a aplicação das diretrizes estabelecidas no documento Uso Seguro de Computação em Nuvem, visando garantir o atendimento dos requisitos mínimos de segurança da informação para utilização segura de *software* e de serviços de computação em nuvem no Inmetro.

Art. 3º Esta Portaria entra em vigor na data da sua publicação no Boletim de Serviço do Inmetro.

DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015 EM 20/05/2025, ÀS 11:10, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

JOÃO NERY RODRIGUES FILHO
Presidente, Substituto

ANEXO ÚNICO

DOCUMENTO USO SEGURO DE COMPUTAÇÃO EM NUVEM

1. DO ESCOPO

1.1. A normativa sobre uso seguro da computação em nuvem tem a finalidade de estabelecer um conjunto de princípios, diretrizes e responsabilidades que visam garantir a segurança da informação no uso de softwares e serviços de computação em nuvem no âmbito do INMETRO.

1.2. Esta normativa visa garantir que os dados corporativos estejam disponíveis e protegidos contra perdas, falhas de hardware, desastres naturais e ameaças cibernéticas.

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

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

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

I - observar os requisitos estabelecidos na legislação vigente, com o objetivo de elevar o nível de proteção das informações no uso de softwares e serviços de computação em nuvem;

II - estabelecer medidas de segurança que deverão ser observadas tanto pelos(as) servidores(as) vinculados(as) ao INMETRO quanto pelas organizações fornecedoras de serviços de computação em nuvem;

III - adotar medidas para proteger as informações contra acessos não autorizados e contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, considerando a natureza das informações tratadas, as características específicas do tratamento, o estado atual da tecnologia e os princípios estabelecidos na legislação pertinente.

2. DOS CONCEITOS E DEFINIÇÕES

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

I - **agente responsável:** servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de implementar procedimentos relativos ao uso seguro de tecnologias de computação em nuvem;

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

III - **nuvem:** recursos computacionais que podem ser utilizados de forma automatizada, dinâmica e sob demanda, disponibilizados através de grandes servidores

compartilhados e interligados por meio da Internet, possibilitando o acesso de qualquer lugar a qualquer hora;

IV - **nuvem privada:** infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

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

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

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

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

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

3. DOS PRINCÍPIOS

3.1. O INMETRO deve observar, no mínimo, os seguintes princípios antes de adotar a tecnologia de computação em nuvem:

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

II - alinhamento com os planos institucionais;

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

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

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

4. DAS DIRETRIZES GERAIS

4.1. O INMETRO ao contratar ou implementar soluções de computação em nuvem, deve garantir que:

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

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

III - o INMETRO deve avaliar quais informações serão hospedadas na nuvem computacional, considerando:

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

b) o valor do ativo de informação;

c) os controles de acesso, físicos e lógicos, relativos à Segurança da Informação;

d) o modelo de serviço e de implementação de computação em nuvem a serem adotados; e

e) a localização geográfica onde as informações estarão fisicamente armazenadas.

5. DOS REQUISITOS PARA A ADOÇÃO SEGURA DA COMPUTAÇÃO EM NUVEM

5.1. Os seguintes requisitos mínimos deverão ser observados pelo INMETRO 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.

5.2. Da transferência de serviços para um provedor de serviço de nuvem

5.2.1. Antes de transferir serviços ou informações para um provedor de serviço de computação em nuvem, o INMETRO deverá, no mínimo:

I - garantir que o provedor de serviços esteja em conformidade com a legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros as seguintes operações:

a) de coleta, armazenamento, guarda e tratamento de registros de dados pessoais; e

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

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, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas do INMETRO; e

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 do serviço de computação em nuvem.

5.3. **Da capacidade do provedor de serviço de nuvem para implementar atualizações**

5.3.1. Em função da capacidade de o provedor de serviço de computação em nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, o INMETRO deverá, no mínimo:

I - definir os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem; e

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

5.4. **Do gerenciamento de identidades e de registros (logs)**

5.4.1. O gerenciamento de identidades e de registros no INMETRO conforme suas incumbências e responsabilidades, deverá, no mínimo:

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 INMETRO;

III - adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia *single sign-on*, o qual deve ser acompanhado:

a) de autenticação multifator; ou

b) de outra alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem;

IV - exigir do provedor de serviço de nuvem que:

a) registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações; e

b) armazene, pelo período de um ano, todos os registros de que trata a alínea a;

V - armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por cinco anos, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do órgão ou da entidade contratante;

VI - manter em ambiente próprio controlado, pelo período de cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem; e

VII - capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de computação em nuvem.

5.5. **Do uso de recursos criptográficos**

5.5.1. Em relação à necessidade do uso de recursos criptográficos, o INMETRO deverá, no mínimo:

I - verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação;

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

III - utilizar, sempre que possível, chaves de encriptação baseadas em hardware.

5.6. **Da segregação de dados e da separação lógica**

5.6.1. Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o INMETRO, em conjunto com o provedor de serviço de computação em nuvem, deverão estabelecer, no mínimo, as seguintes ações:

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 pelos diferentes órgãos ou entidades da administração pública federal e por outros usuários do serviço em nuvem;

II - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados;

III - garantir a separação de todos os recursos utilizados pelo Provedor de Serviço de Computação em Nuvem daqueles recursos utilizados pela administração interna do INMETRO; e

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

5.7. **Do gerenciamento da nuvem**

5.7.1. Em relação ao gerenciamento da nuvem, o INMETRO deverá, no mínimo:

I - capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;

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

III - elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias; e

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

5.8. **Do tratamento da informação**

5.8.1. Em relação ao tratamento da informação em ambiente de computação em nuvem, o INMETRO, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e

III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) a informação com restrição de acesso prevista na legislação;

b) o material de acesso restrito regulado pelo próprio INMETRO;

c) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e

d) o documento preparatório não previsto no inciso II do caput.

5.8.2. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo INMETRO, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável;

III - informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do caput do item 5.8.1, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e

IV - no caso de dados pessoais, deverão ser observadas as orientações previstas na legislação competente sobre sobre privacidade e proteção de dados.

5.8.3. Os dados tratados em ambiente de nuvem devem ser armazenados em data centers localizados em território brasileiro, admitindo-se 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 no modelo de contratação de software e de serviços de computação em nuvem estabelecido pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

5.9. **Da contratação de software e de serviços de computação em nuvem**

5.9.1. As contratações de software e de serviços de computação em nuvem deverão ser realizadas observando-se o processo de contratação de soluções de tecnologia da informação e comunicação disposto pela Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, e o modelo de contratação descrito no Anexo I da Portaria nº 5.950, de 26 de outubro de 2023.

5.9.2. O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos estabelecidos nesta normativa e, no mínimo, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do órgão ou da entidade para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte do INMETRO, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III - proibição do uso de informações do INMETRO pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV - conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem ao INMETRO ao término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do INMETRO sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e

VII - garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 - LGPD.

5.9.3. Nas contratações de serviços em nuvem (IaaS, PaaS e SaaS) devem ser observados, no mínimo, os requisitos de privacidade e segurança da informação, além daqueles constantes nos *templates* de artefatos da contratação disponibilizados pelos órgãos competentes:

I - a contratação deve estar alinhada às normas correlatas publicadas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, a exemplo da

IN 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;

II - cada provedor de nuvem deve possuir, no mínimo, dois data centers em território brasileiro, capaz de ofertar serviços padronizados e altamente automatizados, nos quais os recursos de infraestrutura (por exemplo, computação, rede e armazenamento) são complementados por serviços de plataforma integrados, e deve cumprir os requisitos de segurança da informação estabelecidos nos artigos 20 e 25 da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021;

III - deve-se exigir, mediante justificativa prévia, que os provedores de serviços em nuvem possuam, no momento da assinatura do contrato, certificações de normas de segurança da informação aplicáveis ao objeto da contratação, assim como outros requisitos que objetivem mitigar riscos relativos à segurança da informação;

IV - devem ser predefinidos canais para comunicação, de maneira rápida e eficiente, e de acordo com os requisitos legais, regulatórios e contratuais, de eventos de segurança da informação;

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

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

VII - deve-se prever cópia dos logs fornecidos pelo provedor, de acordo com a política de retenção do cliente;

VIII - deve-se implementar controle de acesso lógico apropriado ao grau de confidencialidade dos dados armazenados na nuvem e controles para transferência de dados, como criptografia e uso de VPN adequada;

IX - cada provedor deve garantir controles eficazes e compatíveis com as políticas e procedimentos do cliente para gerenciamento de identidades de usuários e controle de acessos;

X - devem ser estabelecidas políticas e procedimentos para o uso de criptografia, incluindo gerenciamento de chaves criptográficas, que devem ser seguidos pelo cliente e pelo provedor;

XI - os dados armazenados no provedor devem estar criptografados, sendo que o esquema criptográfico deve ser adequado ao nível de sigilo das informações e as chaves criptográficas não devem ser armazenadas na nuvem;

XII - devem ser estabelecidos os limites do acesso do provedor aos dados do cliente e a responsabilidade do provedor em garantir o isolamento de recursos e dados contra acesso indevido por outros clientes;

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

XIV - a utilização de termo de confidencialidade, que deverá conter cláusula que impeça o integrador ou provedor de serviço de nuvem de usar, transferir, e liberar dados, sistemas, processos e informações do órgão ou da entidade para terceiros, como empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros, além

de incluir a proibição do uso de informações do INMETRO para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não autorizado;

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

XVI - deve-se exigir que o *cloud broker* disponibilize uma estrutura exclusiva de contas nos provedores de nuvem em nome do órgão ou entidade contratante, por meio das quais os serviços serão provisionados; e

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

6. **DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM**

6.1. Para que esteja habilitado a prestar serviços de computação em nuvem para o INMETRO, 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 INMETRO 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 INMETRO, 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 multifator 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 INMETRO 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 INMETRO 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;

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 INMETRO;

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

X - em relação à segregação de dados:

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

b) segregar o tráfego de gerenciamento do tráfego de dados do INMETRO; 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.

7. DA UTILIZAÇÃO DE CLOUD BROKERS

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

7.2. Caso o INMETRO contrate por meio do *cloud broker* plataforma de gestão multinuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

I - em relação às funcionalidades de provisionamento e orquestração de multinuvem:

a) um único portal integrado de provisionamentos para o usuário final;

b) utilização de modelos de provisionamento;

c) automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;

d) fluxos de trabalho de orquestração baseada em eventos; e

e) soluções seguras integradas de criação de infraestrutura por código - IaaC;

II - em relação às funcionalidades de monitoramento e análise em multinuvem:

a) relatórios de monitoramento de desempenho de recursos na nuvem;

b) coleta e monitoramento de registros; e

c) procedimentos de monitoramento de alertas.

III - em relação às funcionalidades de inventário e classificação em multinuvem:

a) inventário de recursos na nuvem;

b) procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem; e

c) detecção de recursos sem etiqueta.

IV - em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade:

a) mecanismos de *single sign-on* e de autenticação multifator das plataformas em nuvem;

b) gerenciamento seguro de usuários e de grupos de usuários;

c) gerenciamento de segurança dos recursos;

d) notificações de eventos de alerta multicanal;

e) gerenciamento de identidade e acesso - IAM; e

f) registros de atividade da plataforma em nuvem.

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

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

I - cumpram todos os requisitos previstos nesta normativa e na legislação brasileira; e

II - operem de acordo com as melhores práticas de segurança.

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

8. DAS RESPONSABILIDADES

8.1. Da Alta Administração

8.1.1. Compete à Alta Administração:

I - aprovar as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem e divulgá-las às partes interessadas.

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

III - disponibilizar recursos (humanos, tecnológicos e financeiros) para a implementação desta normativa.

8.2. Do Comitê de Segurança da Informação

8.2.1. Compete ao Comitê de Segurança da Informação:

I - estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem (com apoio do Gestor de Segurança da Informação e da CTINF);

II - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem (com apoio do Gestor de Segurança da Informação e da CTINF); e

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

8.3. Do Gestor de Segurança da Informação

8.3.1. Compete ao Gestor de Segurança da Informação:

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

II - supervisionar a aplicação do ato normativo sobre o uso seguro de computação em nuvem;

III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao INMETRO, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;

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, exceto se envolver dados pessoais, quando o Encarregado de dados será o responsável pela comunicação;

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.

9. **DA REVISÃO E ATUALIZAÇÃO**

9.1. Esta normativa bem como os documentos gerados a partir dela poderão ser revisados a qualquer tempo pela ETIR, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

9.2. Deverão ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas políticas e normas do INMETRO, quando considerada necessária pelo Comitê de Segurança da Informação.

9.3. Em função da capacidade de os provedores de serviço de computação em nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a presente normativa poderá ser revisada periodicamente, **não excedendo 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.

10. **DAS DISPOSIÇÕES FINAIS**

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

10.1.1. A certificação SOC 2 oferece uma evidência concreta de que o fornecedor adota boas práticas de segurança da informação e proteção de dados, contribuindo para a conformidade com a legislação vigente e demais normativos correlatos.

10.2. Esta normativa deve ser divulgada amplamente a todos os usuários e partes interessadas, a fim de promover sua observância e seu conhecimento.

10.3. A Alta Administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

10.4. O INMETRO adotará o foro brasileiro para dirimir quaisquer questões jurídicas relacionadas aos contratos firmados entre o contratante e o fornecedor do serviço.

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

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