MINISTÉRIO DAS COMUNICAÇÕES

PORTARIA MCOM Nº 5053, DE 24 DE MARÇO DE 2022

Aprova a Norma Complementar para Utilização Segura de Soluções de Computação em Nuvem.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, e a Instrução Normativa nº 05, de 30 de agosto de 2021, ambas do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Utilização Segura de Soluções de Computação em Nuvem.

Art. 2º O Ministério deverá adequar os contratos vigentes que possuam serviços de nuvem à esta Norma Complementar até o prazo previsto no art. 26 da Instrução Normativa GSI/PR nº 5, de 2021.

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

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA UTILIZAÇÃO SEGURA DE SOLUÇÕES DE COMPUTAÇÃO EM NUVEM

OBJETIVO

Esta norma tem por objetivo estabelecer as diretrizes e procedimentos para utilização segura de soluções de computação em nuvem no âmbito do Ministério das Comunicações - MCOM.

APLICAÇÃO

Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA

Instrução Normativa 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;

Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa 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;

Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;

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

1 DISPOSIÇÕES GERAIS

1.1 Para fins desta Norma Complementar, serão considerados os conceitos constantes do Glossário de Segurança da Informação, aprovado e atualizado por portaria do Gabinete de Segurança Institucional da Presidência da República.

1.2 A computação em nuvem é composta pelos seguintes modelos de implantação:

a) 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 e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

b) nuvem comunitária - infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

c) 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; e

d) 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.

1.3 O ambiente de computação em nuvem será gerenciado pelo administrador do ambiente de nuvem e seu substituto, sendo servidores ocupantes de cargo em comissão ou função comissionada da Coordenação-Geral de Tecnologia da Informação (CGTI).

1.3.1 São atribuições do administrador do ambiente de nuvem:

a) realizar a aplicação dos atos normativos sobre uso seguro de computação em nuvem;

b) configurar as soluções de computação em nuvem;

c) verificar os eventos gerados pela solução de computação em nuvem, tomando as providências necessárias para remediação de eventuais falhas;

d) tomar medidas preventivas para evitar falhas;

e) gerenciar mensagens e registros de auditoria (LOGs) da solução de computação em nuvem;

f) disponibilizar informações que subsidiem as decisões referentes à gestão da solução de computação em nuvem;

g) solicitar inclusão ou remoção de serviços e informações no ambiente de computação em nuvem, com anuência do gestor da informação;

h) propor modificações visando ao aperfeiçoamento desta Norma; e

1.4 Os gestores da informação são agentes públicos formalmente responsável pelo serviço e/ou pela informação disponibilizada no ambiente em nuvem. Preferencialmente, tanto o titular quanto o substituto devem ser da área negocial.

1.4.1 São atribuições dos gestores da informação:

a) solicitar, formalmente, a inclusão de informações no ambiente de computação em nuvem;

b) solicitar, formalmente, a remoção de informações no ambiente de computação em nuvem;

c) autorizar a solicitação de inclusão ou remoção de serviços e informações no ambiente de computação em nuvem feitas pela CGTI; e

d) validar, negocialmente, a inclusão ou remoção de serviços e informações eventualmente solicitadas.

1.5 Ao Gestor de Segurança da Informação compete:

a) instituir e coordenar a equipe responsável pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem;

b) supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;

c) assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

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

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

f) divulgar o ato normativo sobre uso seguro de nuvem às partes interessadas.

1.6 Ao Comitê de Segurança da Informação compete:

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

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

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

1.7 Esta Norma Complementar será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos.

2 PROCEDIMENTOS

2.1 Plano de migração e uso do ambiente de computação em nuvem

2.1.1 Deverá ser elaborado um plano de migração e uso do ambiente de computação em nuvem, conforme requisitos presentes na Instrução Normativa GSI/PR nº 05, de 2021, bem como nesta Norma Complementar.

2.1.2 O plano deverá, no mínimo, conter:

I – 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;

II - o modelo de serviço e de implementação de computação em nuvem que será adotado;

III – indicação de quais serviços e informações serão hospedados 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

IV - 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;

V – planejamento dos custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem;

2.1.3 Em relação aos serviços e informações previstos no inciso V do item 2.1.2 desta Norma, devem ser observadas 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, conforme o Anexo II desta Norma Complementar;

b) o material de acesso restrito regulado pelo próprio órgão ou pela entidade;

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

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

2.1.4 O plano deverá ser elaborado pela equipe responsável pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem, com a participação dos gestores da informação e ser aprovado pelo Comitê de Segurança da Informação.

2.1.5 O plano deverá ser revisado de forma periódica ou sempre que se fizer necessário, como nos casos de inclusão ou remoção de informações e serviços hospedados no ambiente em nuvem, não excedendo o período máximo de dois anos.

2.2 Contratação de novos provedores de serviço de nuvem

2.2.1 estar em conformidade com os requisitos previstos na Instrução Normativa GSI/PR nº 05, de 30 de agosto de 2021, bem como em conformidade com esta Norma Complementar.

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

2.2.3 Recomenda-se a utilização do Anexo I – Lista de verificação para uso seguro de soluções de computação em nuvem – desta Norma Complementar para facilitar a conferência dos

requisitos necessários.

2.2.4 A Lista de verificação não é exaustiva e deverá ser utilizada como instrumento de apoio.

2.2.5 A Lista de verificação deverá ser revisada sempre que houver alteração na IN GSI/PR nº 05, de 2021, bem como na alteração de processos internos do MCOM.

2.3 Contratos vigentes com provedores de serviço de nuvem

2.3.1 Os instrumentos contratuais em vigor devem ser analisados, considerando os requisitos apresentados na Instrução Normativa GSI/PR nº 05, de 30 de agosto de 2021, bem como nesta Norma Complementar.

2.3.2 Os instrumentos contratuais que não estejam em conformidade com o normativo vigente devem ser aditivados, incluindo os requisitos faltantes.

2.3.3 Na impossibilidade de realizar termos aditivos aos instrumentos contratuais vigentes, deve-se iniciar o planejamento de nova contratação de provedor de serviços em nuvem.

2.3.4 Os serviços e informações que estão disponíveis em ambiente de nuvem deverão ser analisados, conforme requisitos apresentados na Instrução Normativa GSI/PR nº 05, de 30 de agosto de 2021, especialmente nos arts. 11 e 17, e nesta Norma Complementar.

2.3.5 Os serviços e informações que não estejam em conformidade com os itens 2.1 e 2.2.4 desta Norma Complementar devem ser removidos do ambiente de nuvem.

2.3.6 Recomenda-se a utilização dos Anexo I e II desta Norma Complementar para facilitar a conferência dos requisitos necessários.

Anexo I – Lista de verificação para uso seguro de soluções de computação em nuvem

Referência	Descrição	Estado (Sim, Não, Não se aplica)	Observação	Evidência
IN GSI/PR nº 05, de 2021	**Dos atos anteriores à transferência de serviços para um provedor de serviço de nuvem**			
Art.11, inciso I, alínea a	A operação de coleta está alinhada à legislação brasileira e aos direitos à privacidade?			
Art.11, inciso I, alínea a	A operação de coleta está alinhada aos direitos à proteção dos dados pessoais?			
Art.11, inciso I, alínea a	A operação de coleta está alinhada ao sigilo das comunicações privadas e dos registros?			
Art.11, inciso I, alínea a	A operação de armazenamento está alinhada à legislação brasileira e aos direitos à privacidade?			
Art.11, inciso I, alínea a	A operação de armazenamento está alinhada aos direitos à proteção dos dados pessoais?			
Art.11, inciso I,	A operação de armazenamento está alinhada ao sigilo das comunicações privadas e dos registros?			

alínea a				
Art.11, inciso I, alínea a	A operação de guarda está alinhada à legislação brasileira e aos direitos à privacidade?			
Art.11, inciso I, alínea a	A operação de guarda está alinhada aos direitos à proteção dos dados pessoais?			
Art.11, inciso I, alínea a	A operação de guarda está alinhada ao sigilo das comunicações privadas e dos registros?			
Art.11, inciso I, alínea a	A operação de tratamento de registros de dados pessoais está alinhada à legislação brasileira e aos direitos à privacidade?			
Art.11, inciso I, alínea a	A operação de tratamento de registros de dados pessoais está alinhada aos direitos à proteção dos dados pessoais?			
Art.11, inciso I, alínea a	A operação de tratamento de registros de dados pessoais está alinhada ao sigilo das comunicações privadas e dos registros?			
Art.11, inciso I, alínea b	A operação de comunicações realizada por provedores de conexão e de aplicações de internet ocorre em território nacional?			
Art.11, inciso I, alínea b	A operação de comunicações realizada por provedores de conexão e de aplicações de internet está alinhada à legislação brasileira e aos direitos à privacidade?			
Art.11, inciso I, alínea b	A operação de comunicações realizada por provedores de conexão e de aplicações de internet está alinhada aos direitos à proteção dos dados pessoais?			
Art.11, inciso I, alínea b	A operação de comunicações realizada por provedores de conexão e de aplicações de internet está alinhada ao sigilo das comunicações privadas e dos registros?			
Art.11, inciso II, alínea a	Foi realizado o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, do tipo de informação a ser migrada?			
Art.11, inciso II, alínea b	Foi realizado o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, do fluxo de tratamento dos dados que podem ser afetados com a adoção da solução?			
Art.11, inciso II, alínea c	Foi realizado o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, do valor dos ativos envolvidos?			
Art.11, inciso II, alínea d	Foi realizado o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação, dos 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?			
Art.11, inciso III	Foi definido o modelo de serviço e de implementação de computação em nuvem que será adotado?			
Art.11, inciso IV	Em caso de sistemas estruturantes, foi utilizado somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas do MCOM?			
Art.11, inciso V, alínea a	Foram avaliadas quais informação seriam hospedadas na nuvem, considerando o processo de classificação da informação de acordo com a legislação?			

Art.11, inciso V, alínea b	Foram avaliadas quais informação seriam hospedadas na nuvem, considerando o valor do ativo de informação?			
Art.11, inciso V, alínea c	Foram avaliadas quais informação seriam hospedadas na nuvem, considerando os controles de acessos físico e lógico relativos à segurança da informação?			
Art.11, inciso V, alínea d	Foram avaliadas quais informação seriam hospedadas na nuvem, considerando o modelo de serviço e de implementação de computação em nuvem?			
Art.11, inciso VI	Foram definidas 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?			
Art.11, inciso VII	Foram planejados os custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem?			
	Da capacidade do provedor de serviço de nuvem para implementar atualizações			
Art. 12, inciso I	Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, foram definidos os critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem?			
Art. 12, inciso II	Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, foram definidas as revisões e atualizações periódicas dos processos internos do MCOM de gestão de riscos de segurança da informação?			
	Do gerenciamento de identidades e de registros (logs)			
Art. 13, inciso I	Foi adotado 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?			
Art. 13, inciso II	Foi negado ao provedor de serviço de nuvem a permissão de uso e acesso direto ao ambiente de autenticação do órgão ou da entidade?			
Art. 13, inciso III	De acordo com o nível de criticidade da informação, foi adotado o uso da tecnologia single sign-on?			
Art. 13, inciso III, alíneas a e b	O uso da tecnologia single sing-on é acompanhado da autenticação multifator OU outra alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem?			
Art. 13, inciso IV, alínea a	Foi exigido que o provedor de serviço de nuvem registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações?			
Art. 13, inciso IV, alínea b	Foi exigido que o provedor de serviço de nuvem armazene, pelo período de um ano, todos os registros de que trata o item anterior?			
Art. 13, inciso V	Os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, foram armazenados por cinco anos no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado?			
Art. 13, inciso VI	Os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem, foram mantidos em ambiente próprio controlado pelo período de cinco anos?			

Art. 13, inciso VII	A equipe de segurança foi capacitada para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem?			
	Do uso de recursos criptográficos			
Art. 14, inciso I	Foi verificado se os dados da organização estão sendo tratados e armazenados de acordo com a legislação?			
Art. 14, inciso II	Foi analisada a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios?			
Art. 14, inciso III	Foram utilizadas chaves de encriptação baseadas em hardware?			
	Da segregação de dados e da separação lógica			
	Art. 15. Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, os órgãos ou as entidades, em conjunto com o provedor de serviço de nuvem, deverão estabelecer, no mínimo, as seguintes ações:			
Art. 15, inciso I	Foi garantido que o ambiente contratado é protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas?			
Art. 15, inciso I	Foram implementados controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelo MCOM e por outros usuários do serviço em nuvem?			
Art. 15, inciso II	Foi garantida a aplicação de 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?			
Art. 15, inciso III	Foi garantida a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pelo MCOM?			
Art. 15, inciso IV	Foram avaliados os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem?			
	Do gerenciamento da nuvem			
Art. 16, inciso I	A equipe responsável pelo gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem foi capacitada?			
Art. 16, inciso II	Foi exigido 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?			
Art. 16, inciso III	Foi elaborada uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias do MCOM?			
Art. 16, inciso IV	Foi elaborado um processo de tratamento de incidentes junto ao provedor de serviço de nuvem?			
Art. 16, inciso IV	A equipe do MCOM responsável pelo gerenciamento da nuvem foi comunicada sobre o processo de tratamento de incidentes junto ao provedor de serviço de nuvem?			
	Do tratamento da informação			
Art. 17, caput	Em relação ao tratamento da informação em ambiente de computação em nuvem, o MCOM cumpriu as orientações contidas na legislação sobre proteção de dados pessoais?			
Art. 17, inciso I	Considerando a possibilidade de tratamento de informação sem restrição de acesso em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação, há esse tipo de informação tratada em ambiente de computação em nuvem do MCOM?			
Art. 17, inciso II	Considerando a impossibilidade de tratamento de informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada em ambiente de nuvem, esse tipo			

	de informação é tratada fora do ambiente de computação em nuvem do MCOM?			
Art. 17, inciso III, alínea a	Considerando a possibilidade de tratamento de informação com restrição de acesso prevista na legislação, conforme o Anexo II da presente Norma Complementar em ambiente de nuvem, observada a legislação e os riscos de segurança da informação, há esse tipo de informação tratada em ambiente de computação em nuvem do MCOM?			
Art. 17, inciso III, alínea b	Considerando a possibilidade de tratamento de material de acesso restrito regulado pelo próprio MCOM , observada a legislação e os riscos de segurança da informação, há esse tipo de informação tratada em ambiente de computação em nuvem do MCOM?			
Art. 17, inciso III, alínea c	Considerando a possibilidade de tratamento de informação pessoal relativa à intimidade, vida privada, honra e imagem, observada a legislação e os riscos de segurança da informação, há esse tipo de informação tratada em ambiente de computação em nuvem do MCOM?			
Art. 17, inciso III, alínea d	Considerando a possibilidade de tratamento de documento preparatório que não possa originar informação classificada, observada a legislação e os riscos de segurança da informação, há esse tipo de informação tratada em ambiente de computação em nuvem do MCOM?			
Art. 18, inciso I	Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo MCOM, transferidos para o provedor de serviço de nuvem, possuem pelo menos uma cópia atualizada de segurança mantida em território brasileiro?			
Art. 18, inciso II	A informação sem restrição de acesso possui cópias atualizadas de segurança fora do território brasileiro?			
Art. 18, inciso III	A informação com restrição de acesso prevista na legislação e o documento preparatório que não possa originar informação classificada, bem como suas cópias atualizadas de segurança, são tratados dentro do território brasileiro?			
Art. 18, inciso IV	No caso de dados pessoais, são observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto?			
	Das cláusulas contratuais específicas			
Art. 19, inciso I	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê o 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?			
Art. 19, inciso II	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê a garantia da exclusividade de direitos, por parte do órgão ou da entidade, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança?			
Art. 19, inciso III	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê a proibição do uso de informações do órgão ou da entidade pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado?			
Art. 19, inciso IV	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê a conformidade da política de segurança da			

	informação do provedor de serviço de nuvem com a legislação brasileira?			
Art. 19, inciso V	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê a devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem ao MCOM ao término do contrato?			
Art. 19, inciso VI	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê a eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do MCOM sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados?			
Art. 19, inciso VII	O instrumento contratual a ser firmado com um provedor de serviço de nuvem prevê a garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 - LGPD?			
	Dos requisitos do provedor de serviço de nuvem			
Art. 20, inciso I	O provedor de serviço de nuvem possui metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas e com a legislação, bem como realiza o gerenciamento de riscos descrito no inciso II do art. 11 da IN GSI/PR nº 05, de 2021?			
Art. 20, inciso II, alínea a	O provedor de serviço de nuvem desabilita ou remove todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional?			
Art. 20, inciso II, alínea b	O provedor de serviço de nuvem configura com segurança todas as interfaces de rede e áreas de armazenamento virtuais?			
Art. 20, inciso II, alínea c	O provedor de serviço de nuvem estabelece limites para a utilização dos recursos de máquina virtual (Virtual Machine - VM)?			
Art. 20, inciso II, alínea d	O provedor de serviço de nuvem mantem todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais?			
Art. 20, inciso II, alínea e	O provedor de serviço de nuvem valida a integridade das operações de gerenciamento de chaves criptográficas?			
Art. 20, inciso II, alínea f	O provedor de serviço de nuvem possui controles que permitam aos usuários autorizados do órgão ou da entidade acessarem os registros de acesso administrativo do monitor de máquina virtual - Hypervisor?			
Art. 20, inciso II, alínea g	O provedor de serviço de nuvem habilita o registro completo do Hypervisor?			
Art. 20, inciso II, alínea h	O provedor de serviço de nuvem suporta o uso de máquinas virtuais confiáveis (Trusted VM) fornecidas pelo MCOM, que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem?			
Art. 20, inciso III, alínea a	O provedor de serviço de nuvem possui 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?			
Art. 20, inciso III, alínea b	O provedor de serviço de nuvem impõe mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso?			
Art. 20, inciso III,	O provedor de serviço de nuvem suporta tecnologia single sign-on para autenticação?			

alínea c				
Art. 20, inciso III, alínea d	O provedor de serviço de nuvem suporta 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?			
Art. 20, inciso III, alínea e	O provedor de serviço de nuvem permiti ao órgão ou à entidade gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem?			
Art. 20, inciso III, alínea f	O provedor de serviço de nuvem atende aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo órgão ou pela entidade em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso)?			
Art. 20, inciso IV, alínea h	O provedor de serviço de nuvem utilizar firewalls especializados na proteção de sistemas e aplicações?			
Art. 20, inciso IV, alínea b	O provedor de serviço de nuvem desenvolve código web em conformidade com as melhores práticas de desenvolvimento seguro e com os normativos existentes?			
Art. 20, inciso IV, alínea c	O provedor de serviço de nuvem utiliza melhores práticas de segurança de sistemas operacionais e de aplicações?			
Art. 20, inciso IV, alínea d	O provedor de serviço de nuvem realiza periodicamente testes de penetração de redes e de aplicações?			
Art. 20, inciso IV, alínea e	O provedor de serviço de nuvem possui um programa de correção de vulnerabilidades?			
Art. 20, inciso V	O provedor de serviço de nuvem possui 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?			
Art. 20, inciso VI	O provedor de serviço de nuvem possui 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?			
Art. 20, inciso VII	O provedor de serviço de nuvem estabelece um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS)?			
Art. 20, inciso VIII	O provedor de serviço de nuvem utiliza um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo MCOM?			
Art. 20, inciso IX	O provedor de serviço de nuvem disponibiliza facilidades que possibilitem a aplicação de uma proteção criptográfica própria do MCOM?			
Art. 20, inciso X, alínea a	O provedor de serviço de nuvem isola, utilizando separação lógica, todos os dados e serviços do MCOM de outros clientes de serviço em nuvem?			
Art. 20, inciso X, alínea b	O provedor de serviço de nuvem segrega o tráfego de gerenciamento do tráfego de dados do MCOM?			
Art. 20, inciso X,	O provedor de serviço de nuvem implementa dispositivos de segurança entre zonas?			

alínea c				
Art. 20, inciso XI, alínea a	O provedor de serviço de nuvem sanitiza ou destrói, 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?			
Art. 20, inciso XI, alínea b	O provedor de serviço de nuvem destrói, 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 discrimina os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição?			
Art. 20, inciso XI, alínea c	O provedor de serviço de nuvem armazena, 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?			
Art. 20, inciso XII	O provedor de serviço de nuvem notifica, imediatamente, ao MCOM incidente cibernético contra os serviços ou dados sob sua custódia?			
Art. 20, inciso XIII	O provedor de serviço de nuvem possui procedimentos necessários para preservação de evidências, conforme legislação?			
Art. 20, inciso XIV	O provedor de serviço de nuvem demonstra 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?			
	Da utilização de Cloud Brokers			
Art. 22, inciso I, alínea a	A ferramenta do cloud broker possui um único portal integrado de provisionamentos para o usuário final?			
Art. 22, inciso I, alínea b	A ferramenta do cloud broker possui utilização de modelos de provisionamento?			
Art. 22, inciso I, alínea c	A ferramenta do cloud broker possui automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis?			
Art. 22, inciso I, alínea d	A ferramenta do cloud broker possui fluxos de trabalho de orquestração baseada em eventos?			
Art. 22, inciso I, alínea e	A ferramenta do cloud broker possui soluções seguras integradas de criação de infraestrutura por código - IaaC?			
Art. 22, inciso II, alínea a	A ferramenta do cloud broker possui relatórios de monitoramento de desempenho de recursos na nuvem?			
Art. 22, inciso II, alínea b	A ferramenta do cloud broker possui coleta e monitoramento de registros?			
Art. 22, inciso II, alínea c	A ferramenta do cloud broker possui procedimentos de monitoramento de alertas?			
Art. 22, inciso III, alínea a	A ferramenta do cloud broker possui inventário de recursos na nuvem?			
Art. 22, inciso III, alínea b	A ferramenta do cloud broker possui procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem?			

Art. 22, inciso III, alínea c	A ferramenta do cloud broker possui detecção de recursos sem etiqueta?			
Art. 22, inciso IV, alínea a	A ferramenta do cloud broker possui mecanismos de single sign-on de autenticação multifator das plataformas em nuvem?			
Art. 22, inciso IV, alínea b	A ferramenta do cloud broker possui gerenciamento seguro de usuários e de grupos de usuários?			
Art. 22, inciso IV, alínea c	A ferramenta do cloud broker possui gerenciamento de segurança dos recursos?			
Art. 22, inciso IV, alínea d	A ferramenta do cloud broker possui notificações de eventos de alerta multicanal?			
Art. 22, inciso IV, alínea e	A ferramenta do cloud broker possui gerenciamento de identidade e acesso - IAM?			
Art. 22, inciso IV, alínea f	A ferramenta do cloud broker possui registros de atividade da plataforma em nuvem?			
Art. 22, parágrafo único	Caso o cloud broker utilize ferramenta de Software as a Service (SaaS) comum de mercado, há risco de dependência tecnológica para disponibilizar essa plataforma?			
Art. 23, inciso I	O cloud broker garante que os provedores de serviço de nuvem que ele representa cumpram todos os requisitos previstos Instrução Normativa GSI/PR nº 05, de 2021, e na legislação brasileira?			
Art. 23, inciso II	O cloud broker garante que os provedores de serviço de nuvem que ele representa operem de acordo com as melhores práticas de segurança?			
Art. 23, parágrafo único	O MCOM prevê no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa?			
Art. 25, parágrafo único	O cloud broker apresentou os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa?			

Anexo II – Quadro exemplificativo de tipos descritivos de informação

Tipo	Descrição	
1. OSTENSIVA	Transparência Ativa	
	Transparência Passiva	
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1 Reservada - Prazo máximo de restrição de acesso de 5 anos	
	2.2 Secreta - Prazo máximo de restrição de acesso de 15 anos	
	2.3 Ultrassecreta - Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.	
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1 Sigilos Decorrentes de Direitos de Personalidade	
		3.1.1 Sigilo Fiscal
		3.1.2 Sigilo Bancário
		3.1.3 Sigilo Comercial
		3.1.4 Sigilo Empresarial
		3.1.5 Sigilo Contábil
	3.2 Sigilos de Processos e Procedimentos	
		3.2.1 Sigilo do Procedimento Administrativo Disciplinar em Curso
		3.2.2 Sigilo do Inquérito Policial
		3.2.3 Segredo de Justiça no Processo Civil
		3.2.4 Segredo de Justiça no Processo Penal
	3.3 Informação de Natureza Patrimonial	
		3.3.1 Segredo Industrial
		3.3.2 Direito Autoral
		3.3.3 Propriedade Intelectual de Programa de Computador
		3.3.3 Propriedade Industrial
4. PESSOAL	4.1. Pessoal - Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, honra e imagem das pessoas.	

Documento assinado eletronicamente por **Wanessa Queiroz de Souza Oliveira**, **Subsecretária de Planejamento e Tecnologia da Informação**, em 24/03/2022, às 10:33 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **9601876** e o código CRC **12D69DB7**.

Referência: Processo nº 53115.007158/2021-12 SEI nº 9601876