ISSN 1677-7042

DIÁRIO OFICIAL DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL • IMPRENSA NACIONAL

Ano CLIX Nº 165 Brasília - DF, terça-feira, 31 de agosto de 2021 SEÇÃO 1

Sumário

..... Esta edição completa do DOU é composta de 268 páginas .....

Atos do Poder Judiciário

SUPREMO TRIBUNAL FEDERAL

PLENÁRIO

DECISÕES
Arguição de Descumprimento de Preceito Fundamental
(Publicação determinada pela Lei nº 9.882, de 03.12.1999)

Acórdãos

ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 419 **(1)**
ORIGEM : ADPF - 419 - SUPREMO TRIBUNAL FEDERAL
PROCED. : DISTRITO FEDERAL
RELATOR : MIN. EDSON FACHIN
REQTE.(S) : CONFEDERAÇÃO NACIONAL DO COMÉRCIO DE BENS, SERVIÇOS E TURISMO - CNC
ADV.(A/S) : WILSON DO PRADO (10435/MS)
INTDO.(A/S) : UNIÃO
PROC.(A/S)(ES) : ADVOGADO-GERAL DA UNIÃO

Decisão: O Tribunal, por maioria, julgou improcedente a arguição de descumprimento de preceito fundamental, nos termos do voto do Relator, vencido o Ministro Marco Aurélio. Plenário, Sessão Virtual de 4.12.2020 a 14.12.2020.

ARGUIÇÃO DE DESCUMPRIMENTO FUNDAMENTAL (ADPF). DIREITO CONSTITUCIONAL. ART. 36, A, §§ 1º E 2º, DO DECRETO 21.981/1932. LIVRE EXERCÍCIO PROFISSIONAL. RESTRIÇÕES. LEILOEIRO. VEDAÇÃO AO EXERCÍCIO DO COMÉRCIO E À CONSTITUIÇÃO DE SOCIEDADE. INTERESSE PÚBLICO. ADEQUAÇÃO. RAZOABILIDADE. CONSTITUCIONALIDADE. IMPROCEDÊNCIA.

1. É legítima restrição legislativa ao exercício profissional quando indispensável à viabilização da proteção de bens jurídicos de interesse público igualmente resguardados pela própria Constituição, de que são exemplos a segurança, a saúde, a ordem pública, a incolumidade individual e patrimonial. Para tanto, requer-se que a disciplina legislativa tendente a condicionar o exercício profissional atenda aos critérios de adequação e de razoabilidade e seja justificada por razão de interesse público e sustentada em parâmetros técnicos idôneos à mitigação de riscos sociais próprios do exercício da profissão. Precedente.

2. As restrições dispostas no art. 36, "*a*", §§ 1º e 2º, do Decreto 21.981/1932, perseguem fins legítimos de interesse público, na medida em que, dada a relevância das atribuições de leiloeiros, relacionadas à administração da hasta pública e à alienação dos bens de terceiros, visam a coibir conflitos de interesse, ou seja, a garantir a atuação profissional proba, livre de ingerências que possam comprometer o desempenho de suas funções.

3. Não havendo restrição legislativa ao exercício da profissão de leiloeiro para além de incompatibilidades que lhe são próprias, as normas questionadas não se mostram injustificadas, arbitrárias ou excessivas para o fim a que se propõem, razão pela qual não há falar na alegada ofensa ao valor social do trabalho e ao livre exercício de qualquer trabalho, ofício ou profissão, consagrados nos arts. 1º, IV e 5º, XIII, da Constituição da República.

4. Arguição de Descumprimento de Preceito Fundamental julgada improcedente.

EMB.DECL. NA ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 419 **(2)**
ORIGEM : ADPF - 419 - SUPREMO TRIBUNAL FEDERAL
PROCED. : DISTRITO FEDERAL
RELATOR : MIN. EDSON FACHIN
EMBTE.(S) : CONFEDERAÇÃO NACIONAL DO COMÉRCIO DE BENS, SERVIÇOS E TURISMO - CNC
ADV.(A/S) : WILSON DO PRADO (10435/MS)
EMBDO.(A/S) : UNIÃO
PROC.(A/S)(ES) : ADVOGADO-GERAL DA UNIÃO

Decisão: O Tribunal, por maioria, acolheu os embargos de declaração, sem efeitos infringentes, para sanar a alegada omissão, nos termos do voto do Relator, vencido o Ministro Marco Aurélio, que dava provimento ao recurso, para, atribuindo efeitos modificativos à decisão, declarar não recepcionados, pela Constituição Federal, os parágrafos 1º e 2º da alínea *a* do artigo 36 do Decreto nº 21.981/1932. O Ministro Gilmar Mendes acompanhou o Relator com ressalvas. Plenário, Sessão Virtual de 4.6.2021 a 11.6.2021.

EMBARGOS DE DECLARAÇÃO EM ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL. DIREITO CONSTITUCIONAL. ART. 36, A, §§ 1º E 2º, DO DECRETO 21.981/1932. LIVRE EXERCÍCIO PROFISSIONAL. RESTRIÇÕES. LEILOEIRO. ALEGAÇÃO DE OMISSÃO. OCORRÊNCIA. RESERVA LEGAL. NORMAS ANTERIORES À CONSTITUIÇÃO. MATERIALMENTE COMPATÍVEIS À ORDEM VIGENTE. JUÍZO DE RECEPÇÃO. POSITIVO. EMBARGOS ACOLHIDOS, SEM EFEITOS MODIFICATIVOS.

1. No acórdão embargado, o Plenário deste Supremo Tribunal Federal julgou válidas as restrições do art. 36, *a* , §§ 1º e 2º, do Decreto 21.981/1932, ao exercício profissional de leiloeiro, por atenderem aos critérios de adequação e de razoabilidade.

2. Nos termos do artigo 1.022 do Código de Processo Civil de 2015, os embargos de declaração são cabíveis nos casos de obscuridade, contradição ou omissão da decisão impugnada, bem como para fins de correção de erro material. Na espécie, constata-se omissão, na decisão atacada, quanto a uma das causas de pedir que compuseram o pedido da reclamante.

3. Esta Corte já reconheceu que a recepção de normas pela Constituição ocorre considerando a compatibilidade do conteúdo do ato normativo, o que se dá na hipótese dos autos, conforme consignado no acórdão embargado.

4. Recepção do Decreto 21.981/1932 pelo ordenamento constitucional vigente como lei ordinária, inexistindo violação à exigência de reserva legal.

5. Embargos de declaração acolhidos, sem efeitos modificativos.

Secretaria Judiciária
PATRÍCIA PEREIRA DE MOURA MARTINS
Secretária

Atos do Poder Executivo

DECRETO Nº 10.782, DE 30 DE AGOSTO DE 2021

Altera o Decreto nº 9.319, de 21 de março de 2018, que institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, **caput**, inciso VI, alínea "a", da Constituição,

D E C R E T A :

Art. 1º O Decreto nº 9.319, de 21 de março de 2018, passa a vigorar com as seguintes alterações:

"Art. 1º .....
.....

§ 3º A E-Digital será disciplinada em ato do Ministro de Estado da Ciência, Tecnologia e Inovações e servirá de referência para o SinDigital." (NR)

"Art. 5º .....
.....

V - Ministério das Comunicações;

V-A - Ministério da Ciência, Tecnologia e Inovações;
....." (NR)

"Art. 11. A Secretaria-Executiva do CITDigital será exercida pelo Ministério da Ciência, Tecnologia e Inovações.
....." (NR)

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Brasília, 30 de agosto de 2021; 200º da Independência e 133º da República.

JAIR MESSIAS BOLSONARO
Marcos César Pontes
Maximiliano Salvadori Martinhão
Ciro Nogueira Lima Filho

Presidência da República

GABINETE DE SEGURANÇA INSTITUCIONAL

INSTRUÇÃO NORMATIVA Nº 5, DE 30 DE AGOSTO DE 2021

Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, e tendo em vista o disposto no art. 12 do Decreto nº 9.637, de 26 de dezembro de 2018, resolve:

Art. 1º Dispor 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.

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 2º Para fins desta Instrução Normativa, 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.

Art. 3º A computação em nuvem é composta pelos seguintes modelos de implantação:

I - 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;

II - 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;

III - 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

IV - 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.

CAPÍTULO II
DO ATO NORMATIVO SOBRE O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 4º Todos os órgãos ou as entidades, que desejarem utilizar computação em nuvem, deverão editar, obrigatoriamente, um ato normativo sobre o uso seguro de computação em nuvem.

Art. 5º O ato normativo sobre o uso seguro de computação em nuvem deverá, no mínimo:

I - ser elaborado com base na política de segurança da informação do órgão ou da entidade;

II - ser homologado pela alta administração e divulgado a todas as partes interessadas;

III - relacionar as metas a serem alcançadas e os objetivos que regem o serviço de computação em nuvem;

IV - definir as funções e as responsabilidades dos agentes designados para o gerenciamento dos serviços de computação em nuvem; e

V - estabelecer a periodicidade para sua revisão, a qual não deve exceder dois anos.

Parágrafo único. A revisão do ato normativo previsto no **caput** poderá ocorrer a qualquer tempo, 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.

Art. 6º O órgão ou a entidade deverá instituir uma equipe para elaboração e revisões do ato normativo sobre o uso seguro de computação em nuvem.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 7º Ao Gestor de Segurança da Informação compete:

I - instituir e coordenar a equipe descrita no art. 6º, responsável pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem;

II - supervisionar a aplicação do ato normativo sobre 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 órgão ou à entidade, 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; e

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.

Art. 8º Ao Comitê de Segurança da Informação ou à estrutura equivalente compete:

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

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

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

Art. 9º À alta administração do órgão ou da entidade compete 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.

CAPÍTULO IV
DOS REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

Art. 10. Deverão ser observados os requisitos mínimos deste Capítulo para que os órgãos ou as entidades adotem soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Seção I
Da transferência de serviços para um provedor de serviço de nuvem

Art. 11. Antes de transferir serviços ou informações para um provedor de serviço de nuvem, os órgãos ou as entidades deverão, no mínimo:

I - garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros as seguintes operações:

a) 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 de órgãos ou de entidades;

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.

Seção II
Da capacidade do provedor de serviço de nuvem para implementar atualizações

Art. 12. Em função da capacidade de o provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, os órgãos ou as entidades deverão, 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.

Seção III
Do gerenciamento de identidades e de registros (logs)

Art. 13. Em relação ao gerenciamento de identidades e de registros, os órgãos ou as entidades deverão, 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 órgão ou da entidade;

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

PRESIDÊNCIA DA REPÚBLICA • SECRETARIA-GERAL • IMPRENSA NACIONAL

JAIR MESSIAS BOLSONARO
Presidente da República

LUIZ EDUARDO RAMOS BAPTISTA PEREIRA
Ministro de Estado Chefe da Secretaria-Geral

SAVIO LUCIANO DE ANDRADE FILHO
Diretor-Geral da Imprensa Nacional

DIÁRIO OFICIAL DA UNIÃO
Em circulação desde 1º de outubro de 1862

ALEXANDRE MIRANDA MACHADO
Coordenador-Geral de Publicação e Divulgação

HELDER KLEIST OLIVEIRA
Coordenador de Editoração e Publicação de Jornais Oficiais

SEÇÃO 1 • Publicação de atos normativos
SEÇÃO 2 • Publicação de atos relativos a pessoal da Administração Pública Federal
SEÇÃO 3 • Publicação de contratos, editais, avisos e ineditoriais

www.in.gov.br ouvidoria@in.gov.br
SIG, Quadra 6, Lote 800, CEP 70610-460, Brasília - DF
CNPJ: 04196645/0001-00 Fone: (61) 3441-9450

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 nuvem.

Seção IV
Do uso de recursos criptográficos

Art. 14. Em relação à necessidade do uso de recursos criptográficos, os órgãos ou as entidades deverão, 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**.

Seção V
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:

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 Nuvem daqueles recursos utilizados pela administração interna do órgão ou da entidade; e

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

Seção VI
Do gerenciamento da nuvem

Art. 16. Em relação ao gerenciamento da nuvem, os órgãos ou as entidades deverão, 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.

Seção VII
Do tratamento da informação

Art. 17. Em relação ao tratamento da informação em ambiente de computação em nuvem, o órgão ou a entidade, 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, conforme o Anexo a esta Instrução Normativa;

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**.

Art. 18. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, 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 - a informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do **caput** art. 17, 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 Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

Seção VIII
Das cláusulas contratuais específicas

Art. 19. 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 nos art. 10 a art. 18 além de, 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 órgão ou da entidade, 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 órgão ou da entidade 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 aos órgãos ou às entidades contratantes 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 órgão ou entidade 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.

CAPÍTULO V
DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art. 20. Para que esteja habilitado a prestar serviços de computação em nuvem para os órgãos ou as entidades da administração pública federal, 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 descrito no inciso II do art. 11;

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 órgão ou da entidade 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 órgão ou pela entidade, 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 órgão ou à entidade 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 órgão ou pela entidade 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 órgão ou pela entidade;

IX - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do órgão ou da entidade;

X - em relação à segregação de dados:

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

b) segregar o tráfego de gerenciamento do tráfego de dados do órgão ou da entidade; e

c) implementar dispositivos de segurança entre zonas;

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

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

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

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

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

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

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

CAPÍTULO VI
DA UTILIZAÇÃO DE **CLOUD BROKERS**

Art. 21. O **cloud broker** deverá atuar como integrador dos serviços de computação em nuvem entre o órgão ou a entidade da administração pública federal e dois ou mais provedores de serviço de nuvem.

Art. 22. Caso o órgão ou a entidade 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; e

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.

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

Art. 23. 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 Instrução Normativa e na legislação brasileira; e

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

Parágrafo único. O órgão ou a entidade deverá prever no instrumento contratual que o **cloud broker** poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

CAPÍTULO VII
DISPOSIÇÕES GERAIS

Art. 24. Para garantir a segurança de que trata esta Instrução Normativa, os órgãos e as entidades poderão adotar outras diretrizes complementares, desde que não confrontem as previsões da legislação.

Art. 25. 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.

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

Art. 26. Os órgãos ou as entidades da administração pública federal que já estiverem utilizando os serviços de provedor de serviço de nuvem terão um prazo de doze meses, após a entrada em vigor desta Instrução Normativa, para adequação de seus contratos.

CAPÍTULO VIII
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 27. Ficam revogados os seguintes atos normativos:

I - Portaria GSI/PR nº 11, de 7 de fevereiro de 2012; e

II - Portaria GSI/PR nº 9, de 15 de março de 2018.

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

AUGUSTO HELENO RIBEIRO PEREIRA

ANEXO
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.	