PRESIDÊNCIA DA REPÚBLICA GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 9, DE 15 DE MARÇO DE 2018

PRESIDÊNCIA DA REPÚBLICA

GABINETE DE SEGURANÇA INSTITUCIONAL

DOU de 19/03/2018 (nº 53, Seção 1, pág. 22)

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso de suas atribuições que lhe são conferidas pelos incisos I e II do parágrafo único do art. 87 da Constituição Federal e tendo em vista o disposto no inciso IV do art. 10 da Lei nº 13.502, de 1º de novembro de 2017, e na , alterada pelas Portarias nº 114 e 132, de 18 de outubro de 2017 e 05 de dezembro de 2017 respectivamente, resolve:

Art. 1º - Fica homologada a Revisão 01 da Norma Complementar nº 14/IN01/DSIC/GSIPR que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação.

SERGIO WESTPHALEN ETCHEGOYEN

ANEXO

PRINCÍPIOS, DIRETRIZES E RESPONSABILIDADES RELACIONADOS À SEGURANÇA DA INFORMAÇÃO PARA O TRATAMENTO DA INFORMAÇÃO EM AMBIENTE DE COMPUTAÇÃO EM NUVEM

ORIGEM

Departamento de Segurança da Informação e Comunicações.

REFERÊNCIA LEGAL, NORMATIVA E BIBLIOGRÁFICA

Lei nº 12.527, de 18 de novembro de 2011.

Lei nº 12.965, de 23 de abril de 2014.

Decreto nº 3.505, de 13 de junho de 2000.

Decreto nº 7.724, de 16 de maio de 2012.

Decreto nº 7.845, de 14 de novembro de 2012.

Decreto nº 8.135, de 4 de novembro de 2013.

Decreto nº 9.203, de 22 de novembro de 2017.

Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República nº 01, de 13 de junho de 2008 e respectivas Normas Complementares.

Instrução Normativa nº 04 do Ministério do Planejamento Desenvolvimento e Gestão, de 11 de setembro de 2014.

CONSELHO NACIONAL DE ARQUIVO (Brasil). Glossário: Documentos Arquivísticos Digitais, 6ª versão, Rio de Janeiro: CONARQ, 2014.

CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

1. OBJETIVO

2. CONSIDERAÇÕES INICIAIS

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

4. CONCEITOS E DEFINIÇÕES

5. PRINCÍPIOS E DIRETRIZES

6. RESPONSABILIDADES

7. VIGÊNCIA INFORMAÇÕES ADICIONAIS

Esta Norma Complementar substitui a NC14/IN01/DSIC/ GSIPR, de 30 de janeiro de 2012.

APROVAÇÃO

NORIAKI WADA

Secretário de Coordenação de Sistemas

1 OBJETIVO

Estabelecer princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

2 CONSIDERAÇÕES INICIAIS

As tecnologias de computação em nuvem oferecem benefícios, como economicidade e eficiência, que podem ser aproveitados pelos órgãos ou entidades da APF. Associado a tais vantagens, o uso dessas novas tecnologias pode ocasionar o surgimento de riscos. Portanto, a Alta Administração de cada órgão ou entidade da APF deve considerar a Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC), de modo a salvaguardar dados, informações e serviços sob sua responsabilidade, visando a continuidade do negócio e preservando a Segurança da Informação e os interesses da sociedade e do Estado.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Incisos I e II do parágrafo único do art. 87 da Constituição Federal, no inciso IV do art. 10 da Lei nº 13.502, de 1 de novembro de 2017 e no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional da Presidência da República.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1 Alta Administração: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo-Direção e Assessoramento Superiores - DAS e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

4.2 Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

4.3 Computação em Nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

4.4 Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão ou entidade não autorizado nem credenciado;

4.5 Continuidade de Negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

4.6 Controle de Acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso aos meios de tecnologia oferecidos;

4.7 Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

4.8 Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

4.9 Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC): conjunto de processos que permitem identificar, analisar, avaliar e implementar as medidas necessárias para o tratamento de riscos e equilibrá-los com os custos operacionais e financeiros envolvidos;

4.10 Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, classificação e tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança de recursos humanos e segurança

documental aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações;

4.11 Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

4.12 Informação Classificada: é a informação sigilosa, à qual foi atribuída um grau de sigilo, conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

4.13 Informação Sigilosa: informação submetida à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

4.14 Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

4.15 Metadado: Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo;

4.16 Política de Segurança da Informação e Comunicações (POSIC): documento aprovado pela autoridade responsável do órgão ou entidade da APF, com o objetivo de estabelecer ações que visam a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações produzidas ou custodiadas por estes, independentemente da forma e do meio físico em que estejam registradas;

4.17 Provedor: ente, público ou privado, prestador de serviço de computação em nuvem;

4.18 Risco: probabilidade da ocorrência de um evento que tenha impacto na segurança da informação;

4.19 Segurança da Informação e Comunicações: consiste em assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação;

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

4.21 Tratamento de Incidentes de Segurança em Redes Computacionais: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

5 PRINCÍPIOS E DIRETRIZES

5.1 O órgão ou entidade da APF deve observar, no mínimo, ao adotar o tratamento da informação em ambiente de Computação em Nuvem:

5.1.1 A prevalência dos direitos e garantias fundamentais no tratamento das informações pessoais;

5.1.2 As diretrizes estabelecidas em sua Política de Segurança da Informação e Comunicações (POSIC) e normas complementares;

5.1.3 As diretrizes relativas à sua Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC);

5.1.4 As informações tratadas em ambiente de computação em nuvem devem passar por um processo de GRSIC;

5.1.5 As diretrizes relativas à sua Gestão de Continuidade, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC);

5.1.6 As legislações vigentes para contratação de Solução de Tecnologia da Informação;

5.1.7 As legislações vigentes relativas à Gestão de Segurança da Informação e Comunicações;

5.1.8 As diretrizes para implementação de controles de acesso relativos à *SIC*; e

5.1.9 A prevalência da legislação brasileira sobre qualquer outra.

5.2 Sobre o tratamento da informação:

5.2.1 Informação sem restrição de acesso: pode ser tratada, a critério do órgão ou entidade da APF, em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de *SIC*;

5.2.2 Informação sigilosa: como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:

5.2.2.1. Informação classificada: é vedado o tratamento em ambiente de computação em nuvem;

5.2.2.2. Conhecimento e informação contida em material de acesso restrito: é vedado o tratamento em ambiente de computação em nuvem;

5.2.2.3. Informação com restrição de acesso prevista em legislação vigente: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de *SIC*. O órgão ou entidade da APF deve adotar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade (DICA);

5.2.2.4. Documento Preparatório: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de *SIC*. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA;

5.2.2.5. Documento preparatório que possa originar informação classificada deve ser tratado conforme o item 5.2.2.1; e

5.2.2.6. Informação pessoal relativa à intimidade, vida privada, honra e imagem: a critério do órgão ou entidade da APF, pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de *SIC*. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA.

5.3 Deve ser assegurado que dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, bem como suas cópias de segurança, residam em território brasileiro;

5.4 Os dados, metadados, informações e conhecimento, produzidos ou custodiados por órgão ou entidade da APF, referentes aos itens 5.2.2.3, 5.2.2.4 e 5.2.2.6, devem residir exclusivamente em território brasileiro;

5.5 Na adoção de serviços de computação em nuvem, o órgão ou entidade da APF deve assegurar que sejam definidos, em instrumento contratual ou similar:

5.5.1 Requisitos que garantam a DICA das informações tratadas em ambiente de computação em nuvem;

5.5.2 Processo de comunicação e tratamento de incidentes de segurança em redes computacionais, considerando as exigências da legislação vigente;

5.5.3 Requisitos necessários para a realização de auditorias;

5.5.4 Que os dados, metadados, informações e conhecimento, tratados pelo provedor, não poderão ser fornecidos a terceiros e/ou usados por este provedor para fins diversos do previsto no referido instrumento contratual ou similar, sob nenhuma hipótese, sem autorização formal do órgão ou entidade da APF;

5.5.5 Requisitos necessários para a continuidade de negócio;

5.5.6 Requisitos necessários, para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva dos dados, metadados, informações e conhecimento; e

5.6 É vedado o tratamento de informação em ambientes de computação em nuvem não autorizados pela Alta Administração do respectivo órgão ou entidade da APF.

6 RESPONSABILIDADES

6.1 A Alta Administração de cada órgão ou entidade da APF, no âmbito de suas competências, é responsável pela segurança das informações tratadas em ambiente de computação em nuvem, em conformidade com as orientações contidas nesta norma e legislação vigente; e

6.2 O Gestor de Segurança da Informação e Comunicação do órgão, no âmbito de suas atribuições, é responsável pelas ações de implementação da gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem.

7 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.