Número da Norma Complementar	Revisão	Emissão	Folha
13/IN01/DSIC/GSIPR	00	30/JAN/12	1/5

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

DIRETRIZES PARA GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA LEGAL E NORMATIVA

Lei nº 10.683, de 28 de maio de 2003.
Decreto nº 7.411, de 29 de dezembro de 2010.
Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, e respectivas Normas Complementares.
ABNT NBR ISO/IEC 27002:2005.
COBIT 4.1.
ITIL.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Estabelecer diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

2 CONSIDERAÇÕES INICIAIS

2.1 Devido ao dinamismo da evolução das Tecnologias da Informação e Comunicações (TIC) nos dias atuais faz-se necessário preparar e adaptar as organizações públicas para as mudanças decorrentes deste avanço.

2.2 A Gestão de Mudanças nos aspectos relativos à segurança da informação e comunicações requer especial atenção e comprometimento da Alta Direção para apoiar estratégias de superação dos desafios das transformações a serem realizadas, visando minimizar possíveis resistências, e obter mudanças eficientes e eficazes.

2.3 O processo decisório das mudanças deve ser balizado por ações que visem viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

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

4.1 **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.

4.2 **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.3 **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

4.4 **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.5 **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 e a marca da organização, e suas atividades de valor agregado.

4.6 **Gestão de mudanças nos aspectos relativos à SIC**: é o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do órgão ou entidade da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

4.7 **Gestão de Riscos de Segurança da Informação e Comunicações**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

4.8 **Gestor de Mudanças**: é o responsável pelo processo de mudanças no âmbito do órgão ou entidade da APF.

4.9 **Gestor de Segurança da Informação e Comunicações**: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.

4.10 **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.11 **Mudança**: transição ou alteração de uma situação atual.

5 RESPONSABILIDADES E COMPETÊNCIAS

5.1 O Gestor de Segurança da Informação e Comunicações (Gestor de SIC) é o responsável pelas recomendações referentes às mudanças nos aspectos relativos à segurança da informação e comunicações, assim como, em observar todas as demais recomendações constantes nesta Norma Complementar. No processo de gerenciamento de mudanças, cabem-lhe as seguintes competências:

5.1.1 Avaliar os potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a implementação da mudança;
5.1.2 Recomendar a implementação ou não das mudanças propostas, indicando, sempre que possível, soluções que mitiguem riscos à SIC;
5.1.3 Verificar se o andamento e o resultado da mudança viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação; e
5.1.4 Capacitar em SIC as equipes envolvidas com os processos de mudanças.

5.2 O Gestor de Mudanças, no âmbito de suas atribuições, é o responsável pelo planejamento e implementação das mudanças no âmbito do órgão ou entidade da APF, assim como, em observar todas as recomendações constantes nesta Norma Complementar.

5.3 Compete ao Gestor de Mudanças, no que tange à SIC, envolver o Gestor de SIC no processo de mudanças nos aspectos relativos à segurança da informação e comunicações, bem como envolver a gestão de risco de SIC e a gestão de continuidade de negócios em SIC do órgão ou entidade da APF.

6 PROCEDIMENTOS

6.1 Recomenda-se adotar uma metodologia de processo de gestão de mudanças que atenda, no mínimo, ao objetivo e às diretrizes gerais definidos nesta Norma Complementar.

6.2 Recomenda-se que o processo de gestão de mudanças seja composto, no mínimo, pelas fases de Descrição, Avaliação, Aprovação, Implementação e Verificação, de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, conforme detalhado a seguir:

6.2.1 **Descrição**: nesta fase, deve-se realizar uma descrição detalhada da mudança, contendo escopo, objetivo e benefícios de modo que, a partir dessa descrição, possa ser feita uma análise dos impactos à segurança da informação e comunicações. O escopo de aplicação da mudança pode abranger o órgão ou entidade como um todo, um segmento ou um ativo de informação.

6.2.2 **Avaliação**: nesta fase, são avaliados os potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a implementação da mudança. Nesta fase deverão ser avaliados:

a) Os detalhes do procedimento de implementação da mudança;
b) A análise de risco do (s) ativo (s) de informação que serão afetados com a mudança;
c) As legislações e normas pertinentes;
d) A relação desta mudança com outras mudanças que possam estar ocorrendo simultaneamente;
e) O impacto de adiar ou de não se fazer a mudança.

6.2.3 **Aprovação**: nesta fase, formaliza-se a aprovação ou não das mudanças propostas com base nas avaliações descritas no item 6.2.2.

6.2.4 **Implementação**: nesta fase, as mudanças aprovadas são agendadas e implementadas de acordo com o procedimento aprovado no item 6.2.3.

6.2.5 **Verificação**: esta fase transcorre paralelamente à fase de Implementação, e nela é verificado se o andamento e o resultado da mudança viabilizam e asseguram a disponibilidade, integridade, confidencialidade e autenticidade da informação.

6.3 Orienta-se ao Gestor de Mudanças observar, ainda, se o processo de gestão de mudanças contempla os seguintes procedimentos:

a) Identificação e registro de todas as etapas das mudanças;
b) Correta alocação dos recursos disponíveis;
c) Planejamento e testes das mudanças;
d) Comunicação dos detalhes das mudanças para todas as pessoas envolvidas; e
e) Procedimentos de recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

7 DIRETRIZES GERAIS

Para que os resultados previstos sejam atingidos e da forma mais eficaz possível, são recomendadas as seguintes ações no processo de gestão de mudanças nos aspectos relativos à SIC:

7.1 Levar sempre em consideração a natureza e finalidade do órgão ou entidade da APF, alinhando-se à sua missão e ao planejamento estratégico.

7.2 Utilizar, sempre que possível, ferramentas e técnicas para gerenciar os vários aspectos envolvidos em um processo de mudança.

7.3 Promover interação constante com a gestão de SIC, gestão de riscos de SIC e gestão de continuidade de negócios em SIC.

7.4 Promover no órgão ou entidade da APF ampla divulgação das mudanças, visando a redução de eventuais resistências e dificuldades de implementação das mesmas.

8 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.