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

DIRETRIZES PARA AVALIAÇÃO DE CONFORMIDADE NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA 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 publicadas no D.O.U pelo DSIC/GSIPR.
ABNT NBR ISO/IEC 27001:2006.
ABNT NBR ISO/IEC 27002:2005.
Livreto de Avaliação de Conformidade, 5ª Edição, maio de 2007 do Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro.
Padrões de Interoperabilidade do Governo Eletrônico (e-PING).

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 avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

2 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.

3 CONCEITOS E DEFINIÇÕES

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

3.1 **Análise de riscos:** uso sistemático de informações para identificar fontes e estimar o risco;

3.2 **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;

3.3 **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;

3.4 **Avaliação de Conformidade em Segurança da Informação e Comunicações:** exame sistemático do grau de atendimento dos requisitos relativos à SIC com as legislações específicas;

3.5 **Avaliação de riscos:** processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

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

3.7 **Conformidade em Segurança da Informação e Comunicações:** cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização.

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

3.9 **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;

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

3.11 **Riscos de Segurança da Informação e Comunicações:** potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

3.12 **Verificação de Conformidade em Segurança da Informação e Comunicações:** procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à Segurança da Informação e Comunicações da organização.

4 PRINCÍPIOS E DIRETRIZES

4.1 As diretrizes gerais para a avaliação de conformidade em segurança da informação e comunicações deverão considerar, no mínimo, as legislações vigentes a respeito de SIC para a APF e normativos internos específicos de cada órgão;

4.2 A avaliação de conformidade em SIC deve ser contínua e aplicada visando contribuir com a Gestão de Segurança da Informação e Comunicações dos órgãos e entidades da APF;

4.3 A avaliação de conformidade em SIC pode ser subsidiada por meio da análise e avaliação de riscos e auditorias internas previsto no item 3.3.5 da NC 02/IN01/GSIPR/DSIC;

4.4 As não-conformidades relativas ao descumprimento de legislações, normas e procedimentos são consideradas riscos de SIC e devem ser tratadas segundo a NC 04/IN01/GSIPR/DSIC;

4.5 Os responsáveis pela verificação de conformidade devem considerar os requisitos mínimos que assegurem a disponibilidade, integridade, confidencialidade e autenticidade das informações, observando, dentre outros, as legislações vigentes a respeito de SIC para a APF e normativos internos específicos de cada órgão;

4.6 Os responsáveis pela avaliação de conformidade devem ser capacitadas nas legislações vigentes referentes à segurança da informação e comunicações; e

4.7 A avaliação de conformidade de SIC tomará, no mínimo, como base no inventário e mapeamento de ativos de informação dos órgãos e entidades da APF, visando manter a disponibilidade, integridade, confidencialidade e autenticidade das informações.

5 RESPONSABILIDADES

5.1 Cabe à Alta Administração do órgão ou entidade da Administração Pública Federal, direta e indireta – APF aprovar as diretrizes para avaliação de conformidade em SIC;

5.2 Cabe ao Gestor de Segurança da Informação e Comunicações:

5.2.1 acompanhar se os procedimentos de SIC estão sendo aplicados de forma atender a conformidade com legislações vigentes a respeito de SIC para a APF e normativos internos específicos de cada órgão;

5.2.2 Promover ações de capacitação para os responsáveis pela avaliação de conformidade, visando que esses tenham conhecimento das legislações vigentes que tratam sobre o assunto de SIC; e

5.3 Cabe ao responsável pela avaliação de conformidade remeter os resultados da avaliação de conformidade em SIC ao Gestor de Segurança da Informação e Comunicações.

6 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.