MINISTÉRIO DA CULTURA

CONFORMIDADE NORMATIVA E TÉCNICA

ORIGEM

Ministério da Cultura – MinC.

REFERÊNCIAS LEGAIS E NORMATIVAS

Portaria nº 327/2014/MinC - Aprova, no âmbito do Ministério da Cultura, norma de Segurança que estabelece as Diretrizes de Segurança da Informação e Comunicações.

Portaria nº 119/2011/MinC - Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações e dá outras providências.

Portaria nº 40/2013/MinC – Aprova o Regimento Interno do Ministério da Cultura.

ABNT ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.

Lei nº. 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

Lei nº. 8.666, de 21 de junho de 1993, estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios.

Lei nº. 9.279, de 14 de maio de 1996, que regula os direitos e obrigações relativas à propriedade industrial.

Lei nº. 9.610, de 18 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

Norma Complementar nº 02/IN01/GSIPR/DSIC, que define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

Norma Complementar nº 04/IN01/DSIC/GSIPR – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da Administração Pública Federal.

Norma Complementar nº 11/IN01/DSIC/GSIPR, que estabelece 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.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Ministério da Cultura – MinC.

SUMÁRIO

APROVAÇÃO

Comitê de Segurança da Informação e Comunicações - CSIC

1. OBJETIVO

1.1 Garantir a conformidade dos ativos e processos internos com as políticas e normas organizacionais de segurança da informação.

2. ESCOPO

2.1 Estabelecer diretrizes para verificação da conformidade legal dos ativos e processos internos, visando a evitar violações de segurança da informação previstas em estatutos, regulamentações, portarias, normativos internos e/ou obrigações contratuais.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores envolvidos com as auditorias de segurança da informação e comunicações, sendo de responsabilidade de cada um o seu cumprimento.

4. CONCEITOS E DEFINIÇÕES

4.1 Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações estão conceituados no Dicionário de Referência.

5. PRINCÍPIOS

5.1 Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, integridade, confidencialidade e autenticidade, visando à proteção e à preservação das informações necessárias às atividades da instituição.

6. CONFORMIDADE COM AS POLÍTICAS E NORMAS DE SEGURANÇA DA INFORMAÇÃO

6.1 A avaliação de conformidade em segurança da informação e comunicações deve ser contínua e aplicada visando a contribuir com a Gestão de Segurança da Informação e Comunicações (Ref. NC 11/IN01/DSIC/GSIPR).

6.2 A avaliação de conformidade em segurança da informação e comunicações pode ser subsidiada por meio da análise e avaliação de riscos e auditorias internas, das ações de segurança da informação e comunicações, em intervalos planejados de pelo menos uma vez ao ano (Ref. NC 02/IN01/DSIC/GSIPR e NC 11/IN01/DSIC/GSIPR).

6.3 A avaliação de conformidade de segurança da informação e comunicações tomará como base, no mínimo, o inventário de ativos de informação. (Ref. NC 11/IN01/DSIC/GSIPR).

6.4 Os responsáveis pela verificação de conformidade devem considerar os requisitos mínimos que assegurem disponibilidade, integridade, confidencialidade e autenticidade das informações, observando, dentre outros, as legislações vigentes a respeito de segurança da informação e comunicações e a POSIC (Ref. NC 11/IN01/DSIC/GSIPR).

6.5 Os responsáveis pela avaliação de conformidade devem ser capacitados nas legislações vigentes referentes à segurança da informação e comunicações (Ref. NC 11/IN01/DSIC/GSIPR).

6.6 As não-conformidades relativas ao descumprimento de legislações, normas e procedimentos são consideradas riscos de segurança da informação e comunicações e devem ser tratadas atendendo aos seguintes requisitos e procedimentos (Ref. NC 11/IN01/DSIC/GSIPR):

a) considerar as opções de reduzir, evitar, transferir ou reter o risco, observando (Ref. NC 04/IN01/DSIC/GSIPR):

   - a eficácia das ações de segurança da informação e comunicações já existentes;
   - as restrições organizacionais, técnicas e estruturais;
   - os requisitos legais; e
   - a análise custo/benefício.

b) formular um plano para o tratamento dos riscos, relacionando, no mínimo, as ações de segurança da informação e comunicações, responsáveis, prioridades e prazos de execução necessários à sua implantação (Ref. NC 04/IN01/DSIC/GSIPR);

c) executar as ações de segurança da informação e comunicações incluídas no plano de tratamento dos riscos aprovado (Ref. NC 04/IN01/DSIC/GSIPR); e

d) detectar possíveis falhas nos resultados, monitorar os riscos, as ações de segurança da informação e comunicações e verificar a eficácia do processo de Gestão de Riscos de Segurança da Informação e Comunicações (Ref. NC 04/IN01/DSIC/GSIPR).

6.7 Os relatórios e registros gerados no processo de verificação devem ser tratados e armazenados conforme maior grau de sigilo atribuído às informações envolvidas.

6.8 Os proprietários dos ativos de informação devem assegurar que dentro da sua área de competência seja divulgada e cumprida a Política de Segurança da Informação e Comunicações e normas correlatas, bem como devem executar periodicamente, pelo menos, as seguintes atividades:

a) realizar ações que visem a identificar o grau de cumprimento da Política de Segurança da Informação e Comunicações e normas correlatas junto aos seus subordinados; e

b) estabelecer ações corretivas, tais como: ajuste da documentação, ajuste no processo de trabalho, capacitação de servidores e colaboradores e comunicação à autoridade competente nos casos de infrações disciplinares.

7. VERIFICAÇÃO DA CONFORMIDADE TÉCNICA

7.1 O proprietário do ativo de informação, juntamente com a área responsável pela administração dos recursos de tecnologia da informação, deve adotar medidas para realizar periodicamente verificações nos recursos de tecnologia da informação quanto ao cumprimento da Política de Segurança da Informação e Comunicações e conformidades técnicas contratuais, por meio de atividades, tais como:

a) análise de risco;
b) avaliação das vulnerabilidades;
c) testes de invasão; e
d) testes de carga.

7.2 A verificação de conformidade técnica deve ser realizada por profissional com competência para a realização da respectiva atividade com apoio de ferramentas que automatizem o processo e emitam relatórios técnicos.

7.3 Os relatórios e registros gerados no processo de verificação devem ser tratados e armazenados conforme maior grau de sigilo atribuído às informações envolvidas.

8. PENALIDADES

8.1 Todos os servidores e colaboradores estão sujeitos às regras da Política de Segurança da Informação e Comunicações e devem observar integralmente o que dispõe este documento. A inobservância dessas regras acarretará em apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização administrativa, civil e penal.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 Os servidores e os colaboradores devem ter conhecimento da Política de Segurança da Informação e Comunicações, tendo a obrigação de seguir rigorosamente o disposto nas normas de segurança.

10. DISPOSIÇÕES GERAIS

10.1 Qualquer dúvida ou sugestões sobre a Política de Segurança da Informação e Comunicações e suas orientações devem ser imediatamente encaminhadas à área responsável por Segurança da Informação para análise e/ou esclarecimento.

11. ATUALIZAÇÃO

11.1 Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação e Comunicações, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

12. VIGÊNCIA

12.1 Esta norma entra em vigor na data de sua publicação.