MINISTÉRIO DA CULTURA

CAPACITAÇÃO EM SEGURANÇA

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.

NBR ISO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

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

Norma Complementar nº 18/IN01/DSIC/GSIPR – Estabelece diretrizes para as atividades de ensino em segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.

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 Assegurar que os servidores e colaboradores estejam conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estejam preparados para apoiar a Política de Segurança da Informação e Comunicações da instituição durante os seus trabalhos, a fim de reduzir o risco de erro humano.

2. ESCOPO

2.1 Estabelecer orientações complementares ao processo de capacitação e sensibilização em segurança da informação e comunicações para assegurar que os servidores e colaboradores estejam conscientes das ameaças e das preocupações relativas à segurança da informação e comunicações, suas responsabilidades e obrigações, e estejam preparados para apoiar a Política de Segurança da Informação e Comunicações durante os seus trabalhos diários, reduzindo o risco de quebras de segurança.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores envolvidos com o processo de capacitação e sensibilização em 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. RESPONSABILIDADES DA DIREÇÃO

6.1 A direção da instituição deve assegurar que os servidores e colaboradores possuam os conhecimentos mínimos para a execução de suas tarefas, conheçam a Política de Segurança de Informações e Comunicações e sejam devidamente capacitados para o uso seguro dos ativos de informação.

7. CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

7.1 Atribuições

7.1.1 Cabe ao Gestor de Segurança da Informação e Comunicações – GSIC, com apoio do Serviço de Segurança e Riscos em Tecnologia da Informação – SERTI, elaborar e atualizar anualmente o Programa de Capacitação e Sensibilização em Segurança da Informação e Comunicações - SIC pertencente ao Plano de Capacitação e Desenvolvimento do MinC – PCDMinC.

7.1.2 Cabe ao Comitê de Segurança da Informação e Comunicações – CSIC aprovar o Programa de Capacitação e Sensibilização em SIC, bem como dar o devido apoio estratégico.

7.1.3 Cabe à área responsável pela gestão de pessoas executar o Programa de Capacitação e Sensibilização com o apoio da SERTI e produzir material didático para os cursos e treinamentos, bem como avaliar e propor alterações neste Programa.

7.1.4 Cabe à Assessoria de Comunicação Social – ASCOM produzir o material publicitário para a execução das ações prevista neste Programa.

7.1.5 Cabe à área responsável pelos recursos logísticos prestar apoio operacional nas ações relacionadas à segurança física.

7.1.6 Cabe à área responsável pela administração dos recursos de tecnologia da informação prestar apoio operacional quando há necessidade de utilização dos recursos tecnológicos do Ministério.

7.2 Conteúdo programático

7.2.1 As ações de capacitação e sensibilização devem abordar, no mínimo, esclarecimentos sobre os seguintes temas:

a) Conceitos Gerais de Segurança da Informação;
b) Política de Segurança da Informação e Comunicações – POSIC e suas normas complementares;
c) Melhores Práticas em Segurança da Informação; e
d) Classificação da Informação.

7.3 Orientações metodológicas

7.3.1 Os conteúdos devem ser abordados de maneira dinâmica com ênfase nas melhores práticas.

7.3.2 Os materiais didáticos e publicitários tais como: cartilhas, mídias e cartazes, devem utilizar linguagem adequada aos diversos tipos de público.

7.3.3 A localização e o acesso à POSIC e suas normas complementares devem ser facilitados por meio da utilização de links nos materiais didáticos e publicitários.

7.3.4 As ações devem ter adesão voluntária.

7.3.5 Devem ser capacitados agentes multiplicadores.

7.4 Ações de capacitação e sensibilização

7.4.1 Dia da Segurança da Informação

a) descrição: dia dedicado a orientar os usuários quanto às melhores práticas de Segurança da Informação; e
b) periodicidade: anualmente no segundo semestre.

7.4.2 Cursos Presenciais

a) descrição: cursos presenciais, divididos em, no mínimo, 2 (dois) módulos, podendo ser divididos por semestre, os quais serão ministrados pela SERTI com auxílio da área responsável pela gestão de pessoas, com duração de 4 (quatro) horas cada módulo; e
b) periodicidade: anual.

7.4.3 Cursos de Capacitação e Reciclagem para o CSIC/SERTI

a) descrição: cursos básicos de Segurança da Informação aos membros do CSIC e cursos avançados à SERTI. Ressalta-se que estes cursos de capacitação poderão ser providos por empresas ou profissionais especializados em treinamento de SIC, devendo ser, preferencialmente, realizado nas dependências do MinC; e
b) periodicidade: anual.

7.4.4 Exibição de dicas de Segurança

a) descrição: exibição de dicas de segurança em locais de acesso ao público interno; e
b) periodicidade: mensal.

7.4.5 Simulação de Evacuação do Prédio

a) descrição: simulação de evacuação das dependências do MinC, realizada pelo Corpo de Bombeiros do Distrito Federal com o auxílio da Brigada de Incêndio do MinC; e
b) periodicidade: anual.

7.4.6 Cursos de Prevenção e Combate a Incêndio

a) Descrição: cursos de prevenção e combate a incêndio, ministrados pela Brigada de Incêndio do MinC; e
b) Periodicidade: anual.

7.5 Planejamento da capacitação e sensibilização em Segurança da Informação e Comunicações

7.5.1 O planejamento anual da conscientização, educação e treinamento de servidores e colaboradores sobre Segurança da Informação e Comunicações deve ter orçamento contemplado dentro do Plano de Capacitação e Desenvolvimento do MinC – PCDMinC.

7.5.2 O planejamento anual da conscientização, educação e treinamento de servidores e colaboradores sobre Segurança da Informação e Comunicações deve incluir as orientações/instruções no período de ambientação, formação inicial ou continuada em seus órgãos ou entidades, por meio de atividades de ensino de sensibilização, conscientização, capacitação e especialização (Ref. 18/IN01/DSIC/GSIPR).

8. PROCESSO DISCIPLINAR

8.1 O processo disciplinar referente à segurança da informação e comunicações deve buscar informar, treinar ou estabelecer o desempenho desejado e esperado dos servidores e colaboradores, devendo seguir o exposto nas normas que rege o assunto.

8.2 As infrações e quebras de segurança cometidas pelos servidores e colaboradores devem ser avaliadas pelo Gestor de Segurança da Informação e Comunicações, que pode contar com o apoio do SERTI, em uma verificação prévia das evidências que confirmem se a violação realmente ocorreu.

a) as evidências de infrações e quebras de segurança devem abranger: a admissibilidade da evidência (se a evidência pode ser ou não utilizada) e importância da evidência (relacionada ao risco que impõe à informação).

8.3 Uma vez confirmada a infração ou quebra de segurança e decidido proceder com o processo disciplinar, é imperativa a observância à legislação que rege a matéria e importante que se assegure um tratamento constitucional na apuração, com direito à ampla defesa e contraditório aos servidores e colaboradores suspeitos de cometer violações. De forma gradual conforme reincidência e proporcional aos fatores (natureza e gravidade) da violação e o seu impacto nas atividades da instituição:

a) informar sobre a violação ao servidor ou colaborador, obedecendo aos princípios da simplicidade, formalidade e celeridade;
b) relatar o caso à área de gestão de pessoas para que tome as devidas providências.

9. PENALIDADES

9.1 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.

10. COMPETÊNCIAS E RESPONSABILIDADES

10.1 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.

11. DISPOSIÇÕES GERAIS

11.1 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.

12. ATUALIZAÇÃO

12.1 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.

13. VIGÊNCIA

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