MINISTÉRIO DA CULTURA

PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

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 – 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.

ABNT NBR ISO/IEC 38500:2009 – Governança Corporativa de Tecnologia da Informação.

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 Proteger a integridade do software e da informação contra códigos maliciosos.

2. ESCOPO

2.1 Dispor sobre as regras de segurança a serem seguidas pela área responsável pela proteção contra a ação de códigos maliciosos pelos servidores e colaboradores do MinC.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação da rede corporativa, doravante chamados simplesmente de administradores de recursos de tecnologia da informação, 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. CONTROLES CONTRA CÓDIGOS MALICIOSOS

6.1 Administração da solução contra código malicioso

6.1.1 Os Recursos de Tecnologia da Informação devem estar providos de soluções de detecção e bloqueio de programas de código malicioso, como antispyware, programas antivírus, programas de análise de conteúdo de correio eletrônico e do acesso à Internet.

6.1.2 A área responsável deve especificar e homologar soluções de detecção e bloqueio de programas de código malicioso, considerando, ao menos, as seguintes características:

a) possuírem uma console de administração centralizada;
b) permitirem atualização automática e programável;
c) permitirem bloqueio de alteração das configurações através de senha;
d) proverem serviço de atualização, no mínimo mensal, por parte do fabricante;
e) possuírem um mecanismo de varredura em tempo real;
f) possuírem um mecanismo de controle estatístico e emissão de relatórios;

g) possuírem um mecanismo de controle centralizado com emissão de alertas de problemas;
h) possuírem bloqueio de execução de aplicações não homologadas;
i) possuírem bloqueio de conteúdos web maliciosos; e
j) possuírem *personal firewall*.

6.1.3 A área responsável deve verificar periodicamente junto aos fabricantes, a disponibilidade de atualizações da solução de detecção e bloqueio de programas maliciosos.

6.1.4 As atualizações e correções de versão das soluções de detecção e bloqueio de programas maliciosos devem ser homologadas antes de serem aplicadas ao ambiente de produção.

6.1.5 A área responsável deve elaborar e manter atualizada a documentação com a descrição dos procedimentos de instalação e configuração das soluções de detecção e bloqueio de programas de código malicioso.

6.1.6 As documentações devem ser guardadas em local seguro, com acesso controlado e restrito à área responsável.

6.2 Instalação e configuração da solução contra código malicioso

6.2.1 A instalação e configuração da solução de detecção e bloqueio de programas maliciosos somente devem ser realizadas pela área responsável.

6.2.2 A área responsável deve agendar o software de proteção para executar periodicamente varredura completa nas estações de trabalho ou dispositivos móveis do MinC.

6.2.3 A área responsável deve configurar as soluções de detecção e bloqueio de ameaças para verificar as mensagens recebidas por correio eletrônico e/ou arquivos quanto à contaminação por vírus de computador e código malicioso.

6.3 Uso e manutenção da solução contra código malicioso

6.3.1 É vedada a instalação de softwares nos recursos computacionais do MinC sem o prévio conhecimento e autorização da área responsável.

6.3.2 Os softwares utilizados devem estar devidamente licenciados e respeitar os direitos autorais e contratuais.

6.3.3 A área responsável não se responsabilizará por softwares pessoais instalados pelos usuários em recursos computacionais do MinC ou de terceiros.

6.3.4 É obrigatório o uso de software de proteção nos recursos de tecnologia da informação do MinC disponibilizados para os usuários, considerando as seguintes características:

a) deve ser mantido sempre ativado e atualizado;
b) deve ser configurado para operar de forma transparente para o usuário; e
c) deve ser configurado de forma a impedir que o usuário consiga desabilitar ou interromper o correto funcionamento.

6.3.5 Na detecção de mensagens de correio eletrônico e arquivos contaminados com códigos maliciosos devem ser executados, no mínimo, os seguintes procedimentos:

a) enviar alertas a área responsável, caso sejam identificados códigos maliciosos nos recursos da tecnologia da informação;
b) enviar ao usuário uma notificação quando do recebimento de uma mensagem de correio eletrônico ou arquivo contaminado;
c) guardar as mensagens de correio eletrônico e os arquivos suspeitos em uma área de acesso restrito (quarentena), por tempo determinado, para tratamento adequado; e
d) desligar imediatamente os recursos de tecnologia da informação suspeitos.

6.3.6 Procedimentos necessários para salva e recuperação de software e informação infectados e danificados por programas maliciosos devem ser previstos em planos de contingência.

7. PENALIDADES

7.1 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.

8. COMPETÊNCIAS E RESPONSABILIDADES

8.1 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.

9. DISPOSIÇÕES GERAIS

9.1 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.

10. ATUALIZAÇÃO

10.1 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.

11. VIGÊNCIA

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