ANEXO VII

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES CONTRA CÓDIGOS MALICIOSOS

ÍNDICE

1. DESCRIÇÃO

1.1. Entende-se por código malicioso um programa de computador, ou parte de um programa, desenvolvido para danificar, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores. Esses programas podem ainda fazer cópias de si mesmo e auto propagar-se por toda rede. Esta norma estabelece os critérios seguros a serem seguidos pelos agentes públicos pertencentes à Área de TI do MEC para prevenção e proteção de códigos maliciosos em servidores, estações de trabalho e demais recursos computacionais e de comunicação da rede interna do MEC.

2. PÚBLICO ALVO

2.1. Este documento se aplica a todos os agentes públicos pertencentes à Área de TI do MEC.

3. OBJETIVO

3.1. Definir requisitos de prevenção e proteção a códigos maliciosos nos recursos computacionais e de comunicação da rede interna do MEC.

4. ESCOPO

4.1. Instalação, configuração e administração de mecanismos de proteção contra códigos maliciosos.

5. NÃO ESCOPO

5.1. Aquisição de *softwares* de proteção contra códigos maliciosos.

6. DOCUMENTOS DE REFERÊNCIA

6.1. Norma Técnica ABNT NBR ISO/IEC 27002:2005, Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação.

6.2. Norma Técnica ABNT NBR ISO/IEC 27001:2006, Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos.

6.3. Guia Técnico ABNT ISO GUIA 73:2009, Gestão de Riscos - Vocabulário.

6.4. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

6.5. Decreto nº 4.553, de 27 de dezembro de 2002, revogado pelo Decreto n° 7.845, de 14 de novembro de 2012, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

6.6. Norma Complementar nº 03/IN01/DSIC/GSIPR, estabelece as diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

6.7. Manual de boas práticas em Segurança da Informação do Tribunal de Contas da União, terceira edição, publicado em 2008 no site http://www.tcu.gov.br.

6.8. Política de Segurança da Informação e Comunicações do MEC.

7. DEFINIÇÕES

7.1. Os conceitos e definições dos termos técnicos utilizados nesse documento encontram-se no “Dicionário de referência da Política de Segurança da Informação e Comunicações”.

8. REGRAS GERAIS

8.1. A definição e homologação dos softwares a serem instalados nos recursos computacionais e de comunicação de propriedade do MEC são de responsabilidade da Área de TI do MEC.

8.2. Ao Agente Público descumpridor dessa norma serão aplicadas as sanções previstas na legislação em vigor.

8.3. Na ocorrência de quebra de segurança por meio de recursos computacionais, a Área de TI do MEC deve ser imediatamente informada para adotar as providências necessárias, limitando o acesso às informações e/ou recursos computacionais do MEC, caso seja necessário.

8.4. Os usuários da rede interna do MEC devem reportar à Área de TI do MEC as ocorrências de incidentes que afetem os ativos de informação ou descumprimento dessa norma tão logo tomem ciência do ocorrido.

8.5. Os casos omissos a essa norma devem ser encaminhados à Área de TI do MEC para o devido tratamento.

9. GERENCIAMENTO DE PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

9.1. A Área de TI do MEC deve instalar configurar e gerenciar mecanismos de detecção e bloqueio de códigos maliciosos nos recursos computacionais do MEC, tais como: *softwares* de antivírus, *antispyware*, análise de conteúdo *web*, análise de correio eletrônico e *IPS* (*Intrusion Protection System*).

9.2. A Área de TI do MEC deve definir e homologar mecanismos de detecção e bloqueio de códigos maliciosos, considerando pelo menos as seguintes características:

9.2.1. Possuir uma console de administração centralizada com possibilidade de instalação remota;

9.2.2. Permitir atualização automática e programável;

9.2.3. Permitir configuração de perfis de acesso;

9.2.4. Permitir bloqueio de alteração das configurações por meio de senha;

9.2.5. Ter serviço de suporte do fabricante em idioma português;

9.2.6. Ter serviço de atualização do fabricante;

9.2.7. Possuir um mecanismo de varredura em tempo real;

9.2.8. Possuir um mecanismo de controle estatístico e emissão de relatórios.

9.3. Os *softwares* utilizados como mecanismos de detecção e bloqueio de códigos maliciosos devem estar devidamente licenciados e respeitar os direitos autorais e contratuais do fornecedor.

9.4. A atualização dos mecanismos de detecção e bloqueio de códigos maliciosos deve ser verificada pela Área de TI do MEC junto aos fabricantes dos mecanismos.

9.5. A Área de TI do MEC deve homologar a atualização para a implementação na rede interna do MEC.

9.6. Os mecanismos de detecção e bloqueio a códigos maliciosos devem ser configurados de maneira que não permitam ao usuário desativar ou interromper seu funcionamento.

9.6.1. Caso seja identificado o não funcionamento do mecanismo, a Área de TI do MEC deve tomar as providências imediatas para restabelecer seu funcionamento.

9.7. Os mecanismos de detecção e bloqueio a códigos maliciosos devem ser configurados de maneira e efetuar varredura nas mídias removíveis quando inseridas nos recursos computacionais e de comunicação.

9.8. Os mecanismos de detecção e bloqueio a códigos maliciosos devem ser configurados de maneira a executar diariamente uma varredura dos recursos básicos do sistema e semanalmente uma varredura completa das mensagens de correio eletrônico e dos arquivos armazenados nos recursos computacionais e de comunicação do MEC.

9.9. Os mecanismos de detecção e bloqueio a códigos maliciosos devem emitir alertas aos agentes públicos da Área de TI do MEC responsáveis pela rede interna do MEC quanto às possíveis contaminações encontradas em arquivos e/ou mensagens de correio eletrônico.

9.10. Os arquivos e mensagens de correio eletrônico contaminados com códigos maliciosos devem ser enviados à quarentena, de maneira a minimizar sua ação e impedir a proliferação na rede interna do MEC.

9.11. Os recursos computacionais e de comunicação devem ter suas configurações de operação e segurança padronizadas pela a Área de TI do MEC de maneira que não permitam ao usuário efetuar alterações, a fim de evitar as ameaças de códigos maliciosos.

9.12. Os mecanismos de detecção e bloqueio a códigos maliciosos não homologados/autorizados pela Área de TI do MEC, se encontrados nos recursos computacionais e de comunicação de propriedade do MEC, devem ser removidos imediatamente pela Área de TI do MEC.

9.13. A ação dos mecanismos de detecção e bloqueio a códigos maliciosos deve ocorrer de maneira transparente para o usuário da rede interna do MEC.

10. DOCUMENTAÇÃO

10.1. Os documentos que descrevem os procedimentos de instalação e configuração dos mecanismos de detecção e bloqueio a códigos maliciosos devem ser elaborados e atualizados pela Área de TI do MEC.

10.2. Os documentos devem ser guardados em local seguro, com acesso controlado e restrito à Área de TI do MEC.

10.3. Quando do descarte dos documentos, deve ser realizado de forma a não permitir sua recuperação total ou parcial.

11. IMPLEMENTAÇÃO DE REGRAS

11.1. A operacionalização das regras aqui descritas será tratada em documentos internos desenvolvidos pela Área de TI do MEC.

12. CONDIÇÕES OBRIGATÓRIAS DE ATUALIZAÇÃO DO DOCUMENTO

12.1. Surgimento ou alteração de leis e/ou regulamentações vigentes.
12.2. Mudança estratégica da instituição.
12.3. Mudanças de tecnologia na instituição.

13. PRAZO DE REVISÃO

13.1. Esta norma deve ser revista em intervalos planejados, pelo menos anualmente ou em caso de ocorrência de alguma das condições obrigatórias de atualização do documento.

14. RESPONSÁVEL PELA ATUALIZAÇÃO

14.1. Área de TI do MEC.

15. VIGÊNCIA

15.1. Esta norma entra em vigor a partir da data de sua publicação.