ANEXO IV

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

ÍNDICE

1. DESCRIÇÃO

1.1. Esta norma trata dos requisitos de segurança da informação que devem ser definidos nos processos de aquisição, desenvolvimento e manutenção de sistemas de informação.

2. PÚBLICO ALVO

2.1. Esta norma destina-se aos responsáveis da Área de TI do MEC pelo processo de aquisição, desenvolvimento e manutenção dos sistemas de informação do Ministério da Educação - MEC.

3. OBJETIVO

3.1. Definir as regras de inclusão de segurança na aquisição, desenvolvimento e manutenção de sistemas de informação.

4. ESCOPO

4.1. Todos os *softwares* desenvolvidos internamente, custodiados, adotados ou adquiridos pelo MEC.

5. NÃO ESCOPO

5.1. *Softwares* das entidades vinculadas ao MEC.

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 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. Consultar conceitos e definições dos termos técnicos utilizados neste documento no “Dicionário de referência da Política de Segurança da Informação e Comunicações”.

8. REGRAS GERAIS

8.1 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.

8.2 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.

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

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

9. REQUISITOS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

9.1 Para efeitos desta norma, os requisitos de segurança devem ser identificados e acordados previamente junto ao desenvolvimento/implementação de sistemas.

9.2 Os requisitos de segurança devem ser considerados na aquisição de novos sistemas e em todas as fases de criação: definição, projeto, desenvolvimento, implantação e manutenção.

10. SEGURANÇA DOS ARQUIVOS DE SISTEMA

10.1 Devem ser criados e implementados procedimentos para instalação dos sistemas desenvolvidos.

10.2 Os dados utilizados em ambientes de desenvolvimento, teste e homologação devem ser diferenciados dos utilizados em ambiente de produção.

10.3 Os dados utilizados no ambiente de homologação devem conter uma amostra proveniente de bases de dados extraídas do ambiente de produção.

10.4 Os dados de produção, excetuando-se o banco de dados corporativo, não devem ser copiados para os ambientes de desenvolvimento e teste.

10.5 O acesso ao código-fonte dos sistemas deve ser controlado e previamente autorizado pela Área de TI do MEC.

10.6 Deve ser controlado o versionamento entre os ambientes de homologação, teste, desenvolvimento e produção das estruturas e dicionários de dados.

11. SEGURANÇA EM PROCESSOS DE DESENVOLVIMENTO E DE SUPORTE

11.1 Devem ser implementados controles de versão para garantir a gestão dos códigos-fonte.

11.2 Devem ser realizados procedimentos de verificação de funcionamento na infraestrutura de desenvolvimento após atualizações ou substituições de sistemas.

11.3 Análises de riscos devem ser realizadas durante as fases de teste e homologação dos sistemas, a fim de detectar falhas que possam vir a comprometer os princípios da confidencialidade, integridade e disponibilidade das informações do MEC.

11.4 Devem ser supervisionados pela Área de TI do MEC, desde o processo de planejamento até a implementação, os sistemas que venham a ser desenvolvidos por terceiros.

11.4.1. Quando da implantação de sistemas desenvolvidos por entidades e/ou instituições ligadas ao MEC, a Área de TI do MEC deve testar e homologar os sistemas antes de disponibilizá-los em ambiente de produção.

12. PROCESSAMENTO CORRETO DE APLICAÇÕES

12.1 Os dados de entrada de aplicações devem ser validados a fim de garantir que são corretos e apropriados.

12.2 Deve ser realizada nas aplicações a verificação de validação com o intuito de detectar informações corrompidas por erros ou ações deliberadas.

12.3 Devem ser incorporados controles apropriados em projetos de aplicações, a fim de assegurar o processamento correto.

12.3.1. Devem ser incluídos nos controles, os dados de entrada, processamento interno e de saída.

12.4 Com base nos requisitos de segurança e análise/avaliação de riscos, devem ser implementados controles adicionais para sistemas que processam informações sensíveis, valiosas, críticas ou que nessas exerçam algum impacto.

13. CONTROLES CRIPTOGRÁFICOS

13.1 Devem ser elaboradas e implementadas normas e procedimentos para o uso de controles criptográficos a fim de maximizar os benefícios e reduzir os riscos do uso de técnicas criptográficas para evitar o uso incorreto ou inapropriado.

13.2 Devem ser armazenadas nos servidores, com elevado nível de segurança, as chaves utilizadas nas soluções de criptografia.

14. GESTÃO DE VULNERABILIDADES TÉCNICAS

14.1 A gestão de vulnerabilidades deve ser implementada de forma efetiva, sistemática e repetível com medições de confirmação de sua efetividade.

14.2 As informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas para avaliação da exposição do MEC a estas vulnerabilidades e direcionamento para adoção das medidas que devem ser tomadas para lidar com os riscos associados.

15. IMPLEMENTAÇÃO DE REGRAS

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

16. CONDIÇÕES OBRIGATÓRIAS DE ATUALIZAÇÃO DO DOCUMENTO

16.1 Surgimento ou alteração de leis e/ou regulamentações vigentes.
16.2 Mudança estratégica da instituição.
16.3 Mudanças de tecnologia na instituição.

17. PRAZO DE REVISÃO

17.1 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.

18. RESPONSÁVEL PELA ATUALIZAÇÃO

18.1 Área de TI do MEC.

19. VIGÊNCIA

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