ANEXO VI

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA SISTEMA OPERACIONAL E APLICAÇÕES

ÍNDICE

1. DESCRIÇÃO

1.1. Entende-se que sistemas operacionais são *softwares* que tem como função servir de interface entre os recursos computacionais e o usuário e que aplicações são *softwares* desenvolvidos ou adquiridos pelo Ministério da Educação - MEC para atendimento de uma necessidade específica.

1.2. Esta norma estabelece os critérios seguros para instalação, configuração, controle de acesso e auditoria aos sistemas operacionais e aplicações de propriedade do MEC.

2. PÚBLICO ALVO

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

3. OBJETIVO

3.1. Definir requisitos de segurança para instalação, configuração e administração dos sistemas operacionais e aplicações da rede interna do MEC.

4. ESCOPO

4.1. Instalação, configuração, controle de acesso e auditoria dos sistemas operacionais de propriedade do MEC.
4.2. Instalação, configuração, controle de acesso e auditoria de aplicações desenvolvidas e adquiridas pelo MEC.

5. NÃO ESCOPO

5.1. Aquisição de sistemas operacionais.
5.2. Aquisição e desenvolvimento de aplicações.
5.3. Sistemas operacionais e aplicações das entidades vinculadas.

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 implementação de controles de acesso relativos à segurança da informação e comunicação.

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 Área de TI do MEC deve garantir que os sistemas operacionais e aplicações utilizadas no MEC estejam devidamente licenciados, respeitando a legislação de direitos autorais e os contratos dos fornecedores.

8.2. 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.

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

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

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

9. INSTALAÇÃO, CONFIGURAÇÃO E MANUTENÇÃO

9.1. A instalação, configuração e manutenção dos sistemas operacionais assim como aplicações dos recursos computacionais e de comunicações de propriedade do MEC devem ser realizadas ou acompanhadas pela da Área de TI do MEC.

9.2. Os recursos computacionais e de comunicações utilizados pelos usuários que não fazem parte da Área de TI do MEC devem possuir apenas um sistema operacional instalado.

9.2.1. Caso haja necessidade de utilização de outro sistema operacional, a Área de TI do MEC deve avaliar.

9.3. A Área de TI do MEC deve documentar todos os procedimentos de instalação e configuração dos sistemas operacionais e aplicações de propriedade do MEC.

9.4. A Área de TI do MEC deve utilizar as orientações fornecidas pelos fabricantes dos sistemas operacionais e aplicações quando não houver documentações próprias.

9.5. Os recursos computacionais e de comunicações de propriedade do MEC devem ter seus sistemas operacionais e aplicações atualizados de acordo com as atualizações disponibilizadas pelos fabricantes.

9.5.1. A instalação das atualizações deve ocorrer somente após a Área de TI do MEC homologar.

9.6. Quando das atualizações de sistemas operacionais devem ser observadas as seguintes precauções:

9.6.1. As imagens de instalação dos sistemas operacionais devem ser atualizadas bimestralmente.

9.6.2. Antes de qualquer atualização ser realizada na partição do sistema operacional dos servidores de rede deve ser realizada cópia de segurança.

9.7. A Área de TI do MEC deve desabilitar ou desinstalar dos sistemas operacionais e das aplicações os serviços e protocolos desnecessários para o funcionamento dos recursos computacionais e de comunicações do MEC.

9.8. A utilização da conta com perfil convidado e o *login* automático do sistema operacional deve ser desabilitado.

9.9. Os sistemas operacionais e aplicações devem ser configurados para manterem a sincronização de data e hora de acordo com o servidor de rede responsável por este serviço.

9.10. Os sistemas operacionais dos servidores de rede devem ser configurados para:

9.10.1. Emitir um alerta, nos casos de ocorrência de erro fatal.

9.10.2. Não reiniciar automaticamente após ocorrência de erro fatal.

9.11. As falhas de autenticação nos sistemas operacionais e aplicações devem ser registradas indicando o número de tentativas realizadas.

9.12. A Área de TI do MEC deve elaborar uma documentação que descreva as rotinas de recuperação das contas e senhas de acesso do sistema operacional e aplicações, para o caso de sua perda.

9.13. Os sistemas operacionais e aplicações devem ser configurados para liberarem o acesso mediante a utilização de um mecanismo de autenticação de segurança, conforme descrito na norma de controle de acesso a rede.

9.14. Devem ser criados perfis de acesso nos sistemas operacionais e nas aplicações conforme descrito na norma de controle de acesso a rede.

9.15. A recuperação de sistemas operacionais e aplicações bem como a realização de cópias de segurança devem seguir as orientações da norma de cópias de segurança.

10. AUDITORIA E MONITORAMENTO

10.1. Os sistemas operacionais e aplicações devem estar com a funcionalidade de auditoria habilitada, quando possuírem essa funcionalidade.

10.2. A Área de TI do MEC deve definir um tamanho máximo para arquivos de registros de eventos (*logs*) dos sistemas operacionais e aplicações.

10.3. O MEC deve informar aos usuários que os sistemas operacionais e aplicações instaladas em seus recursos computacionais e de comunicações estão suscetíveis a auditoria a qualquer momento, quando constatado quebra de segurança.

10.4. A Área de TI do MEC deve armazenar em local centralizado e protegido contra acessos indevidos os registros de auditoria gerados pelos sistemas operacionais e aplicações por um período de tempo pré-determinado.

10.5. Os registros de auditoria, logs, gerados pelos sistemas operacionais e aplicações devem ser auditados periodicamente.

10.6. A Área de TI do MEC deve configurar se possível, os sistemas operacionais e aplicações para emitir alertas de problemas de funcionamento ou quebras das regras de segurança.

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.