ANEXO II

NORMA DE INFRAESTRUTURA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ÍNDICE

1. DESCRIÇÃO

1.1. Esta norma trata dos requisitos de segurança quanto à implantação de uma infraestrutura de segurança da informação e comunicações.

2. PÚBLICO ALVO

2.1. Esta norma aplica-se aos agentes públicos da área de TI do MEC.

3. OBJETIVO

3.1. Promover a gestão corporativa da segurança da informação por meio de uma infraestrutura visando garantir a manutenção das ações de segurança dentro do MEC.

4. ESCOPO

4.1. Estrutura interna do MEC.

5. NÃO ESCOPO

5.1. Estrutura das entidades vinculadas ao MEC.

6. DOCUMENTO 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° 7845, 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. Biblioteca *ITIL* (*Information Technology Infrastructure Library*) V3.

6.9. Norma Técnica ABNT NBR ISO/IEC 31000:2009, Gestão de riscos - Princípios e diretrizes.

6.10. Norma Técnica ABNT NBR ISO/IEC 27005:2008, Tecnologia da informação – Técnicas de segurança - Gestão de riscos de segurança da informação.

6.11. 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. Para efeitos dessa norma, o MEC deve:

8.1.1. Atribuir as regras para criação e manutenção de uma infraestrutura de segurança da informação;

8.1.2. Definir as funções da área de segurança;

8.1.3. Coordenar e analisar criticamente o processo de implementação da segurança da informação na instituição.

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. COMPROMETIMENTO DA ALTA GESTÃO COM A SEGURANÇA DA INFORMAÇÃO

9.1. O MEC deve apoiar ativamente a segurança da informação dentro da instituição, por meio de um claro direcionamento, definindo de forma explícita as atribuições dos envolvidos e tendo conhecimento das suas responsabilidades pela segurança da informação.

9.2. Para implementação da infraestrutura de segurança da informação, o MEC deve:

9.2.1. Assegurar que as metas de segurança da informação estejam identificadas e integradas nos processos relevantes, e atendam aos requisitos da instituição.

9.2.2. Analisar criticamente a eficácia da implementação da Política de Segurança da Informação e Comunicações do MEC.

9.2.3. Fornecer os recursos necessários para as ações de segurança.

9.2.4. Aprovar as atribuições de tarefas e responsabilidades específicas para a segurança da informação em todo o MEC.

9.2.5. Promover planos e programas para manter a conscientização sobre segurança da informação em todo o MEC.

9.3. Quando necessário, o MEC deve avaliar a necessidade de uma consultoria interna ou externa em segurança da informação.

10. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

10.1. As atividades de segurança da informação devem ser coordenadas por servidor público do MEC com funções e papéis relevantes, de acordo com a metodologia definida.

10.2. A gestão de segurança da informação deve:

10.2.1. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política de Segurança da Informação e Comunicações do MEC.

10.2.2. Acompanhar a correção das não-conformidades de segurança da informação identificadas na análise de risco.

10.2.3. Avaliar e coordenar a implementação de controles de segurança da informação no MEC.

10.2.4. Fornecer suporte ao comitê de segurança da informação, sugerindo indicadores e metas, notificando sobre as atividades de segurança desenvolvidas e seus resultados.

11. ATRIBUIÇÃO DE RESPONSABILIDADES PARA SEGURANÇA DA INFORMAÇÃO

11.1. Todas as responsabilidades relacionadas à segurança da informação devem estar claramente definidas pelo MEC.

11.2. A atribuição de responsabilidades pela segurança da informação deve ser feita em conformidade com a POSIC do MEC.

11.3. Pessoas com responsabilidades definidas podem delegar as tarefas relacionadas à segurança para terceiros. Todavia, continuam responsáveis e devem avaliar se as tarefas estão sendo corretamente executadas.

11.4. As áreas pelas quais as pessoas são responsáveis devem estar definidas observando os seguintes itens:

11.4.1. Os ativos e os processos associados à segurança da informação do MEC devem ser identificados e definidos.

11.4.2. O responsável por cada ativo ou processo de segurança da informação deverá ter atribuições definidas e os detalhes dessa responsabilidade deverão ser documentados.

12. PROCESSO DE AUTORIZAÇÃO PARA RECURSOS COMPUTACIONAIS E DE COMUNICAÇÕES

12.1. Um processo de autorização para uso dos recursos computacionais e de comunicações do MEC deve ser definido e implementado.

12.2. A instalação de novos recursos computacionais e de comunicação deve ser registrada indicando seus propósitos e uso.

12.3. A utilização de recursos computacionais e de comunicações no ambiente do MEC somente deve ser realizada mediante prévia autorização.

13. ACORDOS DE CONFIDENCIALIDADE

13.1. Acordos de confidencialidade ou de não divulgação das informações relacionadas ao MEC devem ser assinados por empresas prestadoras de serviço ou agentes públicos, após conhecimento e compreensão da Política de Segurança da Informação e Comunicações do MEC e normas correlatas.

13.2. Os acordos de confidencialidade e de não divulgação devem considerar os requisitos para proteger as informações, observando o ponto de vista legal.

13.2.1. Para identificação dos requisitos, devem ser considerados, minimamente os seguintes itens:

13.2.1.1. Uma definição da informação a ser protegida de acordo com a Norma de Segurança da Informação e Comunicações para Classificação da Informação.

13.2.1.2. O tempo de duração esperado de um acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente.

13.2.1.3. Ações requeridas quando um acordo está encerrado.

13.2.1.4. Responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação.

13.2.1.5. O proprietário da informação.

13.2.1.6. Termos para a informação ser retornada ou descartada quando da cessão do acordo.

13.2.1.7. Ações esperadas a serem tomadas no caso de violação do acordo de confidencialidade.

13.3. Os acordos de confidencialidade ou de não divulgação das informações do MEC devem estar em conformidade com todas as leis e regulamentações aplicáveis na jurisdição para a qual ele se aplica.

13.4. Os requisitos para os acordos de confidencialidade ou de não divulgação das informações do MEC devem ser analisados criticamente de forma periódica e quando ocorrerem mudanças que possam refletir nestes requisitos.

14. IMPLEMENTAÇÃO DE REGRAS

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

15. CONDIÇÕES OBRIGATÓRIAS DE ATUALIZAÇÃO DO DOCUMENTO

15.1. Surgimento ou alteração de leis e/ou regulamentações vigentes.
15.2. Mudança estratégica da instituição.
15.3. Mudanças de tecnologia na instituição.

16. PRAZO DE REVISÃO

16.1. 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.

17. RESPONSÁVEL PELA ATUALIZAÇÃO

17.1. Área de TI do MEC.

18. VIGÊNCIA

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