ANEXO III

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA ASPECTOS DA GESTÃO DE CONTINUIDADE DO NEGÓCIO

ÍNDICE

1. DESCRIÇÃO

1.1. Entende-se por gestão de continuidade do negócio o processo de identificação, avaliação, prevenção e recuperação de falhas e desastres que possam gerar interrupções nas atividades essenciais da Organização.

1.2. Este documento apresenta os requisitos de segurança da informação necessários para a gestão da continuidade dos negócios do MEC.

2. PÚBLICO ALVO

2.1. Responsáveis pelos processos e recursos do MEC considerados essenciais para continuidade do negócio a serem definidos, caso a caso, considerando a atuação da DTI nos processos.

3. OBJETIVO

3.1. Esta norma visa mitigar a interrupção das atividades do negócio e proteger os processos e recursos, contra efeitos de falhas ou desastres significativos.

4. ESCOPO

4.1. Processos e recursos do MEC considerados essenciais para continuidade dos negócios.

5. NÃO ESCOPO

5.1. Não se aplica.

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. Norma Técnica ABNT NBR ISO/IEC 27005:2011, Tecnologia da informação – Técnicas de segurança – Gestão de risco de segurança da informação.

6.4. Norma Técnica ABNT NBR ISO/IEC 31000:2009, Gestão de risco – Princípios e diretrizes.

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

6.6. 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.

6.7. 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.

6.8. 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.

6.9. 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.

6.10. 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 efeito desta norma considera-se que o processo de gestão de continuidade do negócio seja implementado para minimizar os impactos sobre os processos do MEC e recuperar os recursos necessários para execução das operações essenciais, a um nível aceitável, por meio da combinação de ações de prevenção e recuperação, dentro do prazo requerido conforme definição no Plano de Gestão da Continuidade do Negócio do MEC.

8.2. Devem ser realizadas análises de impacto no negócio para averiguar as consequências de desastres, falhas de segurança, perda de serviços e disponibilidade.

8.3. 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.

8.4. 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.

8.5. Ao agente público descumpridor dessa norma serão aplicadas as sanções previstas na legislação em vigor.

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

9. PROCESSO DE GESTÃO DA CONTINUIDADE DE NEGÓCIO

9.1. A gestão da continuidade do negócio deve estar incorporada aos processos e a estrutura organizacional do MEC.

9.2. Para efeitos dessa norma, entende-se por plano de continuidade do negócio (PCN), o desenvolvimento preventivo de um conjunto de estratégias e planos de ação visando garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento.

9.3. Os processos de negócios do MEC devem ter PCNs definidos, documentados, auditados e testados adequadamente até que estejam comprovadas suas eficiências.

9.3.1. Os PCNs referidos devem assegurar a manutenção ou a recuperação da operacionalidade dos processos de negócios a que se referem, considerando os requisitos para cada processo.

9.4. Deve ser considerada a contratação de um seguro, como parte integrante do processo de continuidade do negócio.

9.5. Todos os recursos envolvidos em processos de negócio classificados como essenciais devem ser identificados nos PCNs.

9.6. O MEC deve possuir instalações e recursos em ambiente de contingência contendo padrões de segurança adotado nas instalações e recursos do ambiente principal conforme definidos no PCN.

10. CONTINUIDADE DE NEGÓCIOS E AVALIAÇÃO DE RISCOS

10.1. Deve ser realizada análise de riscos para avaliar a probabilidade de ocorrência, os níveis de impacto e as consequências dos eventos identificados para a segurança da informação dos processos de negócio.

10.2. Os responsáveis pelos processos de negócio devem participar da análise de riscos e validação dos relatórios apresentados. Se necessário, o responsável pode solicitar apoio técnico para a melhor compreensão e avaliação dos resultados da análise.

10.2.1. Considerando o resultado da análise/avaliação de riscos, deve ser elaborada uma estratégia para definir a abordagem da continuidade dos negócios.

10.2.2. A estratégia deve ser validada pelos responsáveis pelos processos de negócio.

11. DESENVOLVIMENTO E IMPLEMENTAÇÃO DE PLANOS DE CONTINUIDADE RELATIVOS À SEGURANÇA DA INFORMAÇÃO

11.1. Os PCNs devem tratar as vulnerabilidades do MEC, que possam conter informações sigilosas e que necessitem de proteção adequada.

11.2. O desenvolvimento de um PCN deve ser realizado, preferencialmente, por uma equipe multidisciplinar.

11.3. As cópias de segurança dos PCNs e os componentes necessários para a sua execução devem ser guardados em um ambiente de contingência, de forma que não sejam afetados por qualquer dano ou desastre que ocorra no ambiente principal.

11.4. O gestor das cópias de segurança dos PCNs deve garantir a atualização dos planos quando houver alterações no ambiente principal.

11.5. Os responsáveis pelas áreas ou processos e as equipes encarregadas de atuar em um PCN devem:

11.5.1. Ter pleno conhecimento do seu conteúdo e responsabilidades;

11.5.2. Receber treinamento durante os testes de validação do plano;

11.5.3. Saber como proceder em caso de falha em qualquer dos recursos essenciais que suportem os processos de negócios envolvidos.

12. ESTRUTURA DO PLANO DE CONTINUIDADE DO NEGÓCIO

12.1. Cada PCN deve:

12.1.1. Descrever o escopo para a gestão da continuidade;

12.1.2. Definir e especificar um plano de escalonamento e as suas condições para ativação;

12.1.3. Definir as responsabilidades individuais para execução de cada uma das atividades do plano.

12.1.4. Ter um gestor específico.

12.1.5. Conter os pré-requisitos para sua eficácia.

12.2. Os procedimentos de emergência relacionados aos PCNs devem ser ajustados sempre que novos requisitos forem identificados.

13. TESTES, MANUTENÇÃO E REAVALIAÇÃO DOS PLANOS DE CONTINUIDADE DO NEGÓCIO

13.1. As atividades e os componentes que fazem parte do PCN devem ser testados individualmente, de forma que seja possível identificar falhas que venham a comprometer qualquer parte do processo de continuidade.

13.1.1. Ao final dos testes de cada atividade, o plano deve ser testado em sua totalidade.

13.2. Os testes devem ser planejados levando-se em consideração as menores indisponibilidades e impactos possíveis nos processos de negócio. Tais definições devem ser observadas para fins de aprovação.

13.3. O resultado dos testes deve ser documentado e enviado para o(s) responsável(eis) pelo(s) processo(s) de negócio(s), que deve(m), formalmente, tomar ciência e solicitar as providências cabíveis quando necessárias.

13.4. Os PCNs devem ser revisados e atualizados sempre que houver alterações de:

13.4.1. Ambiente físico e/ou tecnológico;

13.4.2. Pessoas envolvidas, endereços e telefones;

13.4.3. Legislação;

13.4.4. Riscos (operacional e financeiro);

13.4.5. Processo de negócio.

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.