ANEXO V

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA ÁREAS SEGURAS

ÍNDICE

1. DESCRIÇÃO

1.1. Esta norma trata dos requisitos de segurança que norteiam os controles físicos no ambiente de processamento de dados e áreas seguras do Ministério da Educação - MEC.

2. PÚBLICO ALVO

2.1. O presente documento destina-se a Área de TI do MEC e área responsável pelos controles físicos das instalações.

3. OBJETIVO

3.1. Estabelecer regras de segurança quanto à proteção dos ambientes de processamento de dados e áreas seguras no MEC, visando à prevenção de acessos físicos não autorizados, danos e interferências nos processos de trabalho do órgão.

4. ESCOPO

4.1. Ambiente de processamento de dados do MEC.
4.2. Áreas seguras do MEC.

5. NÃO ESCOPO

5.1. Demais áreas do 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° 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 07/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. Consideram-se “ambiente de processamento” as instalações físicas do MEC onde se encontram instalados e/ou armazenados:

8.1.1. Os servidores de rede e os recursos de computação de rede (roteadores, *switches*, *hubs*, e modem), sob responsabilidade da Área de TI do MEC.

8.1.2. Cabeamento de telefonia, cabeamento lógico e elétrico, sob responsabilidade da Área de Logística.

8.1.3. As mídias com os *backups* das informações custodiadas ou de propriedade do MEC;

8.1.4. Os ambientes onde se encontram instalados os geradores de energia elétrica;

8.1.5. Os locais onde se encontram instalados os tanques de combustível dos geradores de energia elétrica;

8.1.6. Os *no-breaks*.

8.2. Os ambientes de processamento devem possuir mecanismos de segurança que salvaguardem a integridade física e lógica dos servidores de rede, recursos de computação e comunicação e demais recursos instalados ou armazenados nesses ambientes.

8.3. Os acessos físicos aos ambientes de processamento e áreas seguras devem ser monitorados, controlados e registrados.

8.4. Materiais combustíveis, tóxicos, ou desnecessários não devem ser armazenados dentro ou próximos dos ambientes de processamento, exceto nos casos dos tanques de combustível que alimentam os geradores de energia.

8.5. As permissões de acesso físico aos ambientes de processamento e áreas seguras devem ser trimestralmente revistas pela Área de TI do MEC e demais áreas responsáveis.

8.6. 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.

8.7. 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.

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

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

9. PERÍMETRO DE SEGURANÇA

9.1. O ambiente de processamento deve ser, quando possível, instalado em local onde o fluxo de pessoas seja baixo, possibilitando facilitar a identificação de acesso não autorizado.

9.2. O ambiente de processamento e áreas seguras deve conter um local de recepção ou outro meio de controle de acesso físico como mecanismo de registro e prevenção de acessos não autorizados.

9.3. Restrições de acesso, indicando que somente pessoas autorizadas podem entrar, devem ser colocadas nos pontos de entrada e saída do ambiente de processamento e áreas seguras.

9.4. Os pontos de acesso físico do ambiente de processamento e áreas seguras devem permanecer trancados, bem como possuírem proteção compatível com seu grau de criticidade para o MEC.

9.4.1. Deve ser evitada a utilização de informações visuais que identifiquem o tipo de atividade realizada ou informação armazenada nesse local.

9.5. A infraestrutura do ambiente de processamento e áreas seguras deve respeitar as normas específicas para esse ambiente, as quais dizem respeito a assuntos, tais como climatização, rede elétrica e lógica, tubulação de gás e água, e edificação.

9.6. A infraestrutura do ambiente de processamento deve ser livre dos sistemas de tubulação de drenagem pluvial, tubulação de esgoto sanitário e tubulação pressurizada de gases, exceto para a finalidade de combate a incêndio.

9.7. O ambiente de processamento e áreas seguras que possuam pouca movimentação de pessoal deve possuir sistema de alarme de presença permanentemente ativo, bem como permanecer trancados.

9.8. O manuseio de alimentos, bebidas e cigarros, bem como o seu consumo no ambiente de processamento é proibido.

9.9. Rondas de segurança devem ser realizadas em regime de 24 x 7, no perímetro do ambiente de processamento e áreas seguras.

9.10. O ambiente de processamento deve possuir sistema de circuito fechado de TV (CFTV) de forma a possibilitar seu monitoramento.

9.10.1. As câmeras de monitoração devem ser instaladas nas partes internas e externas do ambientes de processamento.

9.10.2. As câmeras de monitoração instaladas no interior do ambiente de processamento devem ser posicionadas de forma que evitem a captura da conta de acesso e senhas utilizadas no local.

9.10.3. As imagens captadas pelo CFTV devem ser gravadas de forma contínua, visando dirimir dúvidas futuras nas investigações de suspeitas ou de incidentes de segurança.

9.10.4. Os arquivos de imagens devem ser guardados por um prazo de 01 (um) ano e tratados com os mesmos critérios das mídias de cópia de segurança.

9.10.5. O CFTV deve ser conectado a um sistema de alarme capaz de detectar e alertar eventuais indisponibilidades no seu funcionamento.

9.11. A coleta de lixo e limpeza do ambiente de processamento e áreas seguras deve ser realizada por pessoal com capacitação específica quanto aos cuidados nesse ambiente, devendo ser autorizada e acompanhada por um responsável indicado pela área responsável.

10. PROTEÇÃO CONTRA INCÊNDIO

10.1. O ambiente de processamento deve conter sistema de detecção e combate a incêndio compatível com as características dos recursos e materiais armazenados nesse ambiente, quando aplicável e conforme resultado da análise de riscos.

10.1.1. O ambiente de processamento onde estão localizados os servidores de rede e recursos de computação e comunicação, não deve conter sistemas de válvulas automáticas de pressão de água (*sprinklers*).

10.2. O sistema de alarme de incêndio deve possuir som distinto em tonalidade e altura de todos os outros dispositivos de alerta existentes no MEC.

10.3. No ambiente de processamento e áreas seguras onde não haja sistema automático de combate a incêndio deve conter instalado extintores de incêndio compatível com o tipo de material ou recurso nele armazenado.

10.3.1. Os extintores de incêndio devem ser posicionados em locais de fácil acesso, fácil visualização e onde haja menos probabilidade do fogo bloquear acesso aos mesmos.

10.3.2. Nas áreas seguras devem existir agentes públicos treinados no manuseio dos sistemas de detecção e combate a incêndios aptos a identificar e interpretar os tipos de alarmes existentes. Os produtos utilizados no sistema de detecção e combate a incêndio devem ser o mais inofensivos ao meio-ambiente e às pessoas presentes no local.

10.4. Luzes de emergência devem ser dispostas nos pontos principais do ambiente de processamento, tais como centrais de comunicação, quadros de energia e de cabeamento lógico.

10.5. Os sistemas de combate a incêndio devem ser periodicamente testados de forma a aferir seu pleno funcionamento.

10.6. O MEC deve possuir equipes de brigada de incêndio, a qual deve promover semestralmente atividades de conscientização e capacitação dos Agentes Públicos quanto às ações e serem adotadas em situações de emergência, bem como montar e divulgar as rotas de fuga.

11. PROTEÇÃO DE ACESSO FÍSICO

11.1. A Área de TI do MEC e a Área de Logística são responsáveis pelo controle do acesso físico.

11.1.1. Somente devem ter acesso ao ambiente de processamento os Agentes Públicos imprescindíveis para a realização dos trabalhos rotineiros ou de manutenção desse ambiente.

11.1.2. Os Agentes Públicos que trabalham no ambiente de processamento devem utilizar uma identificação física diferenciada dos demais.

11.1.2.1. Essa identificação física (crachá, cartão de controle de acesso) deve ser usada na parte frontal, de forma a estar sempre visível.

11.2. O acesso ao ambiente de processamento e áreas seguras em horário fora do expediente de trabalho, ou seja, trabalho noturno, finais de semana, feriados ou recessos, somente devem ser permitidos mediante autorização prévia da área responsável.

11.3. O visitante ou Agente Público não lotado no ambiente de processamento ou áreas seguras que necessite entrar no mesmo deve ser identificado e autorizado pela área responsável.

11.3.1. Essas pessoas devem ser acompanhadas por um Agente Público indicado pela área responsável, durante toda a sua permanência no ambiente de processamento ou áreas seguras.

11.3.2. Caso seja identificada alguma pessoa no ambiente de processamento ou áreas seguras sem a identificação física, o Agente Público que observou tal fato deve informar imediatamente à área responsável.

11.4. A realização de manutenções preventivas ou corretivas no ambiente de processamento ou áreas seguras devem ser previamente informadas e autorizadas pela área responsável.

12. IMPLEMENTAÇÃO DE REGRAS

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

13. CONDIÇÕES OBRIGATÓRIAS DE ATUALIZAÇÃO DO DOCUMENTO

13.1. Surgimento ou alteração de leis e/ou regulamentações vigentes.
13.2. Mudança estratégica da instituição.
13.3. Mudanças de tecnologia na instituição.

14. PRAZO DE REVISÃO

14.1. 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.

15. RESPONSÁVEL PELA ATUALIZAÇÃO

15.1. Área de TI do MEC.

16. VIGÊNCIA

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