MINISTÉRIO DA EDUCAÇÃO
SECRETARIA EXECUTIVA
Subsecretaria de Assuntos Administrativos

M **E** **C**

EDUCAÇÃO COM QUALIDADE CONTRIBUI PARA UMA SOCIEDADE MELHOR

BOLETIM DE SERVIÇO
Nº 33 /2013
SUPLEMENTO

EDITADO, COMPOSTO E IMPRESSO PELA
Coordenação de Documentação e Gestão de Processos
Coordenação Geral de Gestão Administrativa

S U M Á R I O

EXPEDIENTE

Boletim de Serviço Volume 23 nº 33
De 27.08.2013

SUPLEMENTO

Endereço: Av. N2 – Anexo II – 2º Andar Sala nº 209
Telefones: (061) 2022-7403 e 2022-7404
CEP: 70.047-900 – Brasília – DF

Editado e Composto pela
Coordenação de Documentação e Gestão de Processos
Coordenação Geral de Gestão Administrativa

GABINETE DO MINISTRO

RESOLUÇÃO Nº 03 , DE 27 DE AGOSTO DE 2013

Publica conjunto de 9 (nove) normas deliberadas pelo Comitê de Segurança da Informação e Comunicações do Ministério da Educação, instituído pela Portaria MEC nº 942, de 22 de junho de 2012.

O PRESIDENTE DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO MINISTÉRIO DA EDUCAÇÃO, no uso das atribuições que lhe conferem a Portaria MEC nº 942, de 22 de junho de 2012,

RESOLVE:

Art. 1º Publicar as seguintes normas aprovadas em reuniões do Comitê de Segurança da Informação e Comunicações do Ministério da Educação – CSIC-MEC:

I - Norma de Segurança da Informação e Comunicações de Responsabilidade do Usuário (ANEXO I);

II - Norma de Infraestrutura de Segurança da Informação e Comunicações (ANEXO II);

III - Norma de Segurança da Informação e Comunicações para Aspectos da Gestão de Continuidade do Negocio (ANEXO III);

IV - Norma de Segurança da Informação e Comunicações para Aquisição, Desenvolvimento e Manutenção de Sistemas (ANEXO IV);

V - Norma de Segurança da Informação e Comunicações de Areas Seguras (ANEXO V);

VI - Norma de Segurança da Informação e Comunicações para Sistema Operacional e Aplicações (ANEXO VI);

VII - Norma de Segurança da Informação e Comunicações contra Códigos Maliciosos (ANEXO VII);

VIII - Norma de Segurança da Informação e Comunicações para Controle de Acesso a Rede (ANEXO VIII);

IX - Norma de Segurança da Informação e Comunicações de Controle de Acesso do Usuário (ANEXO IX).

Art. 2º Esta resolução entra em vigor na data de sua publicação.

José Henrique Paim Fernandes

ANEXO I

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
DE RESPONSABILIDADE DO USUÁRIO

ÍNDICE

1. DESCRIÇÃO

1.1. Entende-se que o usuário é responsável pelos recursos computacionais e de comunicações por eles utilizados.

1.2. Esta norma trata dos requisitos de segurança da informação que devem ser seguidos pelos usuários da rede interna do Ministério da Educação - MEC.

2. PUBLICO ALVO

2.1. Este documento se aplica a todos os usuários do MEC.

3. OBJETIVO

3.1. Definir as responsabilidades do usuário sobre o uso dos recursos computacionais e de comunicações, sistemas e aplicações da rede interna do MEC.

4. ESCOPO

4.1. Uso de contas e senhas na rede interna do MEC.
4.2. Uso de recursos computacionais e de comunicação e informações do MEC.
4.3. Manutenção e suporte dos recursos computacionais e de comunicação do MEC.

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. 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. 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. O usuário deve conhecer a Política de Segurança da Informação e Comunicações e as normas correlatas do MEC referentes à sua função, bem como cumprir suas determinações.

8.2. A chefia imediata é responsável por assegurar o cumprimento da Política de Segurança da Informação e Comunicações e suas normas correlatas e deve promover a educação e conscientização sobre segurança das informações.

8.3. O MEC deve instituir uma metodologia de divulgação contínua para a conscientização de todos os usuários quanto a Política de Segurança da Informação e Comunicações e normas correlatas.

8.4. 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.

8.5. 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.

8.6. Ao Agente Público descumpridor dessa norma serão aplicadas as sanções previstas no regimento interno do MEC e na legislação em vigor.

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

9. USO DE CONTAS E SENHAS

9.1. O acesso às informações e aos recursos computacionais e de comunicações do MEC será concedido ao usuário somente após a finalização do processo de autorização para acesso entre a coordenação-geral do usuário, área de gestão de pessoas e a Área de TI do MEC.

9.1.1. Para o acesso de pessoal terceirizado será necessária a autorização da coordenação-geral do usuário e a Área de TI do MEC.

9.2. Ao usuário é concedida apenas uma única conta de acesso aos recursos computacionais e de comunicações do MEC.

9.3. Toda a atividade realizada na rede interna, sistemas, aplicações e nos recursos computacionais e de comunicações do MEC utilizando a identificação do usuário é de sua inteira responsabilidade.

9.4. A conta de acesso aos sistemas, aplicações e recursos computacionais e de comunicações do MEC é pessoal e intransferível responsabilizando o usuário por todos os acessos realizados. As regras de criação e utilização das senhas estão definidas na Norma de Segurança da Informação e Comunicações de Controle de acesso do usuário.

9.5. Os direitos de acesso dos usuários têm perfis definidos de acordo com a sua alocação e função, conforme determinação de sua coordenação-geral.

9.6. O usuário não deve fornecer, compartilhar, ceder ou repassar sua senha de acesso a outras pessoas.

9.7. O usuário deve evitar anotações da senha.

9.8. O Usuário deve modificar sua senha de acesso aos recursos de informática e à rede local periodicamente, conforme descrito na Norma de Segurança da Informação e Comunicações de Controle de Acesso do Usuário.

10. USO DE RECURSOS COMPUTACIONAIS E DE COMUNICAÇÕES E INFORMAÇÕES

10.1. O usuário deve:

10.1.1. Proteger as informações e os recursos computacionais e de comunicações que estão sob sua responsabilidade, protegendo contra atividades não autorizadas.

10.1.2. Utilizar os recursos computacionais e de comunicações prioritariamente para realização das atividades profissionais desempenhadas para o MEC nos limites dos princípios da ética, razoabilidade e legalidade.

10.1.3. Bloquear a sessão do recurso computacional e de comunicações sempre que se ausentarem dele.

10.1.3.1. Em caso de recursos compartilhados por diferentes usuários deve ser efetuado *logoff*, liberando o acesso ao recurso.

10.1.4. Desligar os recursos computacionais e de comunicações utilizados por eles ao final do expediente, seguindo as orientações da Área de TI do MEC.

10.1.5. Armazenar nos servidores de arquivos do MEC as informações pertinentes a instituição, evitando o armazenamento nos recursos locais.

10.1.6. Utilizar somente os meios de comunicações fornecidos pelo MEC para a troca de informações com outras instituições, observando a classificação da informação atribuída a elas.

10.1.7. Tratar de assuntos sensíveis do MEC somente em locais que ofereçam proteção adequada, evitando locais públicos ou sem reserva.

10.1.8. Contribuir ativamente na resolução dos problemas e no processo de aprimoramento da segurança da informação do MEC.

10.1.9. Armazenar os documentos impressos em locais seguros conforme descrição da Norma de Segurança da Informação e Comunicações para Classificação da Informação.

10.2. O usuário não deve:

10.2.1. Consumir alimentos, bebidas e fumo nas proximidades dos recursos computacionais e de comunicações do MEC.

10.2.2. Instalar softwares de sua propriedade ou de terceiro nos recursos computacionais e de comunicações do MEC sem prévia homologação da Área de TI do MEC. As instalações dos *softwares* são definidas pela Área de TI do MEC e qualquer necessidade de instalação deve ser encaminhada a essa área através do sistema de atendimento ao usuário. Caso seja identificado à instalação de *softwares* não homologados, estes serão removidos.

10.2.3. Alterar as configurações dos recursos computacionais e de comunicações utilizados por ele. As configurações seguem um padrão definido pela Área de TI do MEC e qualquer necessidade de alteração deve ser encaminhada a essa área através do sistema de atendimento ao usuário. Caso sejam identificadas alterações não autorizadas, será feita uma nova padronização.

10.2.4. Compartilhar pastas e arquivos diretamente entre seu recurso computacional e/ou de comunicações local e o de outro usuário.

10.2.5. Armazenar nos servidores do MEC arquivos particulares, tais como: música, fotos, vídeos e documentos. Quando encontrados estes serão apagados sem prévia comunicação.

10.2.6. Remover os lacres dos recursos computacionais e de comunicações ou modificar o hardware, sendo essas atribuições exclusivas da área responsável.

10.2.7. Ligar os recursos computacionais custodiados ou de propriedade do MEC em rede elétrica.

10.2.8. Remanejar recursos computacionais tais como *desktops* e impressoras.

11. MANUTENÇÃO E SUPORTE

11.1. O suporte técnico da Área de TI do MEC é o responsável pela manutenção preventiva e corretiva dos recursos computacionais e de comunicações custodiados ou de propriedade do MEC utilizados pelo usuário.

11.2. Quando da ocorrência de falhas nos recursos computacionais e de comunicações custodiados ou de propriedade do MEC o usuário deve solicitar atendimento ao suporte técnico da Área de TI do MEC.

11.3. O atendimento do técnico deve ser acompanhado pelo usuário quando realizado no local ou através de software de acesso remoto, esse último deve ser autorizado pelo usuário. Em caso de indisponibilidade do usuário para acompanhamento, o atendimento deve ser remarcado.

11.4. Caso seja necessária a remoção do recurso para manutenção, o responsável pelo recurso deve conceder autorização ao técnico, por meio de um canal formal, para retirada.

11.5. O usuário deve monitorar a resolução da sua solicitação de atendimento através do sistema do suporte técnico da Área de TI do MEC.

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 e Coordenação-Geral de Recursos Logísticos – CGRL.

16. VIGÊNCIA

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

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.

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.

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.

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.

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.

ANEXO VII

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES CONTRA CÓDIGOS MALICIOSOS

ÍNDICE

1. DESCRIÇÃO

1.1. Entende-se por código malicioso um programa de computador, ou parte de um programa, desenvolvido para danificar, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores. Esses programas podem ainda fazer cópias de si mesmo e auto propagar-se por toda rede. Esta norma estabelece os critérios seguros a serem seguidos pelos agentes públicos pertencentes à Área de TI do MEC para prevenção e proteção de códigos maliciosos em servidores, estações de trabalho e demais recursos computacionais e de comunicação da rede interna do MEC.

2. PÚBLICO ALVO

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

3. OBJETIVO

3.1. Definir requisitos de prevenção e proteção a códigos maliciosos nos recursos computacionais e de comunicação da rede interna do MEC.

4. ESCOPO

4.1. Instalação, configuração e administração de mecanismos de proteção contra códigos maliciosos.

5. NÃO ESCOPO

5.1. Aquisição de *softwares* de proteção contra códigos maliciosos.

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 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. 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 definição e homologação dos softwares a serem instalados nos recursos computacionais e de comunicação de propriedade do MEC são de responsabilidade da Área de TI do MEC.

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

8.3. 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.

8.4. 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.

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

9. GERENCIAMENTO DE PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

9.1. A Área de TI do MEC deve instalar configurar e gerenciar mecanismos de detecção e bloqueio de códigos maliciosos nos recursos computacionais do MEC, tais como: *softwares* de antivírus, *antispyware*, análise de conteúdo *web*, análise de correio eletrônico e *IPS* (*Intrusion Protection System*).

9.2. A Área de TI do MEC deve definir e homologar mecanismos de detecção e bloqueio de códigos maliciosos, considerando pelo menos as seguintes características:

9.2.1. Possuir uma console de administração centralizada com possibilidade de instalação remota;

9.2.2. Permitir atualização automática e programável;

9.2.3. Permitir configuração de perfis de acesso;

9.2.4. Permitir bloqueio de alteração das configurações por meio de senha;

9.2.5. Ter serviço de suporte do fabricante em idioma português;

9.2.6. Ter serviço de atualização do fabricante;

9.2.7. Possuir um mecanismo de varredura em tempo real;

9.2.8. Possuir um mecanismo de controle estatístico e emissão de relatórios.

9.3. Os *softwares* utilizados como mecanismos de detecção e bloqueio de códigos maliciosos devem estar devidamente licenciados e respeitar os direitos autorais e contratuais do fornecedor.

9.4. A atualização dos mecanismos de detecção e bloqueio de códigos maliciosos deve ser verificada pela Área de TI do MEC junto aos fabricantes dos mecanismos.

9.5. A Área de TI do MEC deve homologar a atualização para a implementação na rede interna do MEC.

9.6. Os mecanismos de detecção e bloqueio a códigos maliciosos devem ser configurados de maneira que não permitam ao usuário desativar ou interromper seu funcionamento.

9.6.1. Caso seja identificado o não funcionamento do mecanismo, a Área de TI do MEC deve tomar as providências imediatas para restabelecer seu funcionamento.

9.7. Os mecanismos de detecção e bloqueio a códigos maliciosos devem ser configurados de maneira e efetuar varredura nas mídias removíveis quando inseridas nos recursos computacionais e de comunicação.

9.8. Os mecanismos de detecção e bloqueio a códigos maliciosos devem ser configurados de maneira a executar diariamente uma varredura dos recursos básicos do sistema e semanalmente uma varredura completa das mensagens de correio eletrônico e dos arquivos armazenados nos recursos computacionais e de comunicação do MEC.

9.9. Os mecanismos de detecção e bloqueio a códigos maliciosos devem emitir alertas aos agentes públicos da Área de TI do MEC responsáveis pela rede interna do MEC quanto às possíveis contaminações encontradas em arquivos e/ou mensagens de correio eletrônico.

9.10. Os arquivos e mensagens de correio eletrônico contaminados com códigos maliciosos devem ser enviados à quarentena, de maneira a minimizar sua ação e impedir a proliferação na rede interna do MEC.

9.11. Os recursos computacionais e de comunicação devem ter suas configurações de operação e segurança padronizadas pela a Área de TI do MEC de maneira que não permitam ao usuário efetuar alterações, a fim de evitar as ameaças de códigos maliciosos.

9.12. Os mecanismos de detecção e bloqueio a códigos maliciosos não homologados/autorizados pela Área de TI do MEC, se encontrados nos recursos computacionais e de comunicação de propriedade do MEC, devem ser removidos imediatamente pela Área de TI do MEC.

9.13. A ação dos mecanismos de detecção e bloqueio a códigos maliciosos deve ocorrer de maneira transparente para o usuário da rede interna do MEC.

10. DOCUMENTAÇÃO

10.1. Os documentos que descrevem os procedimentos de instalação e configuração dos mecanismos de detecção e bloqueio a códigos maliciosos devem ser elaborados e atualizados pela Área de TI do MEC.

10.2. Os documentos devem ser guardados em local seguro, com acesso controlado e restrito à Área de TI do MEC.

10.3. Quando do descarte dos documentos, deve ser realizado de forma a não permitir sua recuperação total ou parcial.

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.

ANEXO VIII

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES PARA CONTROLE DE ACESSO À REDE

ÍNDICE

1. DESCRIÇÃO

1.1. Entende-se por controle de acesso à rede o conjunto de atividades, procedimentos e direcionamentos necessários à regulação das permissões ou conjunto de permissões definidas e necessárias às informações custodiadas pela Área de TI do MEC em formato eletrônico.

1.2. Esta norma estabelece os critérios seguros para a implementação de controles de acessos à rede interna do Ministério da Educação - MEC.

2. PÚBLICO ALVO

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

3. OBJETIVO

3.1. Definir requisitos de segurança para proteção dos acessos à rede interna do MEC.

4. ESCOPO

4.1. Controle de acesso à rede interna.
4.2. Controle de acesso remoto à rede interna.

5. NÃO ESCOPO

5.1. Controle de senhas de acesso à rede.
5.2. Controle de usuário da rede interna.

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

6.7. Norma Complementar nº 07/IN01/DSIC/GSIPR, estabelece as diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicação.

6.8. 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.

6.9. 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 desta norma define-se como administrador de rede, o agente público com essa atribuição e que faça parte da Área de TI do MEC.

8.2. O acesso local ou remoto à rede interna do MEC deve ser controlado e monitorado pela Área de TI do MEC.

8.3. A Área de TI do MEC deve implementar mecanismos de segurança para que o usuário com acesso às redes e aos serviços de rede não comprometa a segurança desses serviços.

8.4. O acesso local ou remoto à rede interna do MEC deve ser configurado e utilizado para os interesses de negócio da Instituição.

8.5. A definição e as medidas de controle de acesso à rede interna do MEC ficarão sob a responsabilidade da Área de TI do MEC.

8.6. A Área de TI do MEC deve conceder acesso à rede interna do MEC mediante solicitação da Coordenação-Geral de Gestão de Pessoas para adotar as providências necessárias, limitando o acesso às informações e/ou recursos computacionais do MEC, caso seja necessário.

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

8.8. 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.

8.9. 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.

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

9. CONTROLE DE ACESSO À REDE INTERNA

9.1. É permitido o acesso à rede interna do MEC, seja cabeada ou sem fio, somente a usuários identificados e/ou autenticados, que terão acesso restrito ao que lhes for autorizado.

9.2. A autenticação poderá ser feita utilizando diferentes mecanismos de identificação, tais como senhas, biometria, *tokens* e *Smart Card*.

9.3. A criação, autorização, manutenção e revogação de direitos de acesso à rede interna do MEC devem ser implementadas conforme definições na Norma de Segurança da Informação e Comunicações de Controle de Acesso do Usuário.

9.4. A autenticação do usuário deve ser válida caso todas as entradas confirmadas estejam de acordo com informações de acesso fornecidas a ele pela Área de TI do MEC. Na ocorrência de erro na entrada de dados do usuário convém que o sistema não emita mensagem indicando qual parte da entrada esteja correta ou incorreta.

9.5. Ao usuário que não desempenha função de administrador da rede interna do MEC deve ser fornecida apenas uma única conta de acesso, pessoal e intransferível, conforme definido na Norma de Segurança da Informação e Comunicações de Controle de Acesso do Usuário.

9.6. A identificação dos recursos computacionais e de comunicações autorizados pela Área de TI do MEC a ingressar na rede interna do MEC deve ocorrer de forma automática para que possam autenticar suas conexões na rede interna.

9.7. A rede interna do MEC deve ser segmentada em domínios lógicos de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço público e proteção da rede interna.

9.8. Deve ser estabelecido pela Área de TI do MEC juntamente com a área de RH e responsáveis pelas empresas terceirizadas que atuam no MEC, um processo de revisão contínuo dos direitos de acesso à rede interna.

9.9. A Área de TI do MEC deve utilizar procedimentos que permitam identificar e rastrear de forma fácil os acessos e/ou endereços de origem/destino e serviços utilizados, armazenando os registros de eventos (*logs*).

9.10. A Área de TI do MEC deve disponibilizar para o usuário os serviços e recursos de rede previamente homologados mediante autorização formal.

10. CONTROLE DE ACESSO REMOTO

10.1. O acesso remoto à rede interna do MEC deve ser realizado por meio seguro através de uma VPN (*Virtual Private Network*), conforme estabelecido na Norma para Acesso à VPN do MEC.

10.2. A Área de TI do MEC deve configurar os recursos computacionais destinados ao controle de acesso remoto de maneira que seja criado e armazenado os registros de eventos (logs) de acesso remoto contendo informações do usuário, data, hora e/ou outros dados específicos que possibilitem o rastreamento das ações tomadas para posterior auditoria.

10.3. Os registros de eventos (*log*) de acesso remoto devem ser revisados de maneira contínua, observando a lista de permissões.

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.

ANEXO IX

NORMA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
DE CONTROLE DE ACESSO DO USUÁRIO

ÍNDICE

1. DESCRIÇÃO

1.1. Esta norma trata dos requisitos de segurança que norteiam o uso dos serviços de TI disponibilizados pelo MEC, tais como Internet e correio eletrônico, criação de contas e concessão de acesso aos serviços de TI.

2. PÚBLICO ALVO

2.1. Este documento se aplica a todos os usuários do MEC.

3. OBJETIVO

3.1. Orientar os Usuários do MEC quanto às regras de criação e concessão de contas de acesso, utilização dos serviços de TI tais como: Internet e correio eletrônico de forma a preservar a confidencialidade, integridade e disponibilidade das informações.

4. ESCOPO

4.1. Criação de contas e concessão de acesso à rede interna do MEC.
4.2. Utilização de serviços de TI do MEC.

5. NÃO ESCOPO

5.1. Utilização de serviços de TI de entidades vinculadas e/ou de terceiros 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° 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. 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 conta de acesso à rede interna e ao correio eletrônico é uma concessão do MEC, não um direito do usuário e será obrigatoriamente cancelada quando do seu desligamento, ao final da vigência do contrato ou qualquer outro ato jurídico firmado ou por solicitação da chefia imediata.

8.2. A liberação de acesso aos recursos computacionais e de comunicações e a rede interna do MEC somente será concedido mediante identificação e autenticação do usuário por meio de conta de acesso e senha.

8.2.1. A senha de acesso é pessoal e intransferível sendo dever do usuário zelar pela sua segurança.

8.3. O usuário é responsável por todas as atividades realizadas por meio de sua conta de acesso e por possíveis danos causados à rede interna do MEC pela má utilização da conta.

8.4. Os serviços de Internet, correio eletrônico (@mec.gov.br) e quaisquer outros da Área de TI do MEC disponibilizados pelo MEC aos seus usuários devem ser utilizados para os interesses da Instituição.

8.5. O acesso a Internet e ao correio eletrônico, por meio dos recursos computacionais custodiados ou de propriedade do MEC, deve ser realizado somente por meio de softwares homologados pela Área de TI do MEC.

8.6. Os serviços de Internet, correio eletrônico (@mec.gov.br) e quaisquer outros da Área de TI do MEC disponibilizados pelo MEC não devem ser utilizado para a prática de atos ilícitos, proibidos por lei ou pela presente norma, prejudiciais aos direitos e interesses do MEC ou de terceiros.

8.7. O usuário deve evitar o acesso simultâneo aos recursos computacionais e de comunicações do MEC, ficando o titular da conta de acesso, responsável pelos riscos e danos que a utilização paralela implica.

8.8. O MEC mantém uma divulgação continua para a conscientização de todos os usuários quanto a Política de Segurança da Informação e Comunicações e normas correlatas.

8.9. 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.

8.10. 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.

8.11. Ao Agente Público descumpridor dessa norma serão aplicadas as sanções previstas no regimento interno do MEC e na legislação em vigor.

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

9. CRIAÇÃO E MANUTENÇÃO DE CONTAS

9.1. Para cada usuário é concedida uma única conta de acesso à rede interna e ao correio eletrônico, exceto os usuários com perfis administrativos da área de TI do MEC, que devem possuir credenciais diferenciadas para a execução de tarefas administrativas.

9.2. Cabe a Área de TI do MEC definir os padrões e regras a serem seguidas para a criação e utilização da conta e senha de acesso à rede interna e o ao correio eletrônico.

9.2.1. O usuário deve seguir os padrões e as regras definidas pela Área de TI do MEC.

9.3. Somente servidores efetivos, mediante sistema específico, devem solicitar, formalmente à Área de TI do MEC, a criação da conta de acesso à rede e ao correio eletrônico.

9.4. Em casos de alterações nas atribuições do usuário, a readequação dos direitos de acesso à rede interna do MEC deve ser realizada pela Área de TI do MEC mediante solicitação formal por parte de servidor designado, mediante sistema específico.

9.5. A criação e manutenção da conta de acesso à rede interna e ao correio eletrônico do usuário devem adotar a nomenclatura padronizada pela Área de TI do MEC.

9.6. A senha de acesso deve ser obrigatoriamente alterada pelo usuário, quando da realização do primeiro acesso e periodicamente de acordo com o padrão instituído pela Área de TI do MEC.

9.7. A composição e o período de expiração das senhas devem seguir o padrão definido pela Área de TI do MEC:

9.7.1. O usuário deve evitar a utilização de informações pessoais na criação da senha de acesso à rede.

10. BLOQUEIO E CANCELAMENTO DE ACESSO

10.1. O bloqueio da conta de acesso à rede interna e ao correio eletrônico do MEC será efetuado nos seguintes casos:

10.1.1. 05 (cinco) tentativas de acesso mal sucedidas;

10.1.2. Solicitação formal da chefia imediata do usuário devidamente formalizada e justificada;

10.1.3. Não seja detectada a utilização da conta de acesso do usuário por período igual ou superior a 90 (noventa) dias;

10.1.4. O usuário seja desligado do MEC;

10.2. Nos casos de suspeita de infração à Política de Segurança da Informação em vigor e normas correlatas, a Área de TI do MEC poderá efetuar o bloqueio preventivo da conta de acesso até a conclusão da averiguação dos fatos sob suspeita e comunicará a chefia imediata do usuário sob ação.

10.2.1. O desbloqueio da conta de acesso do usuário à rede será realizado apenas após solicitação formal da chefia imediata à Área de TI do MEC.

10.3. É de responsabilidade da chefia imediata do usuário comunicar formalmente à Área de TI do MEC, o desligamento ou saída do usuário do MEC, para bloqueio ou desativação da conta de acesso à rede e ao correio eletrônico.

11. USO DO CORREIO ELETRÔNICO

11.1. A conta de correio eletrônico corporativo, disponibilizada ao usuário é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos ao MEC que venham a ser ocasionados por mau uso do serviço.

11.2. É vetada a utilização do serviço de correio eletrônico corporativo para receber de forma consentida, armazenar e/ou enviar/encaminhar mensagens contendo:

11.2.1. Códigos maliciosos (vírus, *spams*, *trojans*, entre outros);

11.2.2. Materiais com conteúdo pornográfico, pedofilia, atentatórios à moral e aos bons costumes ou ofensivos;

11.2.3. Conteúdo de incitação à violência;

11.2.4. Conteúdo criminoso ou ilegal ou que façam sua apologia;

11.2.5. Conteúdo que não respeite os direitos autorais ou objetivos comerciais particulares;

11.2.6. "Correntes" de mensagens eletrônicas ou qualquer *e-mail* que atrapalhe a condução e continuidade do trabalho;

11.3. O uso do correio eletrônico particular é de inteira responsabilidade do usuário, cabendo ao mesmo a responsabilidade por riscos ou danos causados.

11.3.1. A Área de TI do MEC não é responsável por prestar suporte técnico quanto ao uso e/ou configuração do serviço de correio eletrônico particular.

11.4. O correio eletrônico particular do usuário, não deve ser utilizado para envio e/ou recebimento de informações de interesse do MEC.

11.5. O usuário deve utilizar os serviços de correio eletrônico, tanto corporativo quanto particular, de forma a não prejudicar o trabalho de terceiros, causar tráfego desnecessário na rede de dados ou sobrecarregar os sistemas do MEC e/ou demais organizações.

11.6. O usuário deve realizar periodicamente manutenção em sua caixa de correio eletrônico de forma a garantir que o limite de tamanho definido não seja alcançado e o serviço mantenha-se sempre disponível.

11.7. Mensagens já lidas, sem utilidade, devem ser apagadas regularmente pelo próprio usuário, considerando as armazenadas em pastas personalizadas, rascunhos, enviadas e lixeira.

11.8. Uma assinatura padrão deve ser colocada no final de cada mensagem e deve ser usada somente para identificar seu remetente.

11.9. Mensagens de correio eletrônico que contenham informações sensíveis ao MEC devem, sempre que possível, ser criptografadas antes do envio de forma a preservar o seu sigilo e integridade.

11.10 O usuário deve evitar o uso do correio eletrônico em mais de um recurso computacional ou de comunicação simultaneamente, ficando o titular da conta, responsável pelos riscos e danos que a utilização paralela implica.

11.11 Para preservação e bom funcionamento do serviço de correio eletrônico, o usuário deve atentar-se, minimamente, aos seguintes itens:

11.11.1. Excluir *e-mails*, que contenham *links* de internet e/ou arquivos anexos de origem desconhecida ou duvidosa, a fim de eliminar a possibilidade de execução/instalação de *softwares* que contenham códigos maliciosos;

11.11.2. Não divulgar o endereço de correio eletrônico em *sites*, ou listas de discussão na Internet que não sejam de interesse do MEC;

11.11.3. Evitar anexar arquivos às mensagens a serem enviadas internamente, priorizando disponibilizar o caminho para localização do arquivo na rede interna do MEC;

12. USO DA INTERNET

12.1. Todo usuário pode utilizar o serviço de Internet, homologados pela Área de TI do MEC, após a liberação da concessão de acesso à rede interna. Cabe a sua chefia imediata avaliar a necessidade de utilização do serviço e comunicar a Área de TI do MEC no caso de restrição.

12.2. O usuário não deve disponibilizar informações custodiadas ou de propriedade do MEC na Internet, sem prévia autorização do responsável pela respectiva informação.

12.3. O MEC autoriza o uso da Internet para fins pessoais nos limites dos princípios da ética, razoabilidade e legalidade.

12.4. Nas instalações do Ministério todo acesso a Internet utilizando os recursos computacionais e de comunicação custodiados ou de propriedade do MEC deve ser realizado por meio de conexões disponibilizadas e/ou autorizadas pela Área de TI do MEC.

12.5. O usuário não deve acessar simultaneamente a internet por meio de conexões diferentes tais como rede cabeada e sem fio.

12.6. Caso seja necessário ao desempenho das funções do usuário pode ser efetuado *downloads* de arquivos da Internet desde que sejam respeitados os termos de licença e contratuais dos fornecedores.

12.6.1. Os arquivos que eventualmente forem bloqueados poderão ter o *download* liberado temporariamente, desde que previamente autorizado pela Área de TI do MEC.

12.7. Quando o usuário utilizar o acesso à Internet para a realização de transações que envolvam informações sensíveis do MEC, deve adotar, pelo menos, as seguintes regras de segurança:

12.7.1. Digitar o endereço do site diretamente no Navegador (*browser*);

12.7.2. Não clicar em links indicados nas páginas Internet ou mensagens de correio eletrônico;

12.7.3. Quando for acessar sites de instituições bancárias, verificar a existência do uso de certificado digital (cadeado indicado na janela do navegador);

12.7.4. Quando da transmissão de informações, verificar se o endereço do *site* (URL) inicia-se por "HTTPS";

12.7.5. Nos casos de dúvidas quanto à utilização das regras acima, contatar a Área de TI do MEC.

12.8. A Internet no MEC não deve ser utilizada para:

12.8.1. Transmitir para si ou para terceiros softwares e/ou informações custodiadas ou de propriedade do MEC, sem prévia autorização da chefia imediata;

12.8.2. Acessar sites de pornografia, pedofilia, ou que façam incitação à violência e outros contrários à legislação e regulamentação em vigor, mesmo que alguns desses sites não estejam bloqueados pelos mecanismos de segurança implementados na rede interna do MEC, exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho realizados.

12.8.3. Acessar sites com materiais atentatórios à moral e aos bons costumes, ofensivos ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de *softwares*;

12.8.4. Executar atividades relacionadas a jogos eletrônicos;

12.8.5. Acessar conteúdo multimídia, exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho realizados no MEC.

13. MONITORAMENTO

13.1. A Área de TI do MEC tem permissão para monitorar e restringir o uso a Internet e ao correio eletrônico, quanto à origem, destino, quantidade, tipo de conteúdo e volume de informações.

13.2. Nos casos de suspeita de infração à Política de Segurança da Informação em vigor e normas correlatas, a Área de TI do MEC poderá acessar o correio eletrônico do usuário em questão.

13.3. Mediante solicitação formal da chefia imediata do usuário, a Área de TI do MEC poderá conceder acesso ao correio eletrônico de um usuário para o solicitante ou para outro usuário designado, somente nas seguintes situações:

13.3.1. Desligamento do usuário;

13.3.2. Término do contrato de trabalho;

13.3.3. Afastamento do usuário por motivos de licenças;

13.3.4. Falecimento do usuário;

13.3.5. Suspeita de infração à Política de Segurança da Informação e Comunicações em vigor e normas correlatas.

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 e a Coordenação-Geral de Recursos Logísticos – CGRL.

18. VIGÊNCIA

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