

ANEXO VIII

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

ÍNDICE

1. Descrição
2. Público Alvo
3. Objetivo
4. Escopo
5. Não escopo
6. Documentos de referência
7. Definições
8. Regras gerais
9. Controle de acesso à rede interna
10. Controle de acesso remoto
11. Implementação de regras
12. Condições obrigatórias de atualização do documento
13. Prazo de revisão
14. Responsável pela atualização
15. Vigência

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 nº 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.