

## ANEXO IX

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

#### ÍNDICE

1. Descrição
2. Público alvo
3. Objetivo
4. Escopo
5. Não escopo
6. Documento de referência
7. Definições
8. Regras gerais
9. Criação e manutenção de contas
10. Bloqueio e cancelamento de acesso
11. Uso do correio eletrônico
12. Uso da Internet
13. Monitoramento
14. Implementação de regras
15. Condições obrigatórias de atualização do documento
16. Prazo de revisão
17. Responsável pela atualização
18. Vigência

#### **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 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 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 contínua 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/installação 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.