MINISTÉRIO DA CULTURA

CONTROLE DE ACESSO À REDE

ORIGEM

Ministério da Cultura – MinC.

REFERÊNCIAS LEGAIS E NORMATIVAS

Portaria nº 327/2014/MinC - Aprova, no âmbito do Ministério da Cultura, norma de Segurança que estabelece as Diretrizes de Segurança da Informação e Comunicações.

Portaria nº 119/2011/MinC - Institui a Política de Segurança da Informação e Comunicações do Ministério da Cultura e o Sistema de Segurança da Informação e Comunicações e dá outras providências.

Portaria nº 40/2013/MinC – Aprova o Regimento Interno do Ministério da Cultura.

ABNT ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

ABNT NBR ISO/IEC 27002:2007 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação.

ABNT NBR ISO/IEC 38500:2009 – Governança Corporativa de Tecnologia da Informação.

Norma Complementar nº 07/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Ministério da Cultura – MinC.

SUMÁRIO

APROVAÇÃO

Comitê de Segurança da Informação e Comunicações - CSIC

1. OBJETIVO

1.1 Prevenir acesso não autorizado aos serviços de rede.

2. ESCOPO

2.1 Estabelecer os requisitos de segurança da informação para o controle do acesso lógico aos recursos de tecnologia da informação da rede corporativa do MinC.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação da rede corporativa, doravante chamados simplesmente de administradores de recursos de tecnologia da informação, sendo de responsabilidade de cada um o seu cumprimento.

4. CONCEITOS E DEFINIÇÕES

4.1 Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações estão conceituados no Dicionário de Referência.

5. PRINCÍPIOS

5.1 Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, integridade, confidencialidade e autenticidade, visando à proteção e à preservação das informações necessárias às atividades da instituição.

6. POLÍTICA DE USO DOS SERVIÇOS DE REDE

6.1 A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso de usuários à rede corporativa, seja cabeada ou sem fio, atendendo, no mínimo, os seguintes requisitos e procedimentos (Ref. NC 07/IN01/DSIC/GSIPR):

a) configuração e utilização conforme os interesses da instituição (Ref. NC 07/IN01/DSIC/GSIPR);
b) solicitação formal do superior hierárquico do usuário (Ref. NC 07/IN01/DSIC/GSIPR) nos termos da norma de Gerenciamento de Acesso do Usuário; e
c) adoção das medidas de segurança necessárias, como limitar o acesso às informações e aos recursos de tecnologia da informação conforme seus graus de segurança (Ref. NC 07/IN01/DSIC/GSIPR).

6.2 Utilizar legislação específica para a concessão de acesso às informações sigilosas e para o acesso remoto por meio de canal seguro (Ref. NC 07/IN01/DSIC/GSIPR).

7. AUTENTICAÇÃO PARA CONEXÃO EXTERNA DO USUÁRIO

7.1 Implementar, sempre que possível, pelo menos um dos mecanismos que contemplam biometria, *tokens*, *smart cards*, a fim de autenticar a identidade do usuário na rede (Ref. NC 07/IN01/DSIC/GSIPR).

8. IDENTIFICAÇÃO DE EQUIPAMENTO EM REDES

8.1 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados, armazenando os registros de eventos (Ref. NC 07/IN01/DSIC/GSIPR).

8.2 A área responsável pela administração dos recursos de tecnologia da informação deve disponibilizar aos usuários o acesso à rede corporativa conforme a definição de perfis descritos no (Anexo I).

8.3 As solicitações de acesso devem ser realizadas por meio da Central de Serviços de TI.

9. PROTEÇÃO E CONFIGURAÇÃO DE PORTAS DE DIAGNÓSTICO REMOTAS

9.1 Garantir a segurança e o suporte dos sistemas mais complexos e críticos do negócio, para isso os seguintes procedimentos devem ser adotados:

a) implementar uma chave de bloqueio e procedimentos para controlar o acesso físico às portas;
b) estabelecer um procedimento que garanta que essas portas sejam acessíveis somente através de um acordo entre o gestor dos serviços e o pessoal de suporte que solicitou o acesso;
c) desabilitar ou remover dos equipamentos portas, serviços e recursos similares que não são especificamente requeridos para a funcionalidade do negócio.

10. SEGREGAÇÃO DE REDES

10.1 O acesso à rede sem fio deve ser disponibilizado pela área responsável pela administração dos recursos de tecnologia da informação em segmento lógico segregado, garantindo o controle das conexões à Rede MinC e com as exigências necessárias quanto aos protocolos de segurança.

11. CONTROLE DE CONEXÃO DE REDE

11.1 Assegurar a administração adequada dos controles de segurança, a fim de adotar uma política de controle rígida quanto quaisquer potencial ponto de risco à segurança da informação, adotando os seguintes procedimentos:

a) segregar a responsabilidade operacional pela operação dos recursos computacionais;
b) utilizar criptografia robusta e protocolos de segurança como SSL/TLS ou IPSEC para proteger os dados confidenciais durante a transmissão em redes sem fio e públicas;
c) monitorar a presença de pontos de acesso sem fio;
d) usar sistemas de detecção de invasão e/ou sistemas de prevenção contra invasão para monitorar todo o tráfego no ambiente de dados confidenciais cartão e alertar as equipes sobre comprometimentos suspeitos;
e) formalizar, justificar, aprovar e testar todas as conexões de rede, serviços, protocolos e portas de comunicação permitidas e alterações às configurações do firewall e do roteador;
f) analisar os conjuntos de regras do firewall e do roteador pelo menos a cada seis meses;
g) manter diagrama da rede atualizado com todas as conexões com relação aos dados do portador do cartão, incluindo quaisquer redes sem fio;
h) controle rígido sobre equipamentos e/ou softwares com capacidade para analisar tráfego de rede.

12. CONTROLE DE ROTEAMENTO DE REDES

12.1 Implementar controles físicos e lógicos de roteamento de redes.

13. PENALIDADES

13.1 Todos os servidores e colaboradores estão sujeitos às regras da Política de Segurança da Informação e Comunicações e devem observar integralmente o que dispõe este documento. A inobservância dessas regras acarretará em apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização administrativa, civil e penal.

14. COMPETÊNCIAS E RESPONSABILIDADES

14.1 Os servidores e os colaboradores devem ter conhecimento da Política de Segurança da Informação e Comunicações, tendo a obrigação de seguir rigorosamente o disposto nas normas de segurança.

15. DISPOSIÇÕES GERAIS

15.1 Qualquer dúvida ou sugestões sobre a Política de Segurança da Informação e Comunicações e suas orientações devem ser imediatamente encaminhadas à área responsável por Segurança da Informação para análise e/ou esclarecimento.

16. ATUALIZAÇÃO

16.1 Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação e Comunicações, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

17. VIGÊNCIA

17.1 Esta norma entra em vigor na data de sua publicação.

18. ANEXOS

Anexo I - Definição de perfis de acesso.