MINISTÉRIO DA CULTURA

RESPONSABILIDADE PELOS ATIVOS

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.

NC 10/IN01/DSIC/GSIPR – Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos 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 Alcançar e manter a proteção adequada dos ativos da instituição.

2. ESCOPO

2.1 Estabelecer regras a serem seguidas no inventário, na definição dos responsáveis e no uso aceitável dos ativos de informação, visando alcançar e manter sua correta proteção.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos proprietários dos ativos de 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. INVENTÁRIO DOS ATIVOS DE INFORMAÇÃO

6.1 Os ativos de informação de propriedade da instituição devem ser claramente identificados e um inventário de todos os ativos de informação importantes deve ser mantido.

6.2 O inventário deve incluir todas as informações necessárias a partir das necessidades de recuperação ou de substituição eficiente dos ativos de informação em caso de desastre, bem como com vistas a atender aos interesses da sociedade e do Estado. O detalhamento dos ativos de informação deve contemplar, no mínimo e quando aplicável, o seguinte conjunto essencial de informações:

a) identificação única (matrícula, número patrimonial, nome, etc.);
b) tipo de ativo;
c) formato;
d) localização;
e) conteúdo do ativo de informação, com clareza e objetividade (Ref. NC 10/IN01/DSIC/GSIPR);

f) valor do ativo para a instituição, considerando fatores de risco aos quais possa estar exposto, como ameaças, vulnerabilidades e impactos (Ref. NC 10/IN01/DSIC/GSIPR);
g) proprietário do ativo de informação (Ref. NC 10/IN01/DSIC/GSIPR);
h) custodiantes (Ref. NC 10/IN01/DSIC/GSIPR);
i) requisitos de segurança da informação e comunicações (Ref. NC 10/IN01/DSIC/GSIPR);
j) informações sobre cópias de segurança;
k) informações sobre licenças de uso;
l) descrição do hardware e software;
m) relevância; e
n) grau de segurança.

6.3 Recomenda-se que o detalhamento dos ativos de informação contemple também, e sempre que possível, o levantamento das interfaces e das interdependências internas e externas dos ativos de informação considerados críticos, dos órgãos ou entidades da Administração Pública Federal, bem como os impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres, visando atender aos interesses da sociedade e do Estado (Ref. NC 10/IN01/DSIC/GSIPR).

6.4 Na criação do inventário dos ativos de informação deve-se evitar duplicar outros inventários desnecessariamente, porém deve-se assegurar que o seu conteúdo está compatível e coerente com os inventários em uso pela instituição.

6.5 Devem ser identificados os riscos e os respectivos requisitos de segurança de cada ativo inventariado, para tanto, devem ser adotadas metodologias de Gestão de Riscos de Segurança da Informação e Comunicações e de Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC, que incorporem o processo de Inventário e Mapeamento de Ativos de Informação do MinC.

6.6 É necessário que o(s) container(es) dos ativos seja caracterizado, no mínimo, com as seguintes informações:

a) lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado; e
b) respectiva indicação dos responsáveis por manter estes recipientes.

6.7 O inventário de Ativos de Informações do MinC deve ser revisto periodicamente no máximo a cada três meses ou eventualmente quando houver necessidade.

7. PROPRIETÁRIO DOS ATIVOS

7.1 Os ativos de informação importantes em uso na instituição devem possuir um proprietário do ativo de informação e seu substituto.

7.2 O proprietário do ativo de informação e seu substituto devem estar devidamente nomeados por portaria de atribuição, publicada no boletim interno do MinC.

7.3 O proprietário do ativo de informação deve assumir, no mínimo, as seguintes atividades:

a) descrever o ativo de informação (Ref. NC 10/IN01/DSIC/GSIPR);
b) definir as exigências de segurança da informação e comunicações do ativo de informação (Ref. NC 10/IN01/DSIC/GSIPR);
c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários (Ref. NC 10/IN01/DSIC/GSIPR);
d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo (Ref. NC 10/IN01/DSIC/GSIPR);
e) indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação (Ref. NC 10/IN01/DSIC/GSIPR);
f) assegurar que os ativos de informação sob sua responsabilidade estejam adequadamente classificados segundo o grau de segurança das informações nele contidas;
g) assegurar o tratamento adequado conforme o grau de segurança das informações nele contidas, de acordo com as orientações descritas em legislação específica sobre classificação da informação;
h) assegurar que credenciais ou contas de acesso serão habilitadas conforme as restrições ao acesso definidas pelo grau de segurança das informações nele contidas, de acordo com as orientações descritas em legislação específica sobre classificação da informação; e
i) atualizar o inventário quando da mudança de localização ou de responsabilidade do ativo de informação.

7.4 Os proprietários dos ativos de informação devem estabelecer critérios que assegurem a segregação de funções para que ninguém detenha controle de um processo ou sistema na sua totalidade, visando à redução do risco de mau uso acidental ou deliberado dos ativos de informação.

7.5 O proprietário do ativo de informação pode delegar as tarefas de rotina para um custodiante. Todavia, o ativo de informação continua sob sua responsabilidade.

8. USO ACEITÁVEL DOS ATIVOS

8.1 A utilização de recursos de processamento de informação (estações de trabalho, notebooks, netbooks, tablets, smartphones, dentre outros) particulares ou de terceiros na rede corporativa do MinC deve observar os seguintes critérios:

8.1.1 Para acesso restrito à Internet: é permitido, respeitando-se se as regras definidas na POSIC do MinC;

8.1.2 Para acesso a dados: é proibido. Se necessário, exceções devem ser autorizadas pelo gerente da área demandante, desde que sejam adotados os mecanismos de segurança.

8.2 Recursos de processamento de informação fornecidos pelo MinC só podem ser usados por servidores ou colaboradores, respeitando o perfil de acesso de cada usuário.

Trabalho remoto:

8.3 O acesso remoto de servidores e colaboradores do MinC aos recursos e informações corporativas a partir da Internet, deve observar os seguintes critérios:

8.3.1 Deve ser realizado em horário de expediente. Se necessário, exceções devem ser autorizadas pela área responsável pela administração dos recursos de tecnologia da informação;

8.3.2 No período de férias, licença ou afastamento é proibido, sem exceção;

8.3.3 Acesso ao correio eletrônico é permitido e automaticamente criptografado;

8.3.4 Acesso a dados é permitido, desde que seja autorizado pelo coordenador da área demandante;

8.4 Deve ser feito a partir de computadores fornecidos pelo MinC. Acesso a partir de computadores particulares somente pode ser feito quando adotados os mecanismos de segurança homologados pelo MinC. Acesso a partir de computadores públicos (fornecidos por LAN Houses, Cybercafés, etc.) ou de terceiros não são permitidos;

8.5 Se necessário, pode ser realizado a partir de locais públicos (shoppings centers, hotéis, aeroportos, aviões, dentre outros). Os usuários devem atentar para as responsabilidades que assumem quanto à segurança dos computadores utilizados e ter cautela com a exposição de informações sensíveis expostas em tela.

8.6 O acesso remoto da força de trabalho pode ser monitorado ou auditado para apuração de um ato administrativo ou evento de segurança da informação, mediante justificativa e aprovação da área responsável pela administração dos recursos de tecnologia da informação.

8.7 O acesso remoto deve ser imediatamente revogado ao término do vínculo de trabalho com o MinC. Neste caso, os equipamentos de propriedade do MinC deverão ser devolvidos antes da homologação do desligamento.

Uso de correio eletrônico (e-mail):

8.8 É vedado o uso de e-mails não corporativos para envio ou recebimento de mensagens relacionadas ao trabalho, exceto em caso de indisponibilidade do e-mail corporativo, formalmente notificada pela área responsável pela administração dos recursos de tecnologia da informação, e para mensagens urgentes.

Acesso à Internet:

8.9 Pode ser monitorado ou auditado para apuração de um ato administrativo ou evento de segurança da informação, mediante justificativa e aprovação da área responsável pela administração dos recursos de tecnologia da informação;

8.10 Existe controle de acesso baseado nas categorias de sites. Não são permitidos acessos a categorias de sites consideradas ilegais ou impróprias, que oferecem riscos à segurança da informação ou apresentem alto consumo de banda, conforme exemplos mostrados nas Tabelas 1, 2 e 3, respectivamente:

Tabela 1 - Categorias de sites consideradas ilegais ou impróprias	
Categoria	Descrição
Ilegal ou antiético	Sites que apresentam informações, métodos ou instruções sobre ações fraudulentas ou condutas ilegais, tais como fraudes, falsificação, evasão social, furtos, chantagem, etc.
Racismo ou ódio	Sites que discriminam grupos ou indivíduos por raça, cor, etnia, orientação sexual, etc.

Tabela 2 - Categorias de sites que oferecem riscos à segurança da informação	
Categoria	Descrição
Contorno de Proxy	Sites que fornecem informações ou ferramentas sobre como contornar os controles de acesso à Internet e navegar pela Web anonimamente, incluindo os servidores de Proxy anônimos.
Hacking	Sites que retratam as atividades ilícitas em torno da modificação não autorizada ou o acesso aos programas, computadores, equipamentos e outros sites.

Tabela 3 - Categorias de sites que apresentam alto consumo de banda	
Categoria	Descrição
Internet Rádio e TV	Sites que difundem comunicações de rádio ou TV por meio da Internet.
Telefonia via Internet	Sites que permitem comunicações telefônicas por meio da Internet.
Multimídia	Sites que permitem o download de arquivos MP3 ou qualquer outro tipo de áudio ou multimídia.

8.11 O acesso a sites relacionados a redes sociais (Facebook, Google+, Twitter, LinkedIn, Wordpress, Blogger ou similares) é permitido. Os servidores e colaboradores são responsáveis pelo uso e deve, portanto, adotar cautela, atentar para as questões relacionadas à segurança das informações, minimizando riscos e evitando perda de produtividade.

8.12 É proibido postar ou expressar informações ou opiniões pessoais em nome do MinC. Informações que já foram publicadas podem ser compartilhadas, desde que haja autorização formal do responsável pela informação;

8.13 O uso de softwares de compartilhamentos de arquivos Peer-to-peer (eMule, Kazaa, Ares Galaxy, BitTorrent ou similares) é proibido, sem exceção.

Outros recursos de processamento e armazenamento da informação:

8.14 Recursos de processamento de informação fornecidos pelo MinC devem ser usados prioritariamente para atividades relacionadas ao trabalho.

8.15 Estações de trabalho, notebooks, netbooks, smartphones, impressoras, copiadoras, telefones fixos, celulares e aparelhos de fax devem ser usados para fins de trabalho.

8.16 Os servidores e colaboradores são responsáveis pelo uso e deve, portanto, adotar bom senso, atentar para as questões relacionadas à segurança das informações, minimizando riscos e evitando perda de produtividade.

9. PENALIDADES

9.1 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.

10. COMPETÊNCIAS E RESPONSABILIDADES

10.1 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.

11. DISPOSIÇÕES GERAIS

11.1 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.

12. ATUALIZAÇÃO

12.1 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.

13. VIGÊNCIA

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