MINISTÉRIO DA CULTURA

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E MELHORIAS

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.

NBR ISO/IEC 27001:2005 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação.

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

Norma Complementar nº 05/IN01/DSIC/GSIPR – Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal.

Norma Complementar nº 08/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

Instrução Normativa IN 01/2008 GSI – Disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

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 Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.

2. ESCOPO

2.1 Disciplinar o Gerenciamento de Incidentes de Segurança da Informação e Comunicações no Ministério da Cultura - MinC, visando assegurar que este tipo de incidente seja tratado e gerido de modo a permitir a rápida restauração de sistemas e serviços com o mínimo de interrupção, minimizando os impactos negativos nas áreas de negócio do MinC

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores envolvidos com a gestão de incidentes de segurança da informação e comunicações, 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. RESPONSABILIDADES E PROCEDIMENTOS

6.1 Será constituída Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) com a incumbência de:

I - realizar ações de análise de vulnerabilidade e estabelecer mecanismos de registro e controle de conformidade das rotinas e sistemas do Ministério da Cultura à Política de Segurança da Informação e Comunicações e suas normas e procedimentos de segurança, comunicando quebras de segurança e outras desconformidades ao Gestor de Segurança da Informação;

II - receber, analisar e responder a notificações relacionadas aos incidentes de quebra de segurança em computadores no âmbito do Ministério da Cultura, encaminhando-as ao Gestor de Segurança da Informação quando necessário;

III - gerenciar os sistemas de informação do Ministério da Cultura, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários; e

IV - apresentar ao CSIC relatórios periódicos sobre riscos relacionados à segurança da informação e comunicações, acompanhados de proposta de aperfeiçoamento dos sistemas de informação deste Ministério, quando for o caso;

V – o funcionamento da ETIR do MinC deverá seguir o Documento de Constituição da ETIR (Anexo I), alinhado com a Política de Segurança da Informação e Comunicações e devidamente aprovado pelo Comitê de Segurança da Informação e Comunicações – CSIC (Ref. NC 05/IN01/DSIC/GSIPR).

6.2 Responsabilidades e procedimentos de gerenciamento de incidentes devem ser estabelecidos para assegurar respostas efetivas e ordenadas a incidentes de segurança da informação conforme o (Anexo II).

6.3 Devem ser considerados, minimamente, os seguintes procedimentos técnicos para lidar com os diferentes tipos de incidentes de segurança da informação:

a) falhas de sistemas de informação e perda de serviços;
b) código malicioso;
c) *denial of service* (negação de serviço);
d) violações de confidencialidade e integridade;
e) vazamento de informações; e
f) uso impróprio de sistemas de informação.

7. APRENDENDO COM OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1 Devem ser estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação do MinC sejam quantificados e monitorados.

7.2 Deve ser feita uma análise crítica periódica para identificação dos incidentes de segurança da informação recorrentes e de alto impacto no negócio.

7.3 O resultado da análise deve ser utilizado para identificar a necessidade de melhorias ou controles adicionais para limitar a frequência, danos e custos de ocorrências futuras e para servir como fator de análise crítica da política de segurança.

7.4 A ETIR comunicará a ocorrência de incidentes de segurança em redes de computadores ao CTIR Gov, conforme procedimentos a serem definidos pelo próprio CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a Administração Pública Federal, bem como a geração de estatísticas (Ref. NC 08/IN01/DSIC/GSIPR).

8. COLETA DE EVIDÊNCIAS

8.1 Para fins que envolvam uma ação legal (civil ou criminal), após um incidente de segurança da informação, é necessário que as evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da(s) jurisdição(ões) pertinente(s).

8.2 Devem ser estabelecidos procedimentos internos para atividades de coleta e apresentação de evidências, considerando:

a) as evidências de infrações e quebras de segurança devem abranger: a admissibilidade da evidência (se a evidência pode ser ou não utilizada) e importância da evidência (relacionada ao risco que impõe à informação).

8.3 Para a produção de evidências admissíveis deve-se assegurar que os sistemas de informação utilizados estão de acordo com qualquer legislação e códigos de prática publicados.

8.4 A integridade de todo material de evidência deve ser preservada.

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.

14. ANEXOS

Anexo I - Documento de Constituição da ETIR.
Anexo I - Processo de Gerenciamento de Incidentes.