MINISTÉRIO DA CULTURA

ANÁLISE DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO

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 31000:2009 – Gestão de Riscos – Princípios e diretrizes.

ABNT NBR ISO/IEC 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação.

Norma Complementar nº 02/IN01/DSIC/GSIPR – Metodologia de Gestão de Segurança da Informação e Comunicações.

Norma Complementar nº 04/IN01/DSIC/GSIPR – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da Administração Pública Federal - 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 Identificar, quantificar e priorizar os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a instituição.

2. ESCOPO

2.1 Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC no âmbito do Ministério da Cultura – MinC.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores envolvidos com a análise de risco em segurança da informação e comunicações, sendo responsabilidade de cada um o seu cumprimento. A inobservância desta norma acarretará em apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização penal, civil e administrativa.

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 A 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. PROCESSO DE GRSIC – GENERALIDADES

6.1 O MinC deverá implantar e implementar o Processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC que se baseia no processo de melhoria contínua, no método denominado ciclo “PDCA” - Plan-Do-Check-Act (Ref. NC 04/IN01/DSIC/GSIPR) que consiste em:

a) Planejar (***Plan* – P**) – É fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações planejará as ações de segurança da informação e comunicações que serão implementadas, considerando os requisitos ou pressupostos estabelecidos pelo planejamento organizacional, bem como as diretrizes expedidas pela autoridade decisória de seu órgão ou entidade;

b) Fazer (***Do* – D**) - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações implementará as ações de segurança da informação e comunicações definidas na fase anterior;

c) Checar (***Check* – C**)- É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações avaliará as ações de segurança da informação e comunicações implementadas na fase anterior;

d) Agir (***Action* – A**) - É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicações aperfeiçoará as ações de segurança da informação e comunicações, baseando-se no monitoramento realizado na fase anterior.

6.2 6.2 O processo de GRSIC do MinC deve ser contínuo e produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios – GCN.

6.3 O Processo de GRSIC do MinC deve estar alinhado e considerar, no mínimo, os seguintes fatores:

a) os objetivos estratégicos definidos para o órgão;
b) os processos de negócio do Ministério;
c) os requisitos legais;
d) a estrutura organizacional do MinC;
e) a Política de Segurança da Informação e Comunicações – POSIC vigente.

6.4 O Processo de GRSIC do MinC deve considerar todos os ativos de informação classificados como vitais e críticos para a realização das atividades fins do órgão.

6.5 Cabe ao Gestor de Segurança da Informação e Comunicações - GSIC, no âmbito de suas atribuições, coordenar o processo de GRSIC no MinC.

6.6 O Gestor de Segurança da Informação e Comunicações pode indicar responsáveis pelo gerenciamento de atividades, a quem serão conferidas, no mínimo, as seguintes atribuições (Ref. NC 04/IN01/DSIC/GSIPR):

a) análise/avaliação e tratamento dos riscos (Ref. NC 04/IN01/DSIC/GSIPR);
b) elaboração sistemática de relatórios para os Gestores de Segurança da Informação e Comunicações, em cujo conteúdo constará a análise quanto à aceitação dos resultados obtidos, e consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração (Ref. NC 04/IN01/DSIC/GSIPR).

6.7 Uma abordagem de equipe consultiva pode ser utilizada para:

a) auxiliar a estabelecer o contexto apropriadamente;
b) assegurar que os interesses das partes interessadas sejam compreendidos e considerados;
c) auxiliar a assegurar que os riscos sejam identificados adequadamente;
d) reunir diferentes áreas de especialização em conjunto para análise dos riscos;
e) assegurar que diferentes pontos de vista sejam devidamente considerados quando da definição dos critérios de risco e na avaliação dos riscos;

f) garantir o aval e o apoio para um plano de tratamento;
g) aprimorar a gestão de mudanças durante o processo de GRSIC;
h) desenvolver um plano apropriado para comunicação e consulta interna e externa.

7. ETAPAS DO PROCESSO DE GRSIC

7.1 O processo de gestão de riscos do MinC deve ser estruturado para ser realizado em ciclos anuais, obedecendo as seguintes etapas:

7.2 Definições preliminares

7.3 Nesta fase, deve-se realizar uma análise do órgão a fim de identificar os critérios e o enfoque mais apropriado, apoiando-se na definição do escopo e na adoção de uma metodologia (Ref. NC 04/IN01/DSIC/GSIPR);

a) definição de escopo: visa delimitar o âmbito de atuação. Esse escopo pode abranger o órgão, uma unidade, um processo, um sistema, um recurso ou um ativo de informação;
b) adoção da metodologia: visa adotar uma metodologia de GRSIC que atenda aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.

7.4 Análise/avaliação dos riscos

7.4.1 Nesta etapa, inicialmente são identificados os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados (Ref. NC 04/IN01/DSIC/GSIPR).

a) identificar os ativos e seus respectivos responsáveis dentro do escopo estabelecido e conforme a Política de Segurança da Informação e Comunicações e a legislação pertinente (Ref. NC 04/IN01/DSIC/GSIPR);
b) identificar os riscos associados ao escopo definido, considerando:

- as ameaças envolvidas (Ref. NC 04/IN01/DSIC/GSIPR);
- as vulnerabilidades existentes nos ativos de informação (Ref. NC 04/IN01/DSIC/GSIPR);
- as ações de Segurança da Informação e Comunicações – SIC já adotadas (Ref. NC 04/IN01/DSIC/GSIPR);
- fontes de risco;
- áreas de impactos;
- eventos (incluindo mudanças nas circunstâncias);
- causas;
- consequências potenciais.

c) estimar os riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados (Ref. NC 04/IN01/DSIC/GSIPR);
d) avaliar os riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos (Ref. NC 04/IN01/DSIC/GSIPR);
e) relacionar os riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo órgão ou entidade (Ref. NC 04/IN01/DSIC/GSIPR).

7.5 Plano de Tratamento de Riscos

7.5.1 Nesta etapa devem ser determinadas as formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir/compartilhar ou aceitar o risco, observando:

a) a avaliação do tratamento de riscos já realizado;
b) a eficácia das ações de Segurança da Informação e Comunicações – SIC já existentes (Ref. NC 04/IN01/DSIC/GSIPR);
c) a avaliação da eficácia desse tratamento;
d) as restrições organizacionais, técnicas e estruturais (Ref. NC 04/IN01/DSIC/GSIPR);
e) os requisitos legais (Ref. NC 04/IN01/DSIC/GSIPR);
f) a análise custo/ benefício (Ref. NC 04/IN01/DSIC/GSIPR);
g) a avaliação e decisão quanto aos níveis de risco residual, se não forem toleráveis, deve-se definir a implementação de um novo tratamento para os riscos.

7.5.2 O plano para o tratamento dos riscos deve ser formulado, relacionando, no mínimo:

a) razões para a seleção das opções de tratamento, incluindo os benefícios que se espera obter;
b) responsáveis pela aprovação do plano e os responsáveis pela implementação do plano (Ref. NC 04/IN01/DSIC/GSIPR);
c) ações de SIC propostas (Ref. NC 04/IN01/DSIC/GSIPR);
d) prioridades e prazos de execução necessários à sua implantação (Ref. NC 04/IN01/DSIC/GSIPR);
e) os recursos requeridos, incluindo contingências;
f) medidas de desempenho e restrições;
g) requisitos para a apresentação de informações e de monitoramento;
h) cronograma e programação.

7.6 Aceitação do Risco

7.6.1 Nesta etapa devem ser analisados os resultados do processo de Análise/Avaliação dos Riscos, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação (Ref. NC 04/IN01/DSIC/GSIPR).

7.7 Implementação do Plano de Tratamento dos Riscos

7.7.1 Nesta etapa devem ser executadas as ações/medidas de controles de SIC incluídas no Plano de Tratamento dos Riscos (Ref. NC 04/IN01/DSIC/GSIPR).

7.8 Monitoramento e análise crítica:

7.8.1 Esta etapa, tendo como base a metodologia do PDCA (ver item 6.1), objetiva detectar possíveis falhas nos resultados, monitorar os riscos, as ações de SIC e verificar a eficácia do processo de GRSIC no MinC, visando manter o processo de GRSIC alinhado às diretrizes estratégicas do MinC e manter os riscos monitorados e analisados criticamente (Ref. NC 04/IN01/DSIC/GSIPR), a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) nos critérios de avaliação e aceitação dos riscos (Ref. NC 04/IN01/DSIC/GSIPR);
b) no ambiente (Ref. NC 04/IN01/DSIC/GSIPR);
c) nos ativos de informação (Ref. NC 04/IN01/DSIC/GSIPR);
d) nas ações de SIC (Ref. NC 04/IN01/DSIC/GSIPR);
e) nos fatores do risco – ameaça, vulnerabilidade, probabilidade e impacto (Ref. NC 04/IN01/DSIC/GSIPR).

7.8.2 As responsabilidades relativas ao monitoramento e à análise crítica devem ser claramente definidas.

7.8.3 Os resultados do monitoramento e da análise crítica devem ser:

a) registrados e divulgado internamento para avaliação e as devidas providências e, quando couber, externamente para conhecimento;
b) utilizados como entrada para a análise crítica da estrutura de Gestão de Riscos de Segurança da Informação e Comunicações.

7.9 Melhoria do Processo de GRSIC

7.9.1 Esta etapa visa informar ao Comitê de Segurança da Informação e Comunicações – CSIC a necessidade de implementação de melhorias identificadas na etapa de monitoramento e análise crítica, bem como executar as ações corretivas ou preventivas aprovadas; e assegurar que as melhorias atinjam os objetivos pretendidos (Ref. NC 04/IN01/DSIC/GSIPR).

7.10 Comunicação do Risco

7.10.1 A comunicação e a consulta às partes interessadas internas e externas devem acontecer durante todas as fases do processo de GRSIC, considerando:

a) manter as instâncias superiores informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas (Ref. NC 04/IN01/DSIC/GSIPR);
b) serem realizadas comunicações e consultas regulares a fim de assegurar que os responsáveis pela implementação do processo de GRSIC e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas;
c) abordar questões relacionadas com o risco propriamente dito, suas causas, suas consequências (se conhecidas) e as medidas que estão sendo tomadas para tratá-los.

7.10.2 Os planos de comunicação e consulta devem ser desenvolvidos em um estágio inicial do processo de GRSIC.

8. PENALIDADES

8.1 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.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1 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.

10. DISPOSIÇÕES GERAIS

10.1 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.

11. ATUALIZAÇÃO

11.1 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.

12. VIGÊNCIA

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

13. ANEXOS

Anexo I – Controles e indicadores do processo de GRSIC