MINISTÉRIO DA CULTURA

PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

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.

Lei nº. 8.666, de 21 de junho de 1993, estabelece normas gerais sobre licitações e contratos administrativos pertinentes a obras, serviços, inclusive de publicidade, compras, alienações e locações no âmbito dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios.

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 Garantir a operação segura e correta dos recursos de processamento da informação.

2. ESCOPO

2.1 Estabelecer requisitos de segurança da informação e comunicações que devem ser definidos quanto aos procedimentos e responsabilidades operacionais para garantir o uso correto dos recursos de processamento de informação.

3. PÚBLICO-ALVO

3.1 Esta norma destina-se aos servidores e colaboradores envolvidos com a gestão e uso dos recursos de processamento 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. GESTÃO DE MUDANÇAS

6.1 O MinC deve designar um Gestor de Mudanças, o qual será o responsável pelo processo de mudanças no âmbito deste Ministério (Ref. NC 13/IN01/DSIC/GSIPR).

6.2 O proprietário do ativo de informação deve estabelecer procedimentos e responsabilidades a fim de garantir um controle com relação às mudanças, equipamentos, software e procedimentos vigentes sob sua responsabilidade.

6.3 Somente o pessoal autorizado pelo proprietário do ativo de informação e identificado adequadamente deve ser liberado para acessar os recursos de processamento da informação em produção para implementação de mudanças.

6.4 O processo de gestão de mudanças deve ser composto, no mínimo, pelas fases de:

a) identificação e descrição detalhada de todas as etapas da mudança, contendo escopo, objetivo e benefícios de modo que, a partir dessa descrição, possa ser feita uma análise dos impactos à segurança da informação e comunicações (Ref. NC 13/IN01/DSIC/GSIPR);

b) avaliação dos potenciais impactos à segurança da informação e comunicações que possam ocorrer durante a implementação da mudança, considerando, no mínimo, os seguintes aspectos:

- os detalhes do procedimento de implementação da mudança (Ref. NC 13/IN01/DSIC/GSIPR);
- a análise de risco dos ativos de informação que serão afetados com a mudança (Ref. NC 13/IN01/DSIC/GSIPR);
- as legislações e normas pertinentes (Ref. NC 13/IN01/DSIC/GSIPR);
- a relação desta mudança com outras mudanças que possam estar ocorrendo simultaneamente (Ref. NC 13/IN01/DSIC/GSIPR); e
- o impacto de adiar ou de não se fazer a mudança (Ref. NC 13/IN01/DSIC/GSIPR).

c) aprovação formal para das requisições de mudança (Ref. NC 13/IN01/DSIC/GSIPR);
d) recomendação da implementação ou não das mudanças propostas, indicando, sempre que possível, soluções que mitiguem riscos à SIC (Ref. NC 13/IN01/DSIC/GSIPR);
e) implementação das mudanças autorizadas com base no cronograma de execução (Ref. NC 13/IN01/DSIC/GSIPR);
f) acompanhamento do resultado e fechamento da mudança para assegurar a pleno funcionamento dos serviços ou ativos alterados (Ref. NC 13/IN01/DSIC/GSIPR);
g) correta alocação dos recursos disponíveis (Ref. NC 13/IN01/DSIC/GSIPR);
h) comunicação dos detalhes das mudanças para todas as pessoas envolvidas (Ref. NC 13/IN01/DSIC/GSIPR); e
i) procedimentos de recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados (Ref. NC 13/IN01/DSIC/GSIPR).

6.5 Para que os resultados previstos sejam atingidos de forma eficiente e eficaz devem ser observados, no mínimo, as seguintes ações:

a) adotar medidas que assegurem o alinhamento da missão e do planejamento estratégico do MinC no processo de mudança (Ref. NC 13/IN01/DSIC/GSIPR);
b) utilizar, sempre que possível, ferramentas e técnicas, para gerenciar os vários aspectos envolvidos em um processo de mudança (Ref. NC 13/IN01/DSIC/GSIPR);
c) promover interação constante com a gestão de SIC, gestão de riscos de SIC e gestão de continuidade de negócios em SIC (Ref. NC 13/IN01/DSIC/GSIPR); e
d) promover no MinC ampla divulgação das mudanças, visando à redução de eventuais resistências e dificuldades de implementação das mesmas (Ref. NC 13/IN01/DSIC/GSIPR).

6.6 Todo o processo de mudança deve ser adequadamente documentado por meio de um plano, o qual deve ser elaborado e preenchido com os detalhes de todas as etapas do processo (do início ao fim).

6.6.1 O Plano de Mudança deve ser armazenado em local seguro, sob guarda do Gestor de Mudanças, visando registro histórico para eventuais consultas, bem como auxiliar (como fonte de aprendizado) na resolução de problemas/incidentes ou em ações futuras de mudança.

6.7 Durante a realização da mudança, devem ser adotados procedimentos que visam identificar e registrar, minimamente, os seguintes itens:

a) descrição da mudança;
b) relação de usuários envolvidos e afetados;
c) relação de recursos de processamento da informação envolvidos;
d) responsável pela execução da mudança;
e) procedimentos de recuperação, incluindo procedimentos e responsabilidades pela interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados.

6.7.1 Deve ser mantido um registro de auditoria contendo informações relevantes quanto à realização de uma mudança.

6.8 Todo Plano de Mudança, sempre que possível, deve ser previamente testado antes de sua efetiva implementação.

6.9 Em casos de testes prévios, este deve ser documentado e anexado ao plano de mudança.

6.10 O Plano de Mudança deve ser adaptado, se for o caso, conforme os resultados de eventuais testes prévios.

7. SEGREGAÇÃO DE FUNÇÕES

7.1 A segregação de funções deve ser feita, quando apropriada, visando reduzir o risco de mau uso ou uso doloso dos recursos de processamento da informação.

7.2 Para a implementação da segregação de função, o MinC deve definir as atividades que cada usuário desenvolve, possibilitando a separação dentro de um processo, minimizando a probabilidade de alterações indevidas ou o acesso não autorizado às informações ou recursos de processamento da informação, considerando, pelo menos, os seguintes níveis de competência:

a) gestão: conceder ou solicitar mudança nas atribuições operacionais, preferencialmente sendo o proprietário do ativo de informação;
b) operação: executar as atividades determinadas pelo nível de gestão;
c) monitoramento: acompanhar as atividades de gestão e operação das mudanças nas atribuições operacionais, através de trilhas de auditoria; e

d) auditoria: realizar, de maneira imparcial, o exame analítico e pericial das aplicações e processos.

7.3 Ao se implementar a segregação de função, o proprietário do ativo de informação deve seguir, ao menos, os seguintes controles:

a) definir em sua área de responsabilidade a atuação de cada usuário dentro do processo de trabalho;
b) não destinar a um único usuário o controle total de um processo de trabalho, tal como planejamento, contratação, pagamento e medição dos serviços executados;
c) designar substitutos para os usuários que exercem funções consideradas críticas;
d) estabelecer critérios para o rodízio das atividades dos usuários dentro do processo de trabalho; e
e) criar mecanismos de monitoração quanto à conformidade na utilização de segregação de função, tais como auditoria, implementação de indicadores e reuniões de análise crítica, com o intuito de avaliar os processos de trabalho procurando identificar possíveis fragilidades quanto aos aspectos de segurança da informação.

8. SEPARAÇÃO DOS RECURSOS DE DESENVOLVIMENTO, TESTE E DE PRODUÇÃO

8.1 Ambientes do MinC

8.1.1 Os ambientes de desenvolvimento, homologação, produção, treinamento e testes deste Ministério devem ser distintos, fisicamente e logicamente entre si, visando reduzir o risco de modificação – acidental ou deliberada, possibilidade de erros e/ou acessos não autorizados às informações e serviços suportados pelos sistemas informatizados sob gestão do MinC.

8.1.2 Os processos de desenvolvimento, homologação, produção, treinamento e testes de sistemas devem ser executados exclusivamente nos seus respectivos ambientes.

a) ambientes de desenvolvimento e testes devem ser para uso específico da equipe de tecnologia designada para realizar o desenvolvimento e os testes técnicos do sistema;
b) ambientes de homologação devem ser para uso específico da área de negócio, para homologar as funcionalidades dos sistemas;
c) ambientes de produção são destinados aos sistemas formalmente homologados pela área de negócio, após a conclusão bem sucedida de homologação e testes técnicos e funcionais;

d) ambientes de Treinamento são destinados aos sistemas que estão em produção para transferência de conhecimento da utilização dos sistemas; e
e) ambientes de Teste são destinados aos sistemas que estão em desenvolvimento/homologação para testes de caixa branca e caixa preta.

8.2 Controle de acesso

8.2.1 Os usuários devem ser incentivados a usar diferentes senhas para cada ambiente.

8.2.2 Os sistemas devem ter telas de abertura exibindo mensagens de identificação de cada ambiente.

8.3 Proteção dos dados

8.3.1 Dados de natureza pessoal ou qualquer informação classificada devem, obrigatoriamente, ser descaracterizados (por exemplo: métodos de mascaramento e/ou embaralhamento de dados) e observados os níveis de segurança adequados aos processos de negócio do MinC.

8.3.2 Em casos onde seja fundamental o adequado suporte aos sistemas, a cópia e o uso de base de dados do ambiente de desenvolvimento, homologação, treinamento e teste idêntica ao do ambiente de produção, é obrigatória a autorização formal do proprietário do ativo de informação, bem como devem ser registrados os acessos aos dados de forma a prover trilha para eventuais auditorias.

8.4 Monitoramento

8.4.1 Os ambientes de desenvolvimento, homologação e produção devem ser configurados, no mínimo, para registrar:

a) eventos significativos, principalmente o início e o fim de cada mecanismo de auditoria;
b) falhas de *login*, indicando o número de tentativas realizadas; e
c) a criação e a remoção de usuários, bem como a atribuição e a remoção de direitos do usuário.

8.4.2 Devem ser mantidos os registros de auditoria dos principais logs, trilhas e procedimentos (select, insert, delete) realizados nos dados corporativos do MinC.

8.4.3 Esses registros devem ser mantidos por um período mínimo de 03 meses em servidores, e posteriormente armazenados em mídias de segurança por um período de 24 meses.

8.5 Ambiente de desenvolvimento

8.5.1 O ambiente de teste deve ser o mais semelhante possível ao ambiente de produção, visando à realização adequada dos testes dos sistemas.

8.5.2 O acesso ao código fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) deve ser estritamente controlado com a finalidade de prevenir a introdução de funcionalidades não autorizadas, e para evitar mudanças não intencionais. Para tanto se deve observar:

a) as bibliotecas de códigos fontes de programas não devem ser mantidas no mesmo ambiente dos sistemas em produção;
b) o pessoal de suporte não deve ter acesso irrestrito às bibliotecas de códigos fontes de programas, devem ter acesso apenas aos fontes necessários para a alteração, quando autorizados pelo superior imediato;
c) a atualização das bibliotecas de códigos fontes de programas e itens associados e a entrega de fontes de programas a programadores devem ser efetuados somente após o recebimento da autorização pertinente;
d) as documentações dos programas devem ser mantidas num ambiente seguro; e
e) um registro de auditoria de todos os acessos a códigos fontes de programas deve ser mantido.

8.5.3 Na fase de testes devem ser contemplados testes sobre uso (funcionalidades); segurança; e efeitos sobre outros sistemas vigentes, considerando:

a) as condições definidas na especificação do sistema aplicativo devem ser contempladas nos testes funcionais e de segurança;
b) os ataques mais comuns na plataforma e arquitetura do sistema aplicativo devem ser verificados nos testes de vulnerabilidades;
c) a inspeção de código nos pontos críticos do sistema aplicativo deve ser incluída nos testes de vulnerabilidades;
d) para o uso de bibliotecas e componentes externos em ambiente de produção, é obrigatório testes e homologação prévia dessas; e
e) a documentação dos testes deve incluir registros de falhas de funcionalidades e de detecção de vulnerabilidades, tanto para fins de histórico como para fins de tratamento.

8.5.4 Todas as mudanças devem ser completamente testadas e documentadas para que possam ser reaplicadas, se necessário, em atualizações futuras do software. Se requerido, as modificações devem ser testadas e validadas por um grupo de avaliação independente.

8.5.5 Os aplicativos devem ser transferidos do ambiente de desenvolvimento para a homologação somente após a remoção de informações de depuração e após a verificação da existência e de quaisquer adequações da documentação referente ao sistema.

8.6 Ambiente de homologação

8.6.1 O ambiente de homologação deve ser o mais semelhante possível ao ambiente de produção, visando à realização adequada de testes de aceitação (homologação). Neste caso, a base de homologação poderá ser exatamente igual à base de produção.

8.6.2 Os sistemas somente podem ser implementados em ambiente de produção após testes extensivos e bem sucedidos, os quais devem ser devidamente documentados.

8.7 Ambiente de treinamento

8.7.1 O ambiente de treinamento deve ser o mais semelhante possível ao ambiente de produção, visando à realização adequada do treinamento aos usuários dos sistemas. Neste caso, a base de treinamento pode ser exatamente igual à base de produção.

8.8 Ambiente de produção

8.8.1 Os arquivos e componentes desnecessários ao funcionamento dos sistemas aplicativos devem ser removidos do ambiente de produção.

8.8.2 Em ambientes de produção deve-se assegurar que todas as bibliotecas de código fonte dos programas correspondentes tenham sido atualizadas.

8.8.3 Em casos de manutenção e suporte em banco de dados – principalmente de bases de dados disponíveis em ambientes de produção – é obrigatória a realização prévia de cópia de segurança (backup dos dados).

8.8.4 Visando facilitar o retorno à normalidade em tempo hábil, em caso de qualquer indisponibilidade, configurações de sistemas também devem ser contempladas com políticas e procedimentos de backup.

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 POSIC, 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.