MINISTÉRIO DA CULTURA

CÓPIAS DE SEGURANÇA

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 11515: 2007 – Guia de práticas para segurança física relativas ao armazenamento de dados.

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.

CSN EN 1047-1 - Secure storage units - Classification and methods of test for resistence to fire - Part 1: Data cabinets and diskette inserts.

CSN EN 14450 - Secure storage units - Requirements, classification and methods of test for resistance to burglary - Secure safe cabinets.

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 Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.

2. ESCOPO

2.1 Estabelecer diretrizes para o processo de backup das informações sob guarda da área responsável pela administração dos recursos de tecnologia da informação da rede corporativa, visando garantir, de forma íntegra e confiável, a restauração de dados institucionais armazenados no ambiente computacional 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. CÓPIAS DE SEGURANÇA DAS INFORMAÇÕES

6.1 Os dados institucionais do MinC devem ser protegidos por meio de rotinas sistemáticas de *backup* (cópias de segurança).

6.1.1 A lista de itens que devem ser contemplados nessas rotinas inclui:

a) dados corporativos armazenados em diretórios da rede MinC, onde os acessos e espaço em disco serão disponibilizados pela área responsável conforme item 6.14;
b) e-mails corporativos;
c) arquivos de configurações de sistemas e de seus respectivos computadores servidores;
d) principais logs e trilhas de auditoria de sistemas corporativos; e
e) dados corporativos armazenados em banco de dados.

6.1.2 Os administradores de recursos de tecnologia da informação, juntamente com os respectivos proprietários dos ativos de informação, devem definir os prazos de realização, retenção e descarte das informações armazenadas nas mídias de backup, respeitando os níveis de classificação atribuídos.

6.1.3 O backup das informações armazenadas nos servidores da rede corporativa deve ser realizado em horário de baixa utilização, sendo executado, preferencialmente, fora do horário de expediente.

6.1.4 As rotinas de backup, conforme elencado no item anterior 6.1.1, são de responsabilidade da área administradora dos recursos de tecnologia da informação do MinC.

6.1.5 A área administradora dos recursos de tecnologia da informação deverá documentar e manter atualizadas as rotinas de backup sob sua responsabilidade.

6.1.6 Devem constar nesses documentos, no mínimo:

a) tipo de mídia de armazenamento do *backup*, por exemplo, em fita ou em disco;
b) local de armazenamento de mídias;
c) período de retenção do *backup*;
d) tipo do *backup* – *full* (total), incremental e/ou diferencial;
e) periodicidade do *backup* – diária, semanal, mensal e/ou anual;
f) prazo de validade de mídias, conforme especificação do fornecedor;
g) procedimentos para substituição de mídias; e
h) procedimentos e periodicidade de testes de restauração de *backup*.

6.2 Os backups devem estar catalogados e rotulados de modo que seja possível aos técnicos internos do MinC identificar tempestivamente o conteúdo e a data do backup, considerando, no mínimo, as seguintes informações:

a) tipo do *backup* realizado;
b) número da mídia e quantidade de mídias utilizadas na realização do *backup*;
c) tipo do *backup* – full (total), incremental e/ou diferencial;
d) descrição dos locais ou serviços que foram copiados;
e) data de realização do *backup*;
f) versão e descrição do software utilizado para a realização do *backup*; e
g) tempo de retenção.

6.2.1 O procedimento visa facilitar a identificação em caso de demandas de restaurações.

6.3 As mídias utilizadas na realização de backups, feitas sob demanda, que extrapolem a rotina de backup, devem conter identificação diferenciada das demais mídias, acrescentando às informações descritas no item anterior o nome da área solicitante.

6.4 Os backups devem ser verificados logo após a sua geração e posteriormente deverão ser testados em intervalos regulares, visando garantir a restauração de dados em caso de eventuais perdas parciais ou totais.

6.4.1 Todos os testes de restauração de dados devem ser adequadamente documentados.

6.4.2 Restaurações de sistemas devem ser realizadas em máquina isolada da rede. Caso o sistema em questão tenha sido comprometido, é obrigatória a revisão de todas as configurações visando garantir o retorno correto do serviço.

6.4.3 A infraestrutura de backup corporativo deve ser configurada para ser adaptativa possibilitando possíveis ajustes de dimensionamento ou de implementação de novas tecnologias.

6.5 Os backups devem ser armazenados em locais seguros – interno e externo:

a) o acesso ao local deve ser restrito e monitorado;
b) o local deve ser protegido contra agentes nocivos naturais (poeira, calor, umidade);
c) o local deve ser protegido contra interferências eletromagnéticas; e
d) o local deve possuir controles de prevenção, detecção e combate a incêndio.

6.6 Os cofres para armazenamento das mídias de backup devem, preferencialmente, ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

a) certificação para resistência a fogo, de acordo com a norma CSN EN 1047-1;
b) certificação contra arrombamento, de acordo com a norma CSN EN 14450;
c) atender à norma Brasileira ABNT NBR 11515: 2007;
d) atender à CSN EN 1047-1, teste corta fogo que inclui porta e fechadura; e
e) certificação da ECB-S - *European Certification Bureau*, órgão independente de certificação de produtos de segurança em nível internacional, acreditado pelo *Dar- Deutschen Akkreditierungs Rat*, organismo creditador alemão, membro do IAF, que atesta a segurança dos cofres de segurança.

6.7 É recomendado que sejam realizadas duas cópias dos backups. Uma cópia para armazenamento em local externo/alterno e a outra para ser mantida em local interno visando, se for o caso, a rápida recuperação de dados.

6.8 Torna-se imprescindível à área responsável pela administração dos recursos de tecnologia da informação elaborar, documentar e implementar procedimentos que contemplem a retirada periódica de mídias de backup do local interno para o local externo.

6.9 Essas mídias devem ser transportadas em segurança ao local externo.

6.10 O transporte das mídias para local externo deve ser acompanhado por pessoa autorizada, considerando, minimamente, os seguintes elementos:

a) acondicionar mídias de *backup* em embalagem lacrada sem identificação do seu conteúdo;
b) transportar mídias de *backup* após registro e autorização.

6.11 Não é de responsabilidade da área responsável pela administração dos recursos de tecnologia da informação realizar cópias de segurança de arquivos pessoais.

6.12 Não é de responsabilidade da área administradora dos recursos de tecnologia da informação realizar cópias de segurança de arquivos armazenados em desktops e notebooks. Nestes casos, é de responsabilidade do próprio usuário a realização de backups dos dados armazenados em suas estações de trabalho.

6.13 O usuário deve armazenar dados corporativos nos diretórios de rede disponibilizados pela área administradora dos recursos de tecnologia da informação, onde ocorrem rotinas diárias de backup.

6.14 Solicitações de espaço em diretórios na rede MinC devem ser realizadas formalmente à área responsável.

6.15 Os usuários devem realizar manutenções periódicas nos diretórios de rede, visando evitar o acúmulo de informações desatualizadas e/ou desnecessárias ao órgão, buscando o melhor uso dos recursos computacionais do MinC.

6.16 Solicitações de restauração de backups, desde que estejam contemplados no item 6.1.1 deste documento, devem ser solicitadas formalmente junto à Central de Atendimento, para tanto, o usuário deve informar:

a) o diretório do servidor de arquivos, conta de *e-mail* ou sistema;
b) nome do(s) arquivo(s); e
c) data desejada para restauração – levando em conta que a área responsável pode restaurar dados com o status a partir das 18 horas do dia anterior e de no máximo 30 dias passados.

6.17 Em caso de indisponibilidade de atendimento de solicitações de backup ou de restauração de dados esta será informada com justificativa pela área responsável ao solicitante.

6.18 Sempre que surgir novos sistemas em ambientes de produção, obrigatoriamente, estes devem ser inseridos nas rotinas de backup.

6.19 A troca das mídias utilizadas para realização de backups deve respeitar os critérios definidos pelo fabricante e pela área responsável.

a) é recomendado que nos casos de substituição da solução de *backup* (*hardware* e *software*), as informações contidas nas mídias da antiga solução devem ser transferidas em sua totalidade para a nova solução ou, pelo menos, que a nova solução seja compatível para recuperação dos dados das mídias antigas;

b) caso a nova solução não seja compatível para recuperação dos dados das mídias antigas, a solução de *backup* obsoleta somente pode ser desativada após a certeza de que todas as informações foram transferidas para a nova solução implementada.

6.20 O descarte das mídias utilizadas para cópia de informações deve respeitar a temporalidade prevista na legislação, a política, as normas, os procedimentos de segurança internos e a classificação das informações.

a) o descarte das mídias que contiverem informações classificadas deve ser realizado de forma a impossibilitar sua recuperação total.

6.21 A coleta e o encaminhamento das mídias para o descarte devem ser previamente autorizados pela área responsável.

a) sempre que possível, o processo de descarte das mídias deve ser realizado por empresa especializada que utilize procedimentos seguros, tais como incineração, trituração e desmagnetização.

6.22 O transporte das mídias para descarte deve ser acompanhado por pessoa designada pela área responsável.

7. PENALIDADES

7.1 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.

8. COMPETÊNCIAS E RESPONSABILIDADES

8.1 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.

9. DISPOSIÇÕES GERAIS

9.1 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.

10. ATUALIZAÇÃO

10.1 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.

11. VIGÊNCIA

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