Ministério da Cultura (MinC)

Norma Interna de Segurança da Informação 03 (NISI 03)

Backup e Restauração de Dados Digitais

Brasília, fevereiro de 2024

Escopo

- Esta norma se aplica a todos os dados no âmbito do Ministério da Cultura (MinC), incluindo dados fora deste, armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem e-mail; arquivos pessoais e compartilhados; bancos de dados; códigos fonte de aplicações; logs de auditoria e sistemas operacionais.

- Os serviços de Tecnologia da Informação (TI) críticos do Ministério da Cultura (MinC) devem ser formalmente elencados pelo Comitê de Governança Digital e Segurança da Informação (CGDSI), criado e nomeado por portaria específica do MinC.

- Já ficam previamente estabelecidos os seguintes sistemas críticos do Ministério da Cultura (MinC):

Sistema	**Área MinC**	**Grau de Criticidade**
Sistema Nacional de Cultura	SCDC	7
Sistema Salic	SEFIC	7
Vale Cultura	SEFIC	7
Sistema Eletrônico de Informações (SEI)	SPOA	7
Mapa da Cultura	VÁRIAS	6
Rede Cultura Viva	SCDC	5
Conselho Nacional de Política Cultural	SCC	5
Mapa das Bibliotecas SNBP	SEFLI	5
Portal de Dados da Cultura	SECULT (NECESSÁRIO NOVO INVENTÁRIO)	4
Acervo CTAv	SAV	4
Revista Filme Cultura	SAV	2

Fonte: PDTIC 2023-2027 v.1.0

- Esta norma se aplica a agentes públicos que podem ser criadores e/ou usuários de tais dados. A norma também se aplica a terceiros que acessam e usam no Ministério da Cultura (MinC) sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do Ministério da Cultura (MinC).

Declarações da norma

Dos princípios gerais

I. A Norma de Backup e Restauração de Dados regulamenta as ações referentes à Cópia de Segurança (backup) e Restauração de Dados do Ministério da Cultura em atenção ao disposto no Art. 29º da Política de Segurança da Informação (POSIN).
II. A Norma de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível ministerial.
III. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo (RTO) possível, principalmente quando da indisponibilidade de serviços de TI.
IV. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
V. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos do ministério.
VI. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede do ministério para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
VII. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
VIII. O responsável pelo produto, sistema ou serviço deve solicitar formalmente a área de Tecnologia da Informação a inserção de dados ao sistema de backup, previamente a entrada em operação de tais soluções.
IX. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.
X. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do Ministério da Cultura (MinC) mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.
XI. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).
XII. Sob nenhuma hipótese uma mídia a ser descarta, antes da destruição física, pode ser doada ou armazenada com outros equipamentos do parque tecnológico.

CAPÍTULO I

DA FREQUÊNCIA, RETENÇÃO DOS DADOS E ESTRATÉGIA DE BACKUP

Art. 1º Os backups dos serviços de TI críticos do Ministério da Cultura devem ser realizados utilizando-se as seguintes frequências temporais:

I. Diária;
II. Semanal;
III. Mensal;
IV. Anual.

Art. 2º Os serviços de TI devem ser resguardados sob um padrão mínimo, o qual deve observar o estabelecido a seguir:

Criticidade do Serviço	Tipo	Frequência	Retenção	Janela de Backup	Local (is)

Críticos	Incremental /Diferencial	Diária	15 dias	Segunda à Quinta às 19:00	Storage/ Armazenamento primário
	Full/Completa	Semanal	30 dias	Sábado* às 00:10	Storage/ Armazenamento primário
	Full/Completa	Mensal	365 dias	Último domingo do Mês** por mês às 00:10	Storage/ Armazenamento primário Mídia Secundária/ Ambiente Externo
	Full/Completa	Anual	1825 dias	Último domingo do Ano** por mês às 00:10	Mídia Secundária/ Ambiente Externo
Não Críticos	Incremental /Diferencial	Diária	15 dias	Segunda à Quinta às 21:00	Storage/ Armazenamento primário
	Full/Completa	Mensal	60 dias	Domingo* às 00:10	Storage/ Armazenamento primário

* Exceto na sexta-feira que será realizada a cópia de segurança mensal

** Intervalo Mínimo de 25 dias entre as sextas-feiras que foram realizadas cópias mensais

Art. 3º Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 4º Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Art. 5º A solicitação de salvaguarda, por meio de um Plano de Backup e Restauração (ver ANEXO I), dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos é dever do Custodiante da Informação, cujo é responsável pelo produto, sistema ou serviço, com a anuência prévia e formal do Gestor de Tecnologia da Informação.

Art. 6º O Plano de Backup e Restauração deve refletir os requisitos de negócio do ministério, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I. Escopo (dados digitais a serem salvaguardados);
II. Tipo de backup (completo, incremental, diferencial);
III. Frequência temporal de realização do backup (diária, semanal, mensal, anual);
IV. Retenção;
V. *Recovery Point Objective* (RPO);
VI. *Recovery Time Objective* (RTO).

Art. 7º A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Custodiante da Informação. A aprovação para execução da alteração depende da anuência do Gestor de Tecnologia da Informação.

Art. 8º Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

CAPÍTULO II

DO USO DA REDE DE COMPUTADORES

Art. 9º A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 10º O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do Ministério da Cultura (MinC), garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI deste Ministério.

Art. 11º A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup. As “melhores práticas” apontam para realização do backup fora do horário de produção.

Art. 12º O período de janela de backup deve ser determinado pelo Administrador de Backup em conjunto com a área técnica responsável pela administração da rede de dados do Ministério da Cultura (MinC).

CAPÍTULO III

DO TRANSPORTE E ARMAZENAMENTO

Art. 13º As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I. A criticidade do dado salvaguardado;
II. O tempo de retenção do dado;
III. A probabilidade de necessidade de restauração;
IV. O tempo esperado para restauração;
V. O custo de aquisição da unidade de armazenamento de backup;
VI. A vida útil da unidade de armazenamento de backup.

Art. 14º O Administrador de Backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 15º Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

Art. 15º A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 17º No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo trinta (30) dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

Art. 18º As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

CAPÍTULO IV

DA VERIFICAÇÃO DAS IMAGENS DE BACKUP E DOS TESTES DE RESTAURAÇÃO DE DADOS

Art. 18º Os backups serão verificados periodicamente:

I. Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
II. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
III. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta norma.
IV. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

Art. 19º Os testes de restauração dos backups devem ser realizados, por amostragem uma vez por semana, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de

produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

Art. 20º Verificar se foi atendido os níveis de serviço pactuados, tais como os *Recovery Time Objective* (RTOs).

Art. 21º Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 22º O Administrador de Backup deve ser capacitado para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 23º São atribuições do Administrador de Backup:

I. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II. Definir a Janela de Backup em conjunto com a equipe de Infraestrutura Tecnológica;
III. Providenciar a criação e manutenção dos backups;
IV. Configurar as soluções de backup;
V. Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
VI. Definir os procedimentos de restauração e neles auxiliar;
VII. Solicitar o descarte de mídias de backup inservíveis ou inutilizáveis.

CAPÍTULO VI

DISPOSIÇÕES GERAIS

Art. 24º As auditorias ordinárias ou extraordinárias serão coordenadas pelo Gestor de Segurança da Informação e os relatórios serão encaminhados ao Comitê de Governança Digital e Segurança da Informação (CGDSI) e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Parágrafo Único. As auditorias extraordinárias deverão ser precedidas de autorização do Comitê de Governança Digital e Segurança da Informação.

Art. 25º O disposto na presente norma será atualizado sempre que alterados os procedimentos de backup, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação (POSIN) do Ministério da Cultura (MinC).

Art. 26º Quaisquer exceções à esta norma serão totalmente documentadas e aprovadas por Comitê de Governança Digital e Segurança da Informação (CGDSI).

Art. 27º Esta norma entra em vigor na data de sua publicação, observado o prazo de 180 (cento e oitenta) dias para adequação às disposições contidas neste documento.

ANEXO I

Procedimentos Relevantes

1) **Procedimento para transporte e armazenamento das unidades de armazenamento de backup**
    i. A mídia será claramente identificada e armazenada em uma área segura acessível apenas para o Administrador de Backup ou pessoas por ele autorizadas. Caso exista um fornecedor de armazenamento seguro de mídia externo contratado usado pelo Ministério da Cultura, aquele comunicará seus colaboradores autorizados.
    ii. A mídia não será deixada sem supervisão durante o transporte.
    iii. As mídias de backup, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.
    iv. A movimentação de mídias de backup deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a data e a hora da movimentação

2) **Procedimento de restauração de backup**

O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

    i. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos;
    ii. O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação;
    iii. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.
    iv. O Administrador de Backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.
    v. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

3) **Do Descarte da Mídia**

A mídia de backup será retirada e descartada conforme descrito neste documento:

    i. A partir da solicitação do Administrador de Backup.
    ii. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.
    iii. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

ANEXO II
PLANO DE BACKUP E RESTAURAÇÃO

* Itens mínimos necessários

** Itens já definidos na Norma. Necessário caso os parâmetros precisem ser diferentes.

1. ESCOPO/ABRANGÊNCIA*

<quais arquivos de dados ou de sistemas, quais bases de dados, quais tabelas, quais diretórios>

2. FREQUÊNCIA DE REALIZAÇÃO*

<diário, semana, mensal, anual>

3. TIPO DE CÓPIA A SER REALIZADA*

<completa/full, incremental ou diferencial>

4. TEMPO DE RETENÇÃO*

<Observar a correlação frequência/retenção de dados declarados na Norma>

5. Recovery Point Objective (RPO)*

6. Recovery Time Objective (RTO)*

7. UNIDADE DE ARMAZENAMENTO**

<informar mídia de armazenamento em local seguro diferente do local primário>

8. JANELA DE BACKUP**

<Informar período no qual a execução das cópias de segurança deverá ocorrer preferencialmente>

9. ESTRATÉGIA DE BACKUP**

<Detalhar o esquema de realização das cópias de segurança; informar quais tecnologias e equipamentos serão utilizados nesta estratégia; informar a capacidade necessária para os dados a serem copiados/armazenados>

8. PERIODICIDADE DE TESTE DE RESTAURAÇÃO**

<informar período regular de teste de restauração/recuperação (*restore*) das cópias de segurança>

9. PROCEDIMENTO DE TESTE DE RESTAURAÇÃO**

<Detalhas quais os procedimentos de teste de restauração/recuperação (*restore*) das cópias de segurança>

10. PROCEDIMENTO DE RESTAURAÇÃO**

<Quais os procedimentos para realizar a restauração/recuperação (*restore*) das cópias de segurança quando necessário.>