Boletim de Serviço Eletrônico em 05/01/2022

INSTITUTO BRASILEIRO DE MUSEUS

PORTARIA IBRAM Nº 910, DE 04 DE JANEIRO DE 2022

Dispõe sobre a fixação dos procedimentos próprios ao serviço de backup no âmbito do Ibram, para a Sede, Unidades Museológicas e Representações.

A PRESIDENTE SUBSTITUTA DO INSTITUTO BRASILEIRO DE MUSEUS - IBRAM, no uso das atribuições que lhe conferem o inciso IV do art. 20 do Anexo I ao Decreto nº 6.845, de 7 de maio de 2009, e tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, na Instrução Normativa GSI/PR nº1, de 27 de maio de 2020, na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, na Portaria GSI/PR nº 93, de 26 de setembro de 2019, e na Resolução Normativa Ibram nº 4, de 28 de julho de 2021, resolve:

Art.1º Fica instituída a Política de *Backup* e Recuperação de Dados Digitais no âmbito do Instituto Brasileiro de Museus – Ibram, que objetiva instituir diretrizes, responsabilidades e competências aptas a garantir a segurança, integridade e disponibilidade dos dados digitais custodiados pelo Ibram.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Seção I

Conceitos e definições

Art. 2º Para os fins desta Política, considera-se:

I - administrador de *backup*: pessoa ou equipe responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes e testes dos procedimentos de backup e restauração, devendo ser designado entre os servidores públicos ocupantes de cargo efetivo do Ibram, com formação ou capacitação técnica compatível a tais atribuições;

II - área técnica: unidade responsável pela operação técnica dos ativos e serviços de Tecnologia da Informação e Comunicações - TIC;

III - ativo: qualquer coisa que tenha valor para a organização;

IV - *backup* ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação, tendo fidelidade ao original assegurada; este termo também é utilizado para identificar a mídia em que a cópia é realizada;

V - *backup* completo - *Full*: modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente - cópia de segurança completa - para uma unidade de

armazenamento, independentemente de terem sido ou não alterados desde o último *backup*;

VI - *backup* diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;

VII - *backup* incremental: modalidade de *backup* na qual somente os arquivos novos ou modificados desde o último *backup* – seja ele completo, diferencial ou incremental – são salvaguardados;

VIII - base de dados ou banco de dados: base de dados ou coleção de dados inter-relacionados, armazenando informações sobre um domínio específico; são conjuntos de registros organizados que se relacionam de forma a criar algum sentido - informação, e dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

IX - código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica;

X - comitê de Governança Digital – CGD: Comitê do tipo estratégico-executivo, de natureza Consultiva e deliberativa, com a finalidade de estabelecer políticas e diretrizes para a integração dos sistemas que compõem a plataforma operacional, assim como promover o alinhamento da área de negócio com a área de TIC, em consonância com as ações do Poder Executivo Federal; no âmbito do Ibram, o CGD exerce ainda as funções estabelecidas para o Comitê Gestor de Segurança da Informação e Comunicação – CGSIC, com a responsabilidade de assessorar a implementação das ações de segurança da informação;

XI - computação em nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços;

XII - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados ou credenciados;

XIII - criticidade: grau de importância da informação para a continuidade das atividades e serviços;

XIV - custódia: consiste na responsabilidade de se guardar um ativo para terceiros; a custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

XV - dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XVI - descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais;

XVII - disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa ou entidade devidamente autorizada;

XVIII - escopo: informações dos dados digitais a serem salvaguardados, com apontamento do local;

XIX - gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XX - gestor da informação: agente público formalmente responsável pela administração do serviço de TIC/sistema e pelas informações produzidas em seu processo de trabalho, devendo ser um gestor da área negocial;

XXI - janela de *backup*: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;

XVII - log ou Registro de Auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional, para posterior análise, podendo ser gerado por sistemas operacionais, aplicações, entre outros;

XXIII - operador de *backup*: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup e realização de restaurações de arquivos de usuários, devendo ser designado entre os servidores públicos ou terceirizados do Ibram com formação ou capacitação técnica compatível às suas atribuições;

XXIV - plano de b*ackup*: documento formal onde são definidos os dados que serão armazenados, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de *backup*;

XXV - repositório de arquivo: conjunto de documentos ou lugar onde os documentos são guardados; e

XXVI - retenção: período em que o dado copiado no *backup* ficará retido e disponível para uso numa eventual recuperação antes de ser substituído por uma versão mais nova.

Seção II

Escopo

Art. 3º Todos os sistemas, bases de dados e repositórios de arquivos institucionais em formato digital em uso e de propriedade do Ibram, no âmbito da sede, escritórios de representação e unidades museológicas, deverão ser considerados para avaliação de inclusão no processo de *backup*.

Parágrafo único. 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 pela Coordenação de Tecnologia da informação – CTINF/Ibram, ou que não façam parte de um plano de *backup* formalmente definido, cabendo ao CGD a prerrogativa de deliberar sobre solicitações neste sentido.

Art. 4º Para todos os sistemas, bases de dados e repositórios de arquivos institucionais em uso deve haver um plano de *backup*, conforme modelo em anexo, devidamente assinado pelo gestor da informação, pelo titular da CTINF/Ibram e pelo administrador de *backups.*

Art. 5º A salvaguarda dos dados em formato digital pertencentes a serviços de TIC do Ibram, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, devem estar garantidos nos acordos ou contratos que formalizam a relação entre os envolvidos.

CAPÍTULO II

DOS PADRÕES OPERACIONAIS

Seção I

Dos princípios gerais

Art. 6º A Política de *backup* e recuperação de dados digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional, devidamente amparados nas estratégias de governança de TIC do Ibram.

Art. 7º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TIC.

Art. 8º As rotinas de *backup* devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da

organização.

Parágrafo único. Para mensurar a criticidade de um serviço, sugere-se a utilização de matriz de risco que considera a probabilidade versus o impacto.

Art. 9º O CGD deverá aprovar lista de sistemas com a designação do respectivo gestor da informação e sua classificação quanto à criticidade, críticos e não críticos.

Art. 10. Os *backups* devem estar em conformidade com a legislação vigente, em especial à Lei Geral de Proteção de Dados - LGPD.

Art. 11. Recomenda-se que os *backups* sejam armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Seção II

Das ferramentas de *backup*

Art. 12. As rotinas de *backup* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 13. Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização.

Parágrafo único. Compete à CTINF/Ibram realizar o planejamento das contratações para aquisição de equipamentos ou soluções/serviços relacionados ao *backup*, sendo imprescindível o apoio da alta administração, mediante a disponibilização de recursos orçamentários e humanos para a área de TIC.

Art. 14. Os *backups* dos serviços de TIC devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal; e

IV - anual.

Art. 15. Especificidades dos serviços de TIC críticos e não críticos podem demandar frequência e tempo de retenção diferenciados, que devem estar devidamente registrados no plano de *backup* do sistema, base de dados e repositório de arquivos.

Art. 16. A solicitação de salvaguarda dos dados referentes aos serviços de TIC críticos e aos serviços não críticos deve ser realizada pelos responsáveis técnicos dos serviços de TIC, com a anuência prévia e formal dos gestores das informações, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo:

a) código fonte;

b) banco de dados;

c) repositório de arquivos;

d) arquivos de configuração de servidores e ativos de rede; e

e) máquinas virtuais.

II - tipo de *backup:* completo, incremental, diferencial, podendo ser uma associação destes;

III - frequência temporal de realização do *backup:* diária, semanal, mensal, anual, podendo ser uma associação destes;

IV - retenção que deverá ser definida com base na criticidade, frequência da atualização dos dados e características específicas de cada sistema;

V - RPO - *recovery point objective*: indicador que limita o período de volta no tempo, e define a quantidade máxima tolerada de dados perdidos de uma ocorrência de falha para o último *backup* válido; e

VI - RTO - *recovery time objective*: indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente.

Art. 17. Os *backups* podem ser classificados como on-line ou off-site, a depender da forma de acesso ao backup realizado, da seguinte forma:

I - on-line: uma vez realizado, o *backup* é acessível dentro da rede do Ibram; e

II - off-site: uma vez realizado, o *backup* é armazenado em outro data center, geograficamente separado, ou em serviço de backup em nuvem.

Art. 18. Recomenda-se, se possível, que os *backups* dos sistemas críticos tenham no mínimo duas cópias sendo um on-line e outro off-site.

Art. 19. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Parágrafo Único. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de *backup*.

Art. 20. Legislações e normas vigentes sobre o período de armazenamento de dados deverão ser observadas em razão de especificidades que podem exigir o armazenamento de *backups* por longos períodos ou até mesmo de forma vitalícia.

Seção III

Do uso da rede

Art. 21. O administrador de *backup* deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados do Ibram, garantindo que o tráfego necessário às suas atividades não ocasione problemas aos demais serviços de TIC.

Art. 22. A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de backup, definido por cada gestor da informação.

Art. 23. Deve ser observada a possibilidade de *backup*, utilizando dispositivo de armazenamento remoto, a exemplo do serviço em nuvem.

Seção IV

Das unidades de armazenamento de *backups*

Art. 24. 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*; e

VI - a vida útil da unidade de armazenamento de *backup.*

Art. 25. 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. 26. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

Art. 27. Todos os ativos relacionados ao armazenamento dos *backups* devem ser acondicionados em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de *backup.*

Art. 28. Quando da necessidade de descarte de unidades de armazenamento de *backups*, quando e se aplicável, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Seção V

Dos testes de *backup*

Art. 29. Os *backups* devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados a fim de detectar eventuais falhas lógicas e físicas.

Art. 30. Os testes de restauração dos *backups*, se possível, devem ser realizados em servidores diferentes dos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 31. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* devem ser devidamente registradas no plano de *backup*.

CAPÍTULO III

DAS RESPONSABILIDADES

Art. 32. O administrador de *backup* e o operador de *backup* devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de armazenamento e *backup*.

Art. 33. O administrador de *backup* deverá ser indicado pelo Diretor do Departamento de Planejamento e Gestão Interna – DPGI/Ibram, e o operador de *backup* deve ser indicado pelo administrador de *backup.*

Art. 34. São atribuições do administrador de *backup*:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo Ibram;

II - providenciar a criação e manutenção dos *backups*;

III - configurar as soluções de *backup;*

IV - manter as unidades de armazenamento de *backups* preservadas, funcionais e seguras;

V - definir os procedimentos de restauração e neles auxiliar;

VI - verificar os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;

VII - tomar medidas preventivas para evitar falhas;

VIII - reportar imediatamente ao CGD incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*;

IX - gerenciar mensagens e registros de auditoria e logs de execução dos *backups*;

X - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos *backups*;

XI - propor modificações visando ao aperfeiçoamento da política de *backup* e recuperação de dados digitais; e

XII - coordenar a execução dos testes de restauração e analisar os relatórios de execução.

Art. 35. São atribuições do operador de *backup*:

I - aplicar o plano de b*ackup* na estrutura de *backup* existente;

II - restaurar ou recuperar os *backups* em caso de necessidade;

III - operar e manusear as unidades de armazenamento de *backups*;

IV - informar ao administrador de *backup* qualquer problema que impossibilite a criação ou restauração de um *backup*; e

V - executar os testes de restauração de *backup*.

Art. 36. São atribuições da CTINF/Ibram:

I - solicitar restaurações de dados, com anuência do gestor da informação;

II - sanar dúvidas técnicas do administrador de *backup* acerca das informações salvaguardadas;

III - validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;

IV - validar, tecnicamente, o resultado dos testes de restauração dos *backups*; e

V - verificar periodicamente se as definições do plano de *backup* estão devidamente configuradas na estrutura de backup vigente.

Art. 37. São atribuições dos gestores da informação:

I - solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;

II - validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e

III - validar, negocialmente, o resultado dos testes de restauração dos *backups.*

Art. 38. A solicitação de restauração de dados que tenham sido salvaguardados deve ser realizada por meio da abertura de chamado técnico, e depende de prévia e formal autorização do respectivo gestor da informação.

Art. 39. O CGD será responsável pela aprovação dos planos de *backup* elaborados com base nas especificidades indicadas pelos gestores da informação considerando as criticidades diferentes dos sistemas.

Art. 40. Caberá também ao CGD o acompanhamento da realização das metas estabelecidas na Política.

CAPÍTULO IV

DAS METAS

Art. 41. As unidades do Ibram terão como metas iniciais os seguintes prazos:

I - até 3 (três) meses após a publicação desta Política para elaborar lista de sistemas com classificação quanto a criticidade (críticos e não críticos), encaminhando-a para aprovação do CGD;

II - até 6 (seis) meses após a publicação desta Política para elaborar 100% dos planos de *backup* dos serviços críticos de TIC;

III - até 12 (doze) meses após a publicação desta Política para providenciar a implementação de todos os planos de *backup* dos serviços críticos de TIC;

IV - até 12 (doze) meses após a publicação desta Política, para elaborar 100% dos planos de *backup* dos serviços não críticos de TIC; e

V - até 18 (dezoito) meses após a publicação desta Política, para providenciar a implementação de todos os planos de *backup* dos serviços não críticos de TIC.

Art. 42. A lista de sistemas e os planos de *backup* deverão ser atualizados sempre que necessário e revisados no mínimo a cada 12 (doze) meses.

Art. 43. Os planos de *backup* de novos sistemas, que surgirem após a elaboração da listagem inicial de sistemas, devem ser implementados em até 6 meses.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 44. O tratamento de dados pessoais será disciplinado em instrumento distinto.

Art. 45. Esta política deverá ser amplamente divulgada no âmbito do Ibram.

Art. 46. Esta Política poderá ser revisada pelo CGD a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 47. Os casos omissos serão dirimidos pelo CGD, que poderá expedir normas complementares, bem como disponibilizar em meio eletrônico informações adicionais.

Art. 48. Esta Portaria entra em vigor em 1º de fevereiro de 2022.

Documento assinado eletronicamente por **Carla Janne Farias Cruz**, **Presidente do Instituto Brasileiro de Museus, Substituto(a)**, em 05/01/2022, às 18:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.museus.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1504678** e o código CRC **D8EAE0A2**.

ANEXO I

PLANO DE *BACKUP*

O plano de *backup* deverá ser apresentado por Departamento, Escritório de Representação e Unidade Museológica sob responsabilidade de elaboração pelos respectivos Gestores da Informação, via processo SEI, e submetidos para aprovação do Comitê de Governança Digital que deverá aprovar lista de sistemas e bases para *backup*.

Unidade:	Informar Coordenação Geral, Departamento, Escritório de Representação ou Unidade Museológica
Escopo	

Descrição Informar e especificar quais arquivos de dados ou sistemas, bases de dados, tabelas, pastas/folders deverão ter *backup*. *(inserir uma linha para cada ocorrência)*	**Gestor da Informação** Identificar o gestor da informação responsável.	**Frequência de Realização**	**Tipo de cópia** Completa, incremental ou diferencial	**Janela de *Backup*** informar o dia da semana e horário que preferencialmente deverá ser executado o *backup*.	**Tempo de retenção** Prazo em que os *backups* devem ser mantidos.	**Quantidade de cópias** Número de cópias de *backup*, locais e meios de armazenamento.
(inserir uma linha para cada ocorrência)						
(inserir uma linha para cada ocorrência)						
(inserir uma linha para cada ocorrência)						
(inserir uma linha para cada ocorrência)						

Unidade de armazenamento Informar mídia de armazenamento em local seguro diferente do local original.	**Estratégia de *Backup*** Detalhar o esquema de realização das cópias de segurança: - Informar quais tecnologias e equipamentos será utilizado neste esquema; - Informar a capacidade necessária para os dados a serem copiados/armazenados; - Informar quando deve ser agendada a geração de *backups*; - Informar os responsáveis pela execução e acompanhamento. - considerar requisitos relativos à confidencialidade, à integridade e à disponibilidade das informação	**Procedimento de testes de restauração** Informar período regular de teste de restauração/recuperação *(*restore) das cópias de segurança.	**Procedimento de restauração** Detalhar quais os procedimentos de teste de recuperação/restauração (*restore*) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento). Detalhar quais os procedimentos para realizar a recuperação/restauração (*restore*) das cópias de segurança quando necessário (ou seja, o ”como” recuperar os *backups*).
Operador de *Backup*:		*Preenchimento CTINF*	
Monitoramento dos logs da execução da geração de cópias de segurança Evidência do monitoramento e da execução do procedimento de geração das cópias de segurança, por meio de registros (logs) relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança.	**Monitoramento dos logs da execução execução dos procedimentos de teste de recuperação/restauração (restore) das cópias de segurança**	**Local de armazenamento do backup** Local seguro e em local remoto seguro diferente do local original	
Administrador *Backup*:		*Preenchimento CTINF*	