DIRETRIZES
PARA IMPLEMENTAÇÃO DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS – RDC-ARQ

RESOLUÇÃO CONARQ Nº 51, DE 25 DE AGOSTO DE 2023

Conarq
CONSELHO NACIONAL DE ARQUIVOS

Conarq
CONSELHO NACIONAL DE ARQUIVOS

Diretrizes para implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq)

Versão 2
Rio de Janeiro | 2023

Praça da República, 173 | Rio de Janeiro | RJ | 20211-350
e-mail: conarq@an.gov.br

Presidente da República
Luiz Inácio Lula da Silva

Ministra da Gestão e Inovação em Serviços Públicos
Esther Dweck

Presidente do Conselho Nacional de Arquivos
Ana Flávia Magalhães Pinto

Secretário executivo do Conselho Nacional de Arquivos
Alex Pereira de Holanda

Diretora de Processamento Técnico, Preservação e Acesso ao Acervo
Diana Santos Souza

Coordenadora-geral de Acesso e Difusão Documental
Daiana Ribeiro Dantas Martins

Coordenadora de Pesquisa e Difusão do Acervo
Leticia dos Santos Grativol

Revisão de texto
Mariana Simões

Diagramação e ilustração da capa
Alzira Reis

Projeto gráfico da capa
Mariana Machado Laplace

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Maria Beatriz Nascimento – Arquivo Nacional)

Conselho Nacional de Arquivos (Brasil)
Diretrizes para implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq). [recurso eletrônico] / Câmara Técnica Consultiva – Certificação de Repositórios Arquivísticos Digitais Confiáveis. 2. versão. – Dados eletrônicos (1 arquivo : 649 KB). – Rio de Janeiro : Arquivo Nacional, 2023.

Formato: PDF
Requisitos do sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
ISBN: 978-85-7009-024-9

1. Repositórios arquivísticos digitais. 2. Gestão Arquivística de Documentos. 3. Sistemas informatizados. I. Título.

CDD 025.04

Ficha catalográfica elaborada por Dayo de Araújo Silva Côrbo (CRB 7/5633)

EQUIPE TÉCNICA DE ELABORAÇÃO

2ª versão

Câmara Técnica Consultiva – Certificação de Repositórios Arquivísticos Digitais Confiáveis

Alex Pereira de Holanda
Carlos Eduardo Carvalho Amand
Eloi Juniti Yamaoka
Vanderlei Batista dos Santos
Wilson Roberto Hirata

Colaboração

Érika Maria Nunes Sampaio
Rodrigo Uchôa Cavalcanti de Araújo

1ª Versão

Equipe de redação da Câmara Técnica de Documentos Eletrônicos

Carlos Augusto Silva Ditadi
Claudia Lacombe Rocha
Eloi Juniti Yamaoka
Humberto Celeste Innarelli
João Alberto de Oliveira Lima
Luis Fernando Sayão
Neire do Rossio Martins
Rosely Curi Rondinelli

Integrantes da Câmara Técnica de Documentos Eletrônicos que participaram deste trabalho

Brenda Couto de Brito Rocco | Arquivo Nacional
Carlos Augusto Silva Ditadi | Arquivo Nacional
Carolina de Oliveira | Arquivo Nacional – a partir de 2012
Claudia Lacombe Rocha | Arquivo Nacional
Daniel Flores | Universidade Federal de Santa Maria
Eloi Juniti Yamaoka | Serviço Federal de Processamento de Dados
Humberto Celeste Innarelli | Universidade Estadual de Campinas
João Alberto de Oliveira Lima | Senado Federal
Luis Fernando Sayão | Comissão Nacional de Energia Nuclear
Marco Aurélio Rodrigues Braga | Secretaria de Logística e Tecnologia da Informação – a partir de 2013
Margareth da Silva | Universidade Federal Fluminense
Neire do Rossio Martins | Universidade Estadual de Campinas
Rosely Curi Rondinelli | Fundação Casa de Rui Barbosa
Vanderlei Batista dos Santos | Câmara dos Deputados

Colaboração

Andressa Cristiani Piconi | Universidade Estadual de Campinas
Cássia de Paula Moreira Coghi | Universidade Estadual de Campinas

Revisão

José Márcio Batista Rangel

SUMÁRIO

I APRESENTAÇÃO

Os documentos arquivísticos caracterizam-se por registrarem e apoiarem as atividades do órgão ou entidade, servindo de evidência dessas atividades, bem como de fonte de informação para a pesquisa e para assegurar os direitos dos cidadãos. Assim, é preciso garantir que os documentos sejam acessíveis e permaneçam autênticos em todo o seu ciclo de vida. A produção crescente de documentos arquivísticos em formato digital desafia as organizações produtoras e as instituições de preservação na busca de soluções para a preservação e o acesso de longo prazo. Os documentos digitais sofrem diversas ameaças decorrentes da fragilidade inerente aos objetos digitais, da facilidade de adulteração e da rápida obsolescência tecnológica.

Os documentos arquivísticos digitais em fases corrente e intermediária devem, preferencialmente, ser gerenciados por meio de um sistema informatizado de gestão arquivística de documentos (Sigad),[1] a fim de a ssegurar o controle do ciclo de vida, o cumprimento da destinação prevista e a manutenção da autenticidade e da relação orgânica,[2] características fundamentais desses documentos. Já nessas fases, os produtores precisam tomar cuidados especiais, previstos em um plano de preservação digital, com relação aos documentos digitais que serão mantidos por médio e longo prazos, de forma a garantir sua autenticidade e seu acesso.

A partir da destinação para guarda permanente, pode ocorrer uma alteração na cadeia de custódia, passando a responsabilidade pela preservação dos documentos dos produtores para uma instância de guarda externa, qual seja, o arquivo público na sua esfera de competência. Os documentos digitais em fase permanente dependem de um bom sistema informatizado que apoie o tratamento técnico adequado, incluindo arranjo, descrição e acesso, de forma a assegurar a manutenção da autenticidade e da relação orgânica desses documentos.

---

1 É um conjunto de procedimentos e operações técnicas, característico do sistema de gestão arquivística de documentos, processado por computador. Pode compreender um software em particular, um determinado número de softwares integrados, adquiridos ou desenvolvidos por encomenda, ou uma combinação destes.

2 Quando os documentos arquivísticos são produzidos e mantidos dentro de um sistema informatizado (por exemplo, sistemas de controle acadêmico em instituições de ensino, sistemas de prontuários médicos, sistemas de controle de ponto), esse sistema deve incorporar as funcionalidades básicas de um Sigad previstas no e-ARQ Brasil, para assegurar tais objetivos.

A preservação dos documentos arquivísticos digitais arquivados nas fases corrente, intermediária e permanente deve estar associada a um repositório arquivístico digital confiável, ou seja, deve ocorrer em todo o ciclo vital do documento.

No contexto internacional, algumas iniciativas indicam a importância do desenvolvimento de repositórios digitais confiáveis como solução para a garantia da autenticidade, da preservação e do acesso de longo prazo. Dentre essas iniciativas, destaca-se a do grupo de trabalho liderado pelo Research Library Group (RLG) e pelo Online Computer Library Center (OCLC).[3] Na perspectiva do grupo de trabalho RLG/OCLC, um "repositório digital confiável é aquele que tem como missão oferecer, à sua comunidade-alvo, acesso confiável e de longo prazo aos recursos digitais por ele gerenciados, agora e no futuro" (RLG/OCLC, 2002, p. 5, tradução nossa).[4]

O arquivamento e a preservação digital constituem uma questão complexa que envolve muitas variáveis, compromissos de longa duração e a necessidade de expressivos investimentos em infraestrutura tecnológica, pesquisa e recursos humanos. Diante disso, a formação de consórcios, em determinados casos, pode ser a solução mais viável.

Assim, em face da necessidade de implantação de repositórios digitais confiáveis para documentos arquivísticos digitais, nas fases corrente,[5] intermediária e permanente, o Conarq apresenta esta atualização das diretrizes de repositórios arquivísticos digitais confiáveis (RDC-Arq).

I.1 Objetivo deste documento

Indicar parâmetros e requisitos para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos ou, até mesmo, permanentemente.

I.2 Escopo

Estas diretrizes visam a orientar os órgãos e as entidades integrantes do Sistema Nacional de Arquivos (Sinar) na implantação de repositórios digitais confiáveis para documentos arquivísticos digitais.

---

3 Desde junho de 2006, o RLG e o OCLC estão reunidos em uma única organização. Para mais informações, veja o sítio: http://www.oclc.org/.

4 "A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future".

5 Documentos poderão ser arquivados na fase corrente quando for assim definido, por meio de marcação específica no sistema, observadas as regras estabelecidas pelo programa de gestão de documentos ou regras da instituição.

São integrantes do Sinar:[6]

- Arquivo Nacional;
- arquivos do Poder Executivo Federal;
- arquivos do Poder Legislativo Federal;
- arquivos do Poder Judiciário Federal;
- arquivos estaduais dos poderes Executivo, Legislativo e Judiciário;
- arquivos do Distrito Federal dos poderes Executivo, Legislativo e Judiciário; e
- arquivos municipais dos poderes Executivo e Legislativo.

Podem, ainda, integrar o Sinar pessoas físicas e jurídicas de direito privado detentoras de arquivos, mediante convênio com o órgão central.

Além de parâmetros tecnológicos e de infraestrutura, as diretrizes aqui apresentadas tratam também de políticas e procedimentos técnicos e administrativos. Os parâmetros indicados atendem às necessidades de repositórios digitais confiáveis para o armazenamento de documentos arquivados nas fases corrente, intermediária e permanente.

I.3 Definições[7]

Apresentam-se, aqui, definições importantes no contexto deste documento.

Atualização de suporte

Técnica de migração que consiste em copiar os dados de um suporte para outro, sem mudar sua codificação, para evitar perdas de dados provocadas por deterioração do suporte.

Autenticidade

Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e de que está livre de adulteração ou qualquer outro tipo de corrupção.

Ciclo vital dos documentos

Sucessivas fases por que passam os documentos arquivísticos, de sua produção a guarda permanente ou eliminação.

---

6 De acordo com o decreto n. 4.073, de 3 de janeiro de 2002, que regulamenta a lei n. 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

7 As definições aqui apresentadas foram baseadas nos glossários dos seguintes documentos: e-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (Câmara Técnica de Documentos Eletrônicos, CTDE. Versão adotada pelo Conarq em dezembro de 2009); Glossário da CTDE/Conarq; Resolução GR – Unicamp n. 17/2011, de 29 de junho de 2011; ABNT 27001/2006 – Requisitos para sistemas de gestão de segurança da informação; Diretrizes do preservador – A preservação de documentos arquivísticos digitais: Diretrizes para organizações (Projeto InterPARES 2); ISO 14721/2003 – Reference Model for an Open Archival Information System (OAIS).

Confiabilidade

Credibilidade de um documento arquivístico enquanto afirmação de um fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza, da forma do documento e do grau de controle exercido no seu processo de criação.

Confidencialidade

Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização.

Conversão de formato

Modificação de um formato para outro motivada, principalmente, pela normalização de formatos e para contornar a obsolescência tecnológica.

Disponibilidade

Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Documento arquivístico

Documento produzido (elaborado ou recebido) no curso de uma atividade prática, como instrumento ou resultado dessa atividade, e retido para ação ou referência.

Documento arquivístico digital

Documento digital reconhecido e tratado como documento arquivístico.

Documento digital

Informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.

Evidência

Documentos que comprovem o cumprimento de requisitos, competências, objetivos e responsabilidades.

Integridade

Estado dos documentos que se encontram completos e não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada.

Interoperabilidade

Capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar), de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente.

Metadados

Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo.

Migração

Conjunto de procedimentos e técnicas para assegurar a capacidade de os objetos digitais serem acessados face às mudanças tecnológicas. A migração consiste na transferência de um objeto digital: a) de um suporte que está se tornando obsoleto, fisicamente deteriorado ou instável para um suporte mais novo; b) de um formato obsoleto para um formato mais atual ou padronizado; c) de uma plataforma computacional em vias de descontinuidade para outra mais atual. A migração pode ocorrer por conversão, atualização ou reformatação.

Modelo de referência

Uma estrutura conceitual para compreensão dos principais relacionamentos entre as entidades de um ambiente e para o desenvolvimento de padrões consistentes ou especificações que consolidam esse ambiente. Um modelo de referência é baseado em pequena quantidade de conceitos unificados e pode ser usado como base para aprendizado e explanação de padrões para não especialistas.

Normalização de formatos

Conversão de formatos de arquivo para um elenco gerenciável de formatos apropriados para preservação e acesso.

Plano de preservação

Uma declaração por escrito, autorizada pela gestão do repositório, que descreve as ações a serem executadas para preservar objetos por ele custodiados de acordo com a política de preservação.

Política de acesso

Declaração escrita, autorizada pela gestão do repositório, que descreve a abordagem a ser adotada para a comunidade designada e usuários em geral.

Política de preservação digital

Declaração escrita, autorizada pela gestão do repositório, que descreve a abordagem a ser adotada pelo repositório para a preservação dos objetos por ele custodiados. A política de preservação é consistente com o plano estratégico de preservação.

Prática

Ação realizada para executar procedimentos. As práticas são medidas por registros (logs) ou outras evidências que registrem ações concluídas.

Preservação digital

Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação dos documentos digitais pelo tempo que for necessário.

Preservador de documentos arquivísticos

Entidade responsável pela custódia física e legal dos documentos do produtor, bem como por sua preservação, isto é, por proteger e garantir acesso contínuo aos documentos.

Procedimento

Uma declaração por escrito que especifica as ações necessárias para se concluir um serviço ou para atingir um estado ou condição específica. Os procedimentos especificam como vários aspectos relativos aos planos de preservação devem ser cumpridos.

Provedor

Uma pessoa ou sistema que envia um objeto digital para o repositório. O provedor pode ser o produtor.

Reformatação

Técnica de migração que consiste na mudança da forma de apresentação de um documento para fins de acesso ou manutenção dos dados.

Sistema informatizado de gestão arquivística de documentos (Sigad)

Conjunto de procedimentos e operações técnicas característico do sistema de gestão arquivística de documentos, processado eletronicamente e aplicável em ambientes digitais ou híbridos, isto é, em que existem documentos digitais e não digitais ao mesmo tempo.

II REPOSITÓRIO DIGITAL CONFIÁVEL DE DOCUMENTOS ARQUIVÍSTICOS – PRINCIPAIS REQUISITOS

Desde a década de 1990, a comunidade internacional tem desenvolvido iniciativas no sentido de orientar a modelagem e implementação de repositórios digitais, e de apontar os requisitos para se atribuir confiabilidade a esses repositórios. A implantação de um repositório digital confiável é fundamental para assegurar a preservação, o acesso e a autenticidade de longo prazo dos materiais digitais.

A norma mais importante da área é o Open Archival Information System (OAIS),[8] um modelo conceitual desenvolvido pelo Consultive Committee for Space Data Systems (CCSDS),[9] que resultou na norma ISO 14721:2003 (revisada em 2012). O OAIS descreve as funções de um repositório digital e os metadados necessários para a preservação e o acesso aos materiais digitais gerenciados pelo repositório, que constituem um modelo funcional e um modelo de informação.

A preocupação com a confiabilidade dos repositórios digitais foi evidenciada no relatório da Task Force on Archiving of Digital Information,[10] uma ação cooperativa do RLG e da Commission on Preservation and Access, publicado em 1996, no qual se declarou que "um componente crítico da infraestrutura de arquivamento digital é a existência de um número suficiente de instituições confiáveis, que sejam capazes de armazenar, migrar e prover acesso a acervos digitais".[11] O relatório da Task Force foi mais além, ao apontar a necessidade de um processo de certificação dos repositórios digitais para atribuir esse caráter de confiabilidade de uma forma mais isenta.

Esse relatório estimulou a colaboração do RLG/OCLC, iniciada em março de 2000, no sentido de definir as bases conceituais e os principais atributos para um repositório digital confiável. Como resultado, foi publicado, em 2002, o relatório *Trusted digital repositories: attributes and responsibilities*.

Em continuidade a esse trabalho, o RLG estabeleceu uma parceria com a administração nacional dos arquivos dos Estados Unidos (National Archives and Records Administration, NARA), com o objetivo de definir critérios para a certificação de repositórios confiáveis, em sintonia com os resultados apontados no relatório RLG/OCLC, de 2002, e com o modelo OAIS. Assim, foi publicado, em 2007, o documento *Trustworthy repository audit & certification: criteria and checklist*, mais conhecido pela sigla TRAC,[12] que apresenta um conjunto de critérios e um checklist a serem tomados como referência para a certificação de repositórios digitais confiáveis. Esse documento serviu de base para a elaboração da norma ISO 16363:2012, que

---

8 No Brasil, o modelo OAIS foi traduzido pela ABNT e publicado sob a forma da norma ABNT NBR 15472:2007, com o título Sistema Aberto de Arquivamento de Informação (SAAI).

9 Comitê formado pelas maiores agências espaciais do mundo, com o objetivo de oferecer um fórum para discussão de problemas comuns sobre o desenvolvimento e a operação de sistemas de dados espaciais.

10 *Preserving digital information, report of the Task Force on Archiving of Digital Information*. Maio de 1996. Disponível em: http://www.oclc.org/content/dam/research/activities/digpress-tudy/final-report.pdf?urlm=161430.

11 Texto no original em inglês: "*a critical component of digital archiving infrastructure is the existence of a sufficient number of trusted organizations capable of storing, migrating and providing access to digital collections*".

12 Disponível em: https://www.dcc.ac.uk/resources/repository-audit-and-assessment/trustworthy-repositories.

lista os critérios que um repositório digital confiável deve atender. Paralelamente a essa iniciativa, desenvolveu-se a norma ISO 16919,[13] que estabelece requisitos para entidades certificadoras de repositórios digitais confiáveis.

Esses documentos apontam as diretrizes para repositórios digitais confiáveis e fundamentaram a elaboração deste trabalho. Inicialmente, faz-se necessário esclarecer os conceitos de "repositório digital", "repositório arquivístico digital" e "repositório digital confiável".

No contexto deste documento, **repositório digital** é um ambiente de armazenamento e gerenciamento de materiais digitais. Esse ambiente não se constitui apenas de uma solução informatizada em que os materiais são capturados, armazenados, preservados e acessados. Um repositório digital é, então, um complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos. Tal ambiente tem sido empregado em diversas situações, tais como:

- arquivo corrente (em associação com um Sigad);[14]
- arquivo intermediário (em associação com um Sigad);
- arquivo permanente;
- biblioteca digital;
- acervo de obras de arte digitais;
- depósito legal de material digital; e
- curadoria de dados digitais de pesquisa.

ATENÇÃO: Um repositório digital não se resume a uma solução informatizada para armazenamento (storage), que é apenas um dos componentes do repositório.Vivius apero esulocrem

Um **repositório arquivístico digital** é um repositório digital que armazena e preserva esses documentos, nas fases intermediária e/ou permanente. Como tal, esse repositório deve:

- gerenciar os documentos e metadados de acordo com as práticas e normas da arquivologia, especificamente relacionadas a gestão documental, descrição arquivística multinível e preservação; e
- proteger as características do documento arquivístico, em especial a autenticidade (identidade e integridade) e a relação orgânica entre os documentos.

13 Disponível em: https://www.iso.org/standard/57950.html.

14 Para um melhor entendimento sobre a implantação de RDC-Arq integrado ao Sigad, ver a orientação técnica n. 3 do Conarq, de novembro de 2015. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/Orientacao_tecnica_3.pdf.

ATENÇÃO: Um repositório arquivístico digital não se destina a ser o ambiente de gestão de documentos, para tal deve-se usar um Sigad.

Um **repositório digital confiável** é um repositório digital capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário. Para cumprir essa missão, segundo o relatório *Trusted digital repositories: attributes and responsibilities* (RLG/OCLC, 2002), os repositórios digitais confiáveis devem:

- aceitar, em nome de seus depositantes, a responsabilidade pela manutenção dos materiais digitais;
- dispor de uma estrutura organizacional que apoie não somente a viabilidade de longo prazo dos próprios repositórios, mas também dos materiais digitais sob sua responsabilidade;
- demonstrar sustentabilidade econômica e transparência administrativa;
- projetar seus sistemas de acordo com convenções e padrões comumente aceitos, no sentido de assegurar, de forma contínua, a gestão, o acesso e a segurança dos materiais depositados;
- estabelecer metodologias para avaliação dos sistemas que considerem as expectativas de confiabilidade esperadas pela comunidade;
- considerar, para desempenhar suas responsabilidades de longo prazo, os depositários e os usuários de forma aberta e explícita;
- dispor de políticas, práticas e desempenho que possam ser auditáveis e mensuráveis; e
- observar os seguintes fatores relativos às responsabilidades organizacionais e de curadoria dos repositórios: escopo dos materiais depositados, gerenciamento do ciclo de vida e preservação, atuação junto a uma ampla gama de parceiros, questões legais relacionadas com a propriedade dos materiais armazenados e implicações financeiras.

Uma forma de atestar a confiabilidade de um repositório digital junto à comunidade-alvo é a sua certificação por terceiros. Para esse fim, o RLG/OCLC, em parceria com o NARA, publicou, em 2007, o documento *Trustworthy repository audit & certification: criteria and checklist* (TRAC).

Um repositório arquivístico digital confiável (RDC-Arq) deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável.

Um RDC-Arq deve ter suas estratégias de preservação muito bem documentadas nas suas políticas, procedimentos, planos e práticas. Este deve não só descrever as ações que é capaz de realizar na promoção da preservação dos documentos que custodia, mas, acima de tudo, comprovar que possui capacidade de manter suas estratégias sempre funcionais e que suas decisões mais relevantes sobre essas estratégias garantem a preservação dos documentos arquivísticos digitais de forma eficaz e confiável.

A seguir, serão apresentadas, primeiramente, algumas considerações a respeito dos repositórios digitais de documentos arquivísticos. Num segundo momento, serão abordados os requisitos que um repositório digital deve seguir para que possa ser considerado confiável, com base na norma ISO 16363:2012, independentemente do tipo de material digital (arquivístico ou não).

II.1 Considerações sobre um repositório digital de documentos arquivísticos

Um repositório digital confiável deve seguir os princípios descritos no Anexo III, Seção D, para que seja considerado arquivístico. São eles:

- responsabilidade pelo repositório;
- tratamento arquivístico;
- princípios de preservação digital;
- independência dos repositórios; e
- interoperabilidade.

II.1 Requisitos para um repositório digital confiável

Os requisitos apresentados a seguir estão definidos em nível conceitual e devem ser cumpridos no desenvolvimento de um repositório digital confiável. Reitere-se que esses requisitos estão baseados na norma ISO 16363:2012 e abrangem todos os tipos de materiais digitais, inclusive os documentos arquivísticos. A listagem detalhada dos requisitos e suas possíveis evidências de validação encontram-se no Anexo III.

Os requisitos estão organizados em três conjuntos e suas subdivisões.

A. Infraestrutura organizacional

Aborda questões relativas a como a instituição se organiza técnica, processual e normativamente para atender sua missão como RDC-Arq. A forma como a instituição se organiza e se estrutura impacta diretamente na manutenção do repositório. Inclui, mas não se restringe a eles, os seguintes elementos:

- governança;
- estrutura organizacional;
- mandato ou propósito;
- escopo;
- funções e responsabilidades;
- arcabouço político;
- sistema de financiamento;
- questões financeiras (incluindo ativos);
- contratos, licenças e passivos;
- transparência.

Os referidos elementos, para fins destas diretrizes, estão distribuídos nas seguintes subseções:

A.1 Governança e viabilidade organizacional

Independentemente do tamanho, escopo ou natureza do programa de preservação, um RDC-Arq deve demonstrar um compromisso explícito, exequível e de longo prazo para a conformidade às políticas, aos padrões e melhores práticas vigentes.

A.2 Estrutura organizacional e de pessoal

Um repositório arquivístico digital confiável deve ter funcionários designados com as habilidades e treinamento necessários, além de promover o desenvolvimento contínuo desses profissionais. Deve ser capaz, também, de documentar os esforços para mapear e manter as funções, descrições de cargos, planos de desenvolvimento e habilidades necessárias.

A.3 Transparência de procedimentos e arcabouço político

Um RDC-Arq deve fornecer documentação clara e explícita de seus requisitos, decisões, desenvolvimento e ações para garantir preservação e acesso em longo prazo dos documentos sob sua custódia. Essa documentação garante à comunidade-alvo, gerentes, produtores, auditores e certificadores que o repositório está atendendo aos seus requisitos e desempenhando plenamente sua função.

A certificação, o indicador mais claro da prática sólida baseada em normas e padrões, é facilitada pela reponsabilidade processual que resulta de políticas, procedimentos e práticas abrangentes e atuais.

A.4 Sustentabilidade financeira

Um RDC-Arq deve ser capaz de provar sua sustentabilidade financeira. Em geral, um RDC-Arq segue todas as boas práticas de negócios e deve ter um plano de negócios sustentável – um conjunto geral de documentos que refletem o passado, o presente e o futuro do repositório e suas atividades. Um plano de negócios incorpora planos de gestão e implicações financeiras relacionadas ao desenvolvimento de atividades de produção, podendo observar as estratégias e/ou riscos que afetariam as operações.

Os procedimentos de análise e adequação financeira devem ser revistos anualmente. Devem ser usados procedimentos contábeis aderentes a normas e procedimentos legais e administrativos (estar em *compliance*). Os ciclos de planejamento financeiro de curto e longo prazos devem demonstrar um equilíbrio contínuo de risco, benefício, investimento e despesa. Os orçamentos e reservas operacionais devem ser adequados às necessidades do negócio.

A.5 Contratos, licenças e passivos

Os contratos, licenças e passivos de um RDC-Arq devem ser explícitos e definidos de forma clara e em termos mensuráveis, delinear funções e responsabilidades, prazos e condições, e ser prontamente acessíveis ou disponíveis às partes interessadas sob demanda.

Os contratos incluem aqueles entre o RDC-Arq e os produtores/depositários dos documentos arquivísticos digitais e aqueles entre o RDC-Arq e seus provedores de serviço.

Independentemente do relacionamento, esses contratos e licenças devem estar disponíveis para auditorias.

B. Gerenciamento do documento digital

O gerenciamento dos documentos de um RDC-Arq deve estar de acordo com o modelo de referência OAIS, que estabelece a formação de pacotes de informação envolvendo os documentos digitais (informação de conteúdo) e seus metadados (informação de representação). Incluem-se aspectos organizacionais e técnicos relacionados a essas responsabilidades, como funções do repositório, processos e procedimentos necessários para admitir, gerenciar, preservar e fornecer acesso aos documentos arquivísticos digitais.

Os requisitos desta seção são categorizados em seis grupos com base no agrupamento de funcionalidades das entidades funcionais do modelo OAIS. Estes requisitos pressupõem familiaridade com o OAIS, seus conceitos, fluxos e funcionalidades.

B.1 Admissão: captura de documentos digitais

A admissão consiste na entrada dos documentos e seus metadados no repositório digital. Os requisitos de admissão variam dependendo do tipo de material, do contexto legal e da relação entre o produtor de documentos e o repositório. Independentemente dessas variações, pode-se afirmar que a admissão se inicia com o recebimento de um SIP, que é convertido em AIP, e termina quando um AIP está seguro no repositório, incluindo a criação de cópias de segurança.

B.2 Admissão: criação do pacote de arquivamento

O RDC-Arq deve completar o processo de admissão criando um pacote de informação apropriado para arquivamento (AIP), com toda a informação recebida do produtor.

B.3 Planejamento da preservação

Um RDC-Arq deve fazer o planejamento da preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital e ser bem documentado.

B.4 Armazenamento e preservação/manutenção do AIP

Um repositório deve atender a um conjunto de condições para garantir o bom desempenho da preservação de longo prazo dos AIPs.

B.5 Gerenciamento da informação

Uma funcionalidade essencial de um RDC-Arq é o gerenciamento da informação, aqui entendido como a gestão das informações descritivas (metadados) dos documentos admitidos no repositório. O principal objetivo desses metadados é apoiar o acesso e a recuperação dos documentos, e eles vão além das informações descritivas mais usuais (autor, título, data), envolvendo outras também úteis aos usuários, tais como o tamanho do arquivo disponível para download ou informação sobre a aplicação necessária para ler o arquivo.

B.6 Gerenciamento de acesso

O termo acesso possui vários sentidos diferentes, incluindo, por exemplo, acesso dos usuários ao sistema do repositório; segurança física e autenticação do usuário; e as diferentes fases de acesso aos documentos digitais (fazer uma solicitação, verificar os direitos do solicitante, preparar e enviar um pacote de informação para disseminação, DIP). Esta subseção tratará sobre o assunto.

C. Tecnologia, infraestrutura técnica e segurança

Esses requisitos não prescrevem hardware e software específicos para garantir a preservação de longo prazo dos AIPs, mas apenas descrevem as melhores práticas das áreas de gestão de dados e segurança que devem ser atendidas por um RDC-Arq.

O repositório deve adotar uma tecnologia de hardware e software apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.

De uma forma geral, esses requisitos medem a adequação da infraestrutura técnica do repositório e sua capacidade de atender as demandas de gerenciamento e segurança. Repositórios e instituições que passaram por certificação da ISO 27002 certamente atenderão a muitos desses requisitos.

C.1 Infraestrutura de sistema

Um repositório deve possuir uma infraestrutura tecnológica robusta, de maneira a apoiar a confiabilidade dos AIPs nele mantidos.

C.2 Gestão de risco e segurança

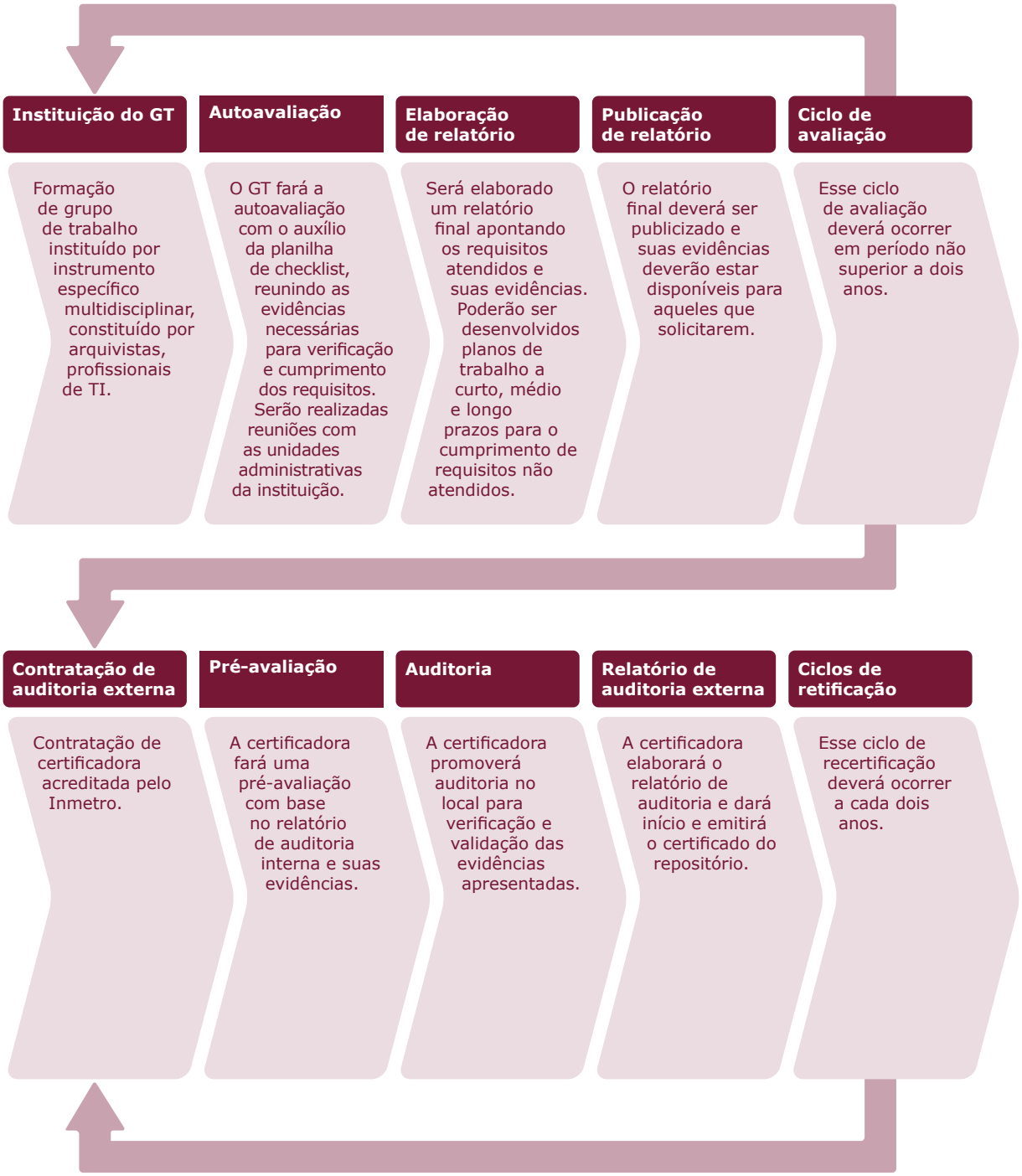
A segurança do repositório não se limita a aspectos de tecnologia, mas abrange também instalações físicas e ações de pessoas.

> Vale ressaltar que um RDC-Arq não se resume a qualquer solução de software ou hardware.

III METODOLOGIA DE APLICAÇÃO

A aplicação desta norma, em termos de auditoria interna, externa ou de terceira parte, deve seguir as diretrizes da ISO 19011:2018, ISO 17021:2016 e ISO 16919:2014. O fluxo a seguir é uma adaptação resumida das normas citadas para fins de referência.

Figura 1 – Fluxo de auditoria e certificação



IV Padrões e normas de referência

A seguir, são apresentados documentos de referência para a construção de repositórios arquivísticos digitais confiáveis (RDC-Arq). Destaca-se que os documentos são variados:

- documentos que definem modelos ou orientam a certificação de repositórios confiáveis;
- definição de metadados, que podem ser utilizados de acordo com o propósito do repositório; e
- codificações, em XML, de metadados e de padrões de transmissão.

IV.1 Modelo de referência OAIS

FONTES

Reference model for an open archival information system (OAIS) – Magenta Book. Issue 2 – CCSDS: junho de 2012.

Space data and information transfer systems – Open archival information system – Reference model: ISO 14721:2012.

Sistemas espaciais de dados e informações – Modelo de referência para um sistema aberto de arquivamento de informação (SAAI): ABNT NBR 15472:2007.

O modelo de referência OAIS (Open Archival Information System)[15] é uma recomendação internacional desde 2003 (ISO 14721). Trata-se de um modelo conceitual que define um repositório digital, identificando o ambiente, os componentes funcionais, suas interfaces internas e externas, os objetos de dados e informações. No Brasil, foi adaptado e publicado como norma ABNT NBR 15472:2007, sob o título Sistema Aberto de Arquivamento de Informação (SAAI).

Um repositório que segue a norma OAIS é constituído por pessoas e sistemas com a responsabilidade de preservar a informação e torná-la disponível. O modelo aborda questões fundamentais relativas à preservação de longo prazo de materiais digitais, independentemente da área de aplicação (arquivo, biblioteca, museu etc.).

O ambiente do modelo conta com três entidades externas:

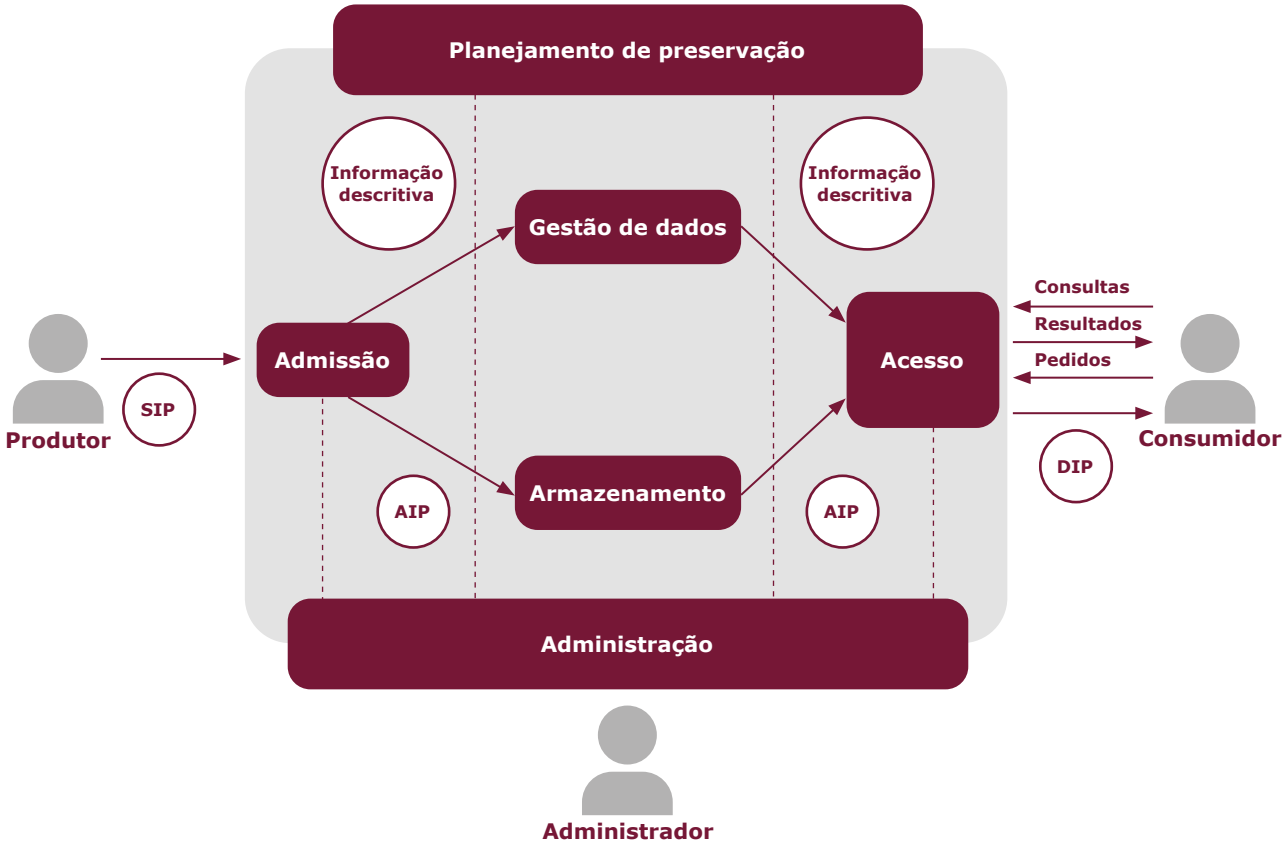
- **produtor** – é o papel desempenhado por pessoas ou sistemas que fornecem a informação a ser preservada;
- **administrador** – é o papel desempenhado por aqueles que estabelecem as políticas gerais que governam o repositório;
- **consumidor** – é o papel desempenhado por pessoas ou sistemas que interagem com os serviços OAIS para acessar a informação preservada desejada.

O OAIS é composto por dois modelos: o modelo funcional e o modelo de informação. O modelo funcional delineia as funções que precisam ser desempenhadas por um

15 O termo *open ("aberto") é usado para indicar que o modelo de referência é construído em fóruns abertos, e não que o acesso ao arquivo é irrestrito*.

repositório OAIS. A Figura 2 apresenta os componentes funcionais, os pacotes de informação e as entidades externas de um repositório digital compatível com o OAIS.

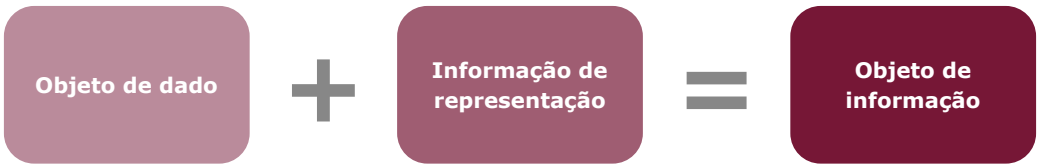
Figura 2 – Entidades funcionais do OAIS



Para fins de preservação, o entendimento claro de determinados conceitos é central. Assim, no âmbito do OAIS, esses conceitos são:

- **informação** – é qualquer tipo de conhecimento que pode ser intercambiado, sempre representado por algum tipo de dado;
- **objeto de informação** – é resultante do objeto de dado, que é interpretado com o uso da informação de representação. Essa informação de representação pode ser decomposta em informação semântica e estrutural, como, por exemplo, um texto em português – informação semântica – codificado no formato ASCII – informação estrutural (Figura 3).

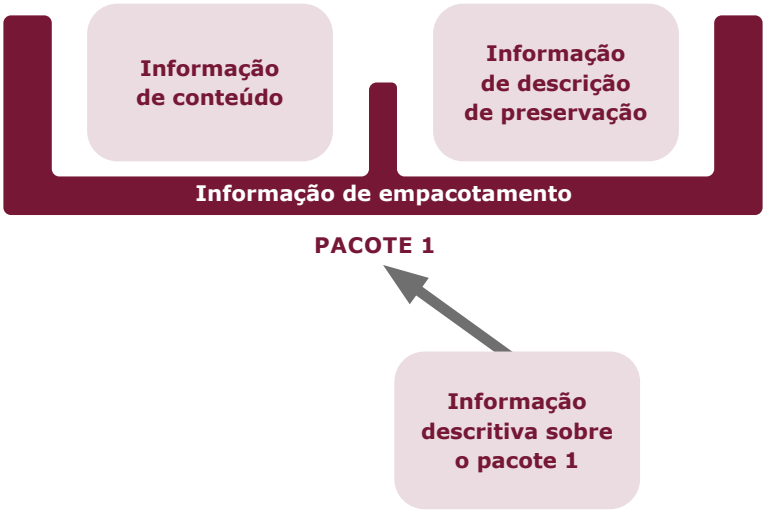
Figura 3 – Informação a partir dos dados



O modelo de informação do OAIS propõe o conceito de pacote de informação (Figura 4), que é formado pela informação de conteúdo e pela informação de descrição de preservação, encapsuladas e identificadas pela informação de empacotamento. A informação de conteúdo é o objeto de informação (objeto de dado + informação de representação) a ser preservado. A informação de descrição de preservação é a informação necessária para a adequada preservação da informação de conteúdo, e que pode ser categorizada como informação sobre proveniência, referência, fixidade e contexto.

O pacote de informação é associado a outras informações descritivas que vão possibilitar sua localização no repositório.

Figura 4 – Conceitos e relacionamentos do pacote de informação



IV.2 Metodologia de interface produtor-arquivo

FONTES

Producer-archive interface methodology abstract standard – Magenta Book. CCSDS: maio de 2004.

Space data and information transfer systems — Producer-archive interface — Methodology abstract standard: ISO 20652:2006.

Sistemas espaciais de transferência de dados e informação – Interface produtor-arquivo – Padrão de metodologia abstrata: ABNT NBR 15862:2010.

É uma recomendação técnica, criada pelo Consultative Committee for Space Data Systems (CCSDS), com objetivo de identificar, definir e estruturar as relações e interações entre um produtor de informação e um arquivo. Define a metodologia para que as ações necessárias sejam estruturadas desde o momento do contato entre o produtor e o arquivo até que os objetos de informação sejam recebidos e validados pelo arquivo. Essas ações abrangem a primeira etapa do processo de ingestão, conforme definido no modelo de referência OAIS.

Este documento descreve parte das entidades funcionais *Administration* ("Acordo de envio de negociação") e *Ingest* ("Recebimento de submissão" e "Garantia de qualidade"). Com a aplicação da metodologia recomendada, o arquivo será capaz de:

- identificar as diferentes fases do processo de transferência de informação entre um produtor e um arquivo;
- definir o objetivo de cada uma dessas fases, as ações que devem ser realizadas durante essas fases e os resultados esperados (por exemplo, administrativo, técnico, contratual) ao final de uma fase;
- formar um quadro metodológico geral, que deve poder ser aplicado e reutilizado nos processos que se relacionam com a interface produtor-arquivo OAIS. Este quadro geral também deve fornecer flexibilidade suficiente para cada caso particular;
- formar uma base para a identificação e/ou desenvolvimento de padrões e guias de implementação, na comunidade em questão;
- formar uma base para a identificação e/ou desenvolvimento de um conjunto de ferramentas de software que auxiliarão no desenvolvimento, operação e verificação das diferentes etapas do processo de transferência de informações entre o produtor e o arquivo.

IV.3 Relatório da Research Library Group (RLG) e da Online Computer Library Center (OCLC) – Repositórios digitais confiáveis: atributos e responsabilidades

FONTE

Trusted digital repositories: attributes and responsibilities – RLG-OCLC Report: maio de 2002.

O relatório, publicado em maio de 2002, apresenta uma proposta conjunta para a implementação de repositórios de organizações de ciência e pesquisa, a partir do modelo OAIS. O relatório estabeleceu as características essenciais e as responsabilidades para a criação e manutenção de repositórios digitais confiáveis que atendessem aos acervos de instituições culturais e científicas, garantindo seu acesso em longo prazo, sua integridade e confiabilidade.

De acordo com a OCLC, um dos princípios básicos de um repositório digital confiável é demonstrar sua capacidade de sustentabilidade, no longo prazo, e de qualificação para o tratamento técnico dos acervos digitais, em diferentes formatos, além de contar com uma infraestrutura tecnológica robusta.

IV.4 Modelo de empacotamento de dados

FONTE

The BagIt file packaging format (V1.0) – Library of Congress: outubro de 2018. RFC 8493.

BagIt é um conjunto de esquemas hierárquicos projetado para suportar armazenamento e transferência de qualquer conteúdo digital (Figura 5). Um *bag* consiste em um diretório contendo os arquivos de *payload* e outros arquivos de metadados que os acompanham, conhecidos como arquivos tag. As *tags* são arquivos de metadados destinados a facilitar e documentar o armazenamento e a transferência do pacote (*bag*). O processamento de um *bag* não requer nenhuma compreensão do conteúdo do arquivo *payload* e os arquivos de *payload* podem ser acessados sem processar os metadados do *BagIt*.

Figura 5 – Exemplo de um *BagIt bag contents*

```
SampleBagIt/
bag-info.txt
bagit.txt
data/
0001.tif
0002.tif
manifest-md5.txt
tagmanifest-md5.txt
```

Fonte: https://blogs.loc.gov/thesignal/2019/04/bagit-at-the-library-of-congress/.

IV.5 Certificação e auditoria de repositórios confiáveis: critérios e checklist – TRAC

FONTES

Trustworthy repositories audit & certification: criteria and checklist – OCLC, CRL, NARA: fevereiro de 2007.

Space data and information transfer systems – Audit and certification of trustworthy digital repositories: ISO 16363:2012.

O documento apresenta um conjunto de critérios e um *checklist* que são tomados como referência para a certificação de repositórios digitais. Nessa direção, ele oferece ferramentas para auditoria, avaliação e certificação potencial de repositórios; estabelece a documentação exigida para a auditoria; delineia um processo de certificação; e estabelece as metodologias apropriadas para determinar a solidez e a sustentabilidade de repositórios digitais.

IV.6 Requisitos técnicos para entidades de auditoria e certificação de organizações candidatas a serem repositórios digitais confiáveis

FONTES

Requirements for bodies providing audit and certification of candidate trustworthy digital repositories – Magenta Book – CCSDS: novembro de 2011.

Space data and information transfer systems – Requirements for bodies providing audit and certification of candidate trustworthy digital repositories: ISO/DIS 16919.

É uma recomendação técnica, criada pelo Consultative Committee for Space Data Systems (CCSDS), que estabelece requisitos para as entidades de auditoria e certificação de repositórios digitais confiáveis. Desde novembro de 2011, encontra-se em fase de desenvolvimento como norma ISO/DIS 16919.

O principal objetivo do documento é definir uma prática sobre a qual devem se basear as operações de uma organização que realiza auditorias para avaliar a confiabilidade de repositórios digitais e fornecer a certificação apropriada. Nesse sentido, apoia o credenciamento de entidades que prestam essa certificação. As exigências contidas nesta norma precisam ser demonstradas, em termos de competência e confiabilidade, por qualquer organização ou organismo de certificação de repositórios digitais.

IV.7 Metadados de preservação (Premis)

FONTE

Premis data dictionary for preservation metadata. Versão 3.0: novembro de 2015.

É uma norma internacional que apresenta um conjunto básico (*core*) de elementos de metadados de preservação para apoiar sistemas que gerenciam objetos digitais. O grupo de trabalho Premis (Preservation Metadata: Implementation Strategies) tem ampla abrangência junto à comunidade dedicada à preservação digital e seu principal documento de referência é o *Premis Data Dictionary for Preservation Metadata*.

Os metadados definidos no *Premis Data Dictionary*:

- contribuem para a viabilidade, disponibilidade, clareza, autenticidade e identidade de objetos no contexto da preservação digital;
- representam as informações sobre os documentos digitais que a maioria dos repositórios precisa conhecer para preservar esses documentos ao longo do tempo;
- prestam especial atenção aos metadados rigorosamente definidos, com base em diretrizes para a criação, gestão e uso, voltados para fluxos de trabalho automatizados;
- são tecnicamente neutros, ou seja, não assumem o uso, em particular, de quaisquer tecnologias de preservação, estratégias, sistemas de armazenamento, gerenciamento de metadados etc.

O *Premis Data Dictionary* também inclui um modelo de esquema em XML que permite incorporar o dicionário de dados em sistemas de gestão de objetos digitais.

A norma é mantida pelo Network Development and MARC Standards Office, da Biblioteca do Congresso dos Estados Unidos da América (Library of Congress).

IV.8 Norma Geral Internacional de Descrição Arquivística, ISAD(G)

FONTE

Norma Geral Internacional de Descrição Arquivística – ISAD(G) – Segunda edição – CIA: 2000.

É uma norma elaborada no âmbito do Conselho Internacional de Arquivos (CIA), publicada, pela primeira vez, em 1994 e, em segunda edição, em 2000, que estabelece diretrizes gerais para a preparação de descrições arquivísticas. Tem por objetivo identificar e explicar o contexto e o conteúdo de documentos de arquivo, a fim de promover o acesso a eles.

IV.9 Norma Brasileira de Descrição Arquivística (Nobrade)

FONTE

Norma Brasileira de Descrição Arquivística – Nobrade – CTNDA/Conarq: 2006.

É uma norma elaborada pela Câmara Técnica de Normalização de Descrição Arquivística do Conselho Nacional de Arquivos (CTNDA/Conarq), publicada em 2006, em conformidade com a ISAD(G) e a Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias, Isaar(CPF).

A Nobrade consiste na adaptação – e não simplesmente na tradução – das normas internacionais à realidade brasileira, visando a facilitar o acesso e o intercâmbio de informações, em âmbito nacional e internacional, por meio de descrições consistentes, apropriadas e autoexplicativas dos documentos arquivísticos.

IV.10 Metadados do e-ARQ Brasil

FONTE

Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil, v2 – CTDE/Conarq: julho de 2021.

O e-ARQ Brasil é o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, elaborado pela Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (CTDE/Conarq) e adotado pelo Sistema Nacional de Arquivos (Sinar) por meio da resolução n. 50, de 6 de maio de 2022, do Conarq.

O objetivo do modelo é orientar a implantação da gestão arquivística de documentos, fornecer especificações técnicas e funcionais, e metadados para orientar a aquisição e/ou desenvolvimento de sistemas informatizados, independentemente da plataforma tecnológica em que forem desenvolvidos e/ou implantados.

A parte II da versão 2 do e-ARQ Brasil elenca os metadados a serem associados aos documentos, a fim de apoiar a gestão, a preservação e a presunção de autenticidade dos documentos arquivísticos. A especificação dos metadados considera as seguintes entidades: documento, evento de gestão, classe, agente, componente digital e evento de preservação.

O e-ARQ Brasil deve ser levado em consideração para a implementação dos repositórios arquivísticos digitais, já que a integração dos repositórios aos sistemas informatizados de gestão arquivística de documentos (Sigads) é fundamental para o sucesso das iniciativas de gestão.

IV.11 Protocolo para coleta de metadados (OAI-PMH)

FONTE

Open Archives Initiative Protocol for Metadata Harvesting – OAI-PMH, Version 2.0 – Open Archives Initiative: junho de 2002.

É um protocolo para coleta de metadados que permite a interoperabilidade de repositórios. Está baseado nas normas abertas HTTP e XML, e visa a facilitar a disseminação eficiente de conteúdo. O OAI-PMH16 não realiza pesquisas em dados, mas possibilita a reunião dos dados num só lugar.

IV.12 Padrão de codificação e transmissão de metadados (METS)

FONTE

METS – Metadata Encoding & Transmission Standard.

16 Disponível em: https://www.openarchives.org/pmh/.

É um esquema XML que permite a codificação e o intercâmbio dos metadados descritivos, administrativos e estruturais relativos a objetos digitais. Trata-se de um padrão para empacotamento que permite organizar, em um único arquivo compactado, tanto os dados quanto os metadados. Atualmente, o METS é mantido pela Biblioteca do Congresso dos Estados Unidos da América (Library of Congress), que mantém sítio oficial.[17]

Algumas implementações do padrão OAIS utilizam o METS para estruturar os pacotes SIP, AIP e DIP. Além disso, alguns repositórios digitais usam o METS para intercâmbio de objetos.

A estrutura de um pacote METS é definida por um modelo que detalha os elementos para a estruturação de um objeto digital. Basicamente, um pacote METS possui, obrigatoriamente, um cabeçalho (header) e até seis seções, que abrangem os metadados descritivos, os metadados administrativos, a lista de arquivos do pacote, seus relacionamentos e comportamento.

O METS é neutro em relação aos formatos de metadados encapsulados no pacote digital. Dessa forma, é necessário que se defina como o pacote digital será estruturado, estabelecendo os formatos de metadados que serão utilizados. Essa configuração padrão é denominada "perfil de aplicação". Como boa prática, deve-se, antes de criar um novo perfil para um determinado repositório, pesquisar se os perfis existentes atendem aos requisitos desejados.

IV.13 Descrição arquivística codificada (EAD)

FONTE

EAD – Encoded Archival Description: dezembro de 2002.

Trata-se de uma codificação desenvolvida e utilizada para a descrição de metadados arquivísticos baseados na linguagem de marcação XML. O projeto, iniciado na Universidade da Califórnia em 1993, teve como base o padrão MARC (machine-readable cataloging), dando origem à EAD.DTD, que foi publicada na versão 1.0 em 1998 e consolidada em dezembro de 2002.[18] A versão vigente atualiza e incorpora metadados relacionados aos padrões de metadados MARC, ISAD(G) e Dublin Core.

A EAD permite a descrição, estruturação e interoperabilidade dos metadados arquivísticos referenciais, que, quando associados ao XML, possibilitam a decodificação e a apresentação das informações referenciais de forma estruturada aos usuários. O padrão EAD, atualmente, é mantido pelo Network Development and MARC Standards Office da Biblioteca do Congresso dos Estados Unidos da América, em parceria com a Society of American Archivists (SAA).

17 Disponível em: http://www.loc.gov/standards/mets.

18 Disponível em: http://www.loc.gov/ead.

ANEXOS

I Documentos mínimos necessários

Os requisitos em toda esta resolução referem-se a documentos (políticas, procedimentos, planos etc.) que um repositório deve manter atualizados. Esta lista identifica os documentos que são exigidos por um ou mais requisitos, portanto, um repositório confiável deve ter e manter sob constante atualização pelo menos esses documentos. Alguns repositórios irão fornecer comprovação do cumprimento de determinados requisitos por meio de documentos que não constam desta lista.

Os ciclos de revisão variam de acordo com a instituição. Os repositórios devem estar preparados para demonstrar que seus ciclos de revisão são adequados às suas atividades e necessidades.

Requisito	Documentos e evidências
A.1.2.1	- Plano de contingência Documento desenvolvido com o objetivo de avaliar, orientar e uniformizar as repostas necessárias no controle e enfrentamento de situações adversas que comprometam a continuidade do negócio. - Plano de sucessão Documento que define a transferência de responsabilidade pela continuidade das atividades do repositório em casos de interrupção das atividades da instituição ou seu fechamento. - Acordos de custódia Documento que estabelece formalmente os direitos e deveres relacionados à custódia dos documentos submetidos ao repositório. Inclui-se neste documento qualquer modalidade de transferência de custódia (transferência, recolhimento, doação etc.). Obs.: a norma ISO 22301:2012, que se refere à implantação de sistemas de gestão de continuidade de negócios, poderá subsidiar a elaboração dos documentos e estratégias de continuidade.
A.3.1	Definição de comunidade(s)-alvo e política relativa aos níveis de serviço.
A.5.1.3	Políticas relacionadas às permissões legais.
A.4.2	Procedimentos financeiros documentados e manualizados.
A.5.1.4	Políticas/procedimentos relativos à disputa de direitos (apenas se houver necessidade comprovada).
B.1.1	Procedimentos relativos à admissão (*ingest*).
B.2.7 B.2.7.1 B.2.7.2 B.2.7.3	Processos de teste de compreensibilidade (os testes deverão ser manualizados, documentados e executados de forma periódica, gerando logs e relatórios).
B.1.5 B.3.1 B.3.3	- Plano de preservação Descrição dos serviços e estratégias de preservação a serem utilizados, definição de formatos, metadados (todas as categorias), descrição da arquitetura do ecossistema do repositório, definição dos sistemas, serviços e tecnologias utilizados, definição de procedimento e periodicidade de testes de fixidez e integridade.

Requisito	Documentos e evidências
B.4.1	Estratégias de armazenamento e migração, manualizados e documentados, com logs e relatórios de testagem.
B.6.1.1	Política de registro de ações de acesso, registros de acesso, tentativas de acesso, falhas e correções.
B.6.1	- Política de acesso Definição de regras de acesso e suas restrições.
C.1.1.5	Processos de mudança de mídia manualizados, documentados, incluindo logs e relatórios do procedimento e testes.
C.1.1.6.1	- Processo de gestão de mudança Normas como a ISO 9001 e ITIL poderão auxiliar no desenvolvimento, manualização e registros desses processos.
C.1.1.6.2	Processos de teste de mudanças críticas manualizados, documentados com logs e relatórios.
C.1.1.4	Processos de atualização de segurança.
C.1.1.1 C.1.1.1.1 C.1.1.1.2 C.1.1.1.3 C.1.1.1.4	Processo de monitoramento de mudança de requisitos de hardware.
C.1.1.1 C.1.1.1.5 C.1.1.1.6 C.1.1.1.7 C.1.1.1.8	Processo de monitoramento de mudança de requisitos de software.
C.2.4	- Plano de desastres Documento que detalha como a instituição deve agir para responder a incidentes (inundação, alagamento, queda de energia, ataque cibernético etc.).

II Planejamento e estratégias de preservação

Um RDC-Arq deve ter suas estratégias de preservação documentadas. Entretanto, não deve simplesmente dizer o que faz; deve demonstrá-lo em políticas, práticas, manuais e procedimentos.

O repositório deve ser capaz de demonstrar:

1. **Decisões relevantes** sobre os formatos que aceita: por exemplo, políticas que definem, estipulam ou restringem os formatos aceitos pelo repositório.
2. ***Workflow*, automatizado ou manual, abrangente para coletar os documentos digitais apropriados**: por exemplo, protocolos para transferência, incluindo funções e responsabilidades do produtor e do repositório; evidência explícita de conversões que ocorrem em AIPs que são gerados a partir dos SIPs; mecanismos de garantia de qualidade e medidas para garantir a integridade e exatidão dos AIPs resultantes da conversão dos pacotes.
3. **Ações de preservação previstas e/ou aplicadas pertencentes a indivíduos e classes de AIPs**: por exemplo, planos de preservação planejados, testados e/ou aplicados; registros de ações de preservação; políticas que abordam estratégias de preservação.
4. **Políticas, procedimentos e práticas de armazenamento que garantem a captura eficaz, armazenamento de arquivos de forma contínua e confiável, capacidade de respostas a mudanças tecnológicas inevitáveis**: por exemplo, documentos de planejamento e investimento em gerenciamento de armazenamento, planos de segurança abrangentes para permitir o fluxo de trabalho, medidas e protocolos de monitoramento dos AIPs armazenados.
5. **Meios independentes de verificação de conteúdo do repositório com base no rastreamento seguro dos documentos digitais recebidos**: por exemplo, registros auditáveis das admissões que não possam ser alterados.

Este é o conjunto chave de atividades para tornar os documentos preservados acessíveis e confiáveis às gerações futuras. A estratégia de preservação estabelece um plano para realizar isso em um ambiente em constante evolução (social, tecnológica etc.).

A estratégia deve fornecer:

- um processo de monitoramento das mudanças que possam afetar a preservação;
- entendimento e experiência para interpretar o impacto/implicações dessas mudanças;
- um processo para implementação de respostas.

As estratégias potenciais são:

- converter o formato na admissão (*ingest*);
- manter o formato original e esperar que outros produzam uma solução de software para o formato;
- produzir um ambiente de emulação compatível para permitir que o formato original continue acessível.

As estratégias podem ser necessárias para cada classe de formatos de documentos digitais mantidos pelo repositório. Verificações de fixidez, *checksums*, *hashes* e correções de erros, assim como análises aleatórias do acervo para monitoramento de degradação de mídia devem ser executados periodicamente, conforme definido nas políticas e procedimentos de monitoramento estabelecidos.

III REQUISITOS

As evidências deverão ser publicizadas, atualizadas e disponíveis aos produtores, comunidade-alvo, auditores, certificadores ou qualquer outro interessado.

Outras evidências, para além daquelas sugeridas nos requisitos, poderão ser apresentadas e apreciadas pela comissão responsável pela auditoria/avaliação de conformidades do repositório.

A. Infraestrutura organizacional

O ambiente em que o repositório digital vai se estabelecer tem que cumprir determinados requisitos, conforme descrito a seguir.

A.1 Governança e viabilidade organizacional

Seção	**A Infraestrutura organizacional**	
Subseção	**A.1** Governança e viabilidade organizacional	
Requisito	**A.1.1** O repositório tem como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. Essa missão é claramente identificada por todos os interessados no repositório e envolve mandato legal, contexto organizacional e requisitos regulatórios.	
Evidência	Declaração de missão, estatuto, regimento interno, política ou qualquer outro ato regulatório legal publicizado, do repositório ou de sua instituição responsável, apontando de forma explícita o compromisso da instituição com a preservação dos documentos digitais sob sua custódia e com a manutenção da sua autenticidade.	
Seção	**A Infraestrutura organizacional**	
Subseção	**A.1** Governança e viabilidade organizacional	
Requisito	**A.1.2** O repositório tem um plano estratégico de preservação que define a abordagem que o repositório adotará no apoio de longo prazo de sua missão.	Obs.: requisito aplicável caso a instituição disponha de planejamento estratégico.
Evidência	Planejamento estratégico, atas de reuniões e documentação que registrem as decisões tomadas, apontando explicitamente questões relativas ao plano estratégico de preservação.	
Seção	**A Infraestrutura organizacional**	
Subseção	**A.1** Governança e viabilidade organizacional	
Requisito	**A.1.2.1** O repositório deve ter um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos para garantir a continuidade do serviço, caso o repositório pare de operar ou a instituição responsável e/ou financiadora mude de escopo.	

Evidência	Plano de sucessão e contingência publicizados; declaração explícita documentada sobre a intenção de garantir a continuidade do repositório e as medidas a serem tomadas para garantir sua continuidade; manutenção de códigos críticos, softwares e metadados suficientes para reconstituir o repositório e seu conteúdo; fundos de emergência e acordos de sucessão que apresentem as medidas a serem tomadas para garantir a transferência completa e formal da responsabilidade pelo repositório e pela custódia dos documentos digitais, concedendo os direitos necessários para garantir a continuidade dos serviços.
Seção	**A Infraestrutura organizacional**
Subseção	**A.1** Governança e viabilidade organizacional
Requisito	**A.1.2.2** O repositório deve monitorar seu ambiente organizacional para determinar quando executar seu plano de sucessão, planos de contingência e/ou acordos de custódia.
Evidência	Políticas, regimento interno, estatuto, procedimentos, protocolos; documentação de análise orçamentária e financeira; planos de negócio e qualquer outra evidência de monitoramento ativo da organização.
Seção	**A Infraestrutura organizacional**
	A.1 Governança e viabilidade organizacional
Requisito	**A.1.3** O repositório deve ter uma política de submissão/acervo ou outro documento que especifique os tipos de documentos que irá preservar, reter, gerenciar e aos quais fornecerá acesso.
Evidência	Política de entrada de acervo admissão, submissão e recolhimento; política de preservação; declaração de missão.

A.2 Estrutura organizacional e de pessoal

Seção	**A Infraestrutura organizacional**
Subseção	**A.2** Estrutura organizacional e de pessoal
Requisito	**A.2.1** O repositório deve ter identificado e estabelecido as tarefas que precisa desempenhar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir essas tarefas.
Evidência	Regimento interno; estatuto; portarias de nomeação; descrições de cargos; organogramas; planos de capacitação e desenvolvimento; políticas de seleção de pessoal.
Seção	**A Infraestrutura organizacional**
Subseção	**A.2** Estrutura organizacional e de pessoal
Requisito	**A.2.1.1** O repositório deve ter identificado e estabelecido as tarefas que precisa desempenhar.
Evidência	Regimento interno; estatuto; políticas; organograma; quadro de pessoal com descrições de cargos, funções e responsabilidades; planos de capacitação e desenvolvimento; documentos que comprovem o monitoramento e atualização das medidas de conformidade deste requisito.
Seção	**A Infraestrutura organizacional**
Subseção	**A.2** Estrutura organizacional e de pessoal
Requisito	**A.2.1.2** O repositório deve ter o número adequado de funcionários para apoiar todas as funções e serviços.
Evidência	Organograma; quadro de pessoal com descrições de cargos, funções e responsabilidades.
Seção	**A Infraestrutura organizacional**
Subseção	**A.2** Estrutura organizacional e de pessoal
Requisito	**A.2.1.3** O repositório deve ter implementado um programa ativo de desenvolvimento profissional que forneça à equipe oportunidades de desenvolvimento de habilidades e conhecimentos.
Evidência	Planos de capacitação e desenvolvimento de pessoal; orçamento para treinamento, capacitação e desenvolvimento de pessoal; metas de desempenho da equipe; certificados de cursos realizados.

A.3 Transparência de procedimentos e arcabouço político

O repositório deve demonstrar explicitamente seus requisitos, decisões, desenvolvimento e ações que garantem a preservação de longo prazo e o acesso aos documentos digitais sob seus cuidados. Dessa forma, assegura aos usuários, gestores, produtores e certificadores que está cumprindo plenamente seu papel enquanto um repositório digital confiável; a confiança no repositório está diretamente ligada ao quão transparente ele é. Para tanto, o repositório deve:

Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.1** Definir a comunidade-alvo e sua base de conhecimento.
Evidência	Políticas; definição documentada da comunidade-alvo; estatuto.
Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.2** Ter políticas de preservação em vigor para garantir que seu plano estratégico de preservação seja cumprido.
Evidência	Política de preservação; declaração de missão do repositório.
Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.2.1** Ter políticas, procedimentos e mecanismos de atualização, à medida que o repositório cresce e a tecnologia e as práticas da comunidade evoluem.
Evidência	Documentação atual e anterior de políticas de preservação, planos estratégicos de preservação, planos de preservação, procedimentos, protocolos, fluxos de trabalho, especificação de ciclos de revisão desta documentação. Documentação detalhando os ciclos de revisão, pesquisas e feedbacks. Se a evidência estiver embutida na parte lógica do sistema, a funcionalidade deve demonstrar a implementação das políticas, planos e procedimentos de preservação.
Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.3** Ter um histórico documentado das alterações em suas operações, procedimentos, infraestrutura, pessoal, organograma, software e hardware.
Evidência	Inventário de equipamentos essenciais; documentação de aquisição, implementação e atualização de software e hardware críticos do repositório; tabelas de temporalidade e destinação destes documentos; cópias das versões anteriores de políticas, procedimentos e atas de reuniões. Documentos que registrem decisões sobre a infraestrutura técnica e organizacional.
Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.4** Se comprometer com a transparência e responsabilidade em todas as ações de apoio à operação e gestão que afetem a preservação dos documentos digitais ao longo do tempo.
Evidência	Relatórios de auditoria, financeiro, divulgação de documentos sobre a governança, relatórios de auditoria sobre contratos.
Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.5** Estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia.

Evidência	Definições escritas sobre as medidas de manutenção de integridade (checksum e hash, por exemplo), planos de preservação, políticas de preservação, definição de metadados de integridade, documentação sobre os mecanismos de monitoramento e aferição de integridade e dos mecanismos de respostas às ocorrências dessas verificações, processos documentados de auditoria para coleta e rastreio de medições de integridade.
Seção	**A Infraestrutura organizacional**
Subseção	**A.3** Transparência de procedimentos e arcabouço político
Requisito	**A.3.6** Estar comprometido em realizar regularmente uma autoavaliação de seu funcionamento e certificação do repositório.
Evidência	Cronograma de avaliação, relatórios de avaliação e auditoria interna, listagens de verificação, certificados de conformidade com padrões ISO, evidência sobre conformidade com resoluções do Conarq, evidência sobre alocações de recursos para auditoria e certificações futuras.

A.4 Sustentabilidade financeira

Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos:

Seção	**A Infraestrutura organizacional**
Subseção	**A.4** Sustentabilidade financeira
Requisito	**A.4.1** Processos de planejamento de negócios, de curto e longo prazos, em vigor para sustentá-lo ao longo do tempo.
Evidência	Planejamento estratégico, políticas, plano de negócio, planejamentos plurianuais, demonstrativos financeiros anuais auditados, planejamento orçamentário, planejamento financeiro, planos de contingência e análises de mercado.
Seção	**A Infraestrutura organizacional**
Subseção	**A.4** Sustentabilidade financeira
Requisito	**A.4.2** Transparência dos procedimentos para obtenção dos recursos e auditoria deles, de acordo com o sistema jurídico no qual o repositório se insere.
Evidência	Planos de negócio, demonstrativos financeiros e contábeis, relatório de prestação de contas, relatórios de auditoria. Evidências que informem sobre finanças, gestão de passivos e contratos.
Seção	**A Infraestrutura organizacional**
Subseção	**A.4** Sustentabilidade financeira
Requisito	**A.4.3** Ter um compromisso contínuo de analisar e relatar riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e encargos).
Evidência	Documentos sobre gerenciamento de riscos que identifiquem ameaças percebidas e potenciais; planos de respostas planejadas ou implementadas para estes riscos; planejamento de investimentos; análises de custo; relatórios de investimentos, contratos e gerenciamento de ativos; evidência sobre a revisão do planejamento baseados nos riscos.

A.5 Contratos, licenças e passivos

Os contratos, licenças e passivos firmados pelo repositório devem ser claros e mensuráveis; delinear funções, responsabilidades, prazos e condições; e ser facilmente acessíveis ou disponíveis aos interessados. Esses contratos, licenças e passivos podem envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. Esses mesmos instrumentos devem especificar todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial no que diz respeito à propriedade intelectual e a restrições de uso, logo devem-se observar os seguintes aspectos:

Seção	**A Infraestrutura organizacional**
Subseção	**A.5** Contratos, licenças e passivos
Requisito	**A.5.1** Ter e manter contratos ou acordos de custódia adequados para os documentos digitais que gerencia, preserva e/ou aos quais fornece acesso.
Evidência	Acordos e licenças de custódia devidamente assinados e executados de acordo com as leis e regulamentos locais, nacionais e internacionais; políticas sobre acordos de custódia de terceiros; definições de níveis de serviço e usos permitidos; políticas de repositório sobre o tratamento de "obras órfãs" e resolução de disputas de direitos autorais; relatórios independentes de avaliações de risco dessas políticas.
Seção	**A Infraestrutura organizacional**
Subseção	**A.5** Contratos, licenças e passivos
Requisito	**A.5.1.1** Contratos ou acordos de custódia que especificam e transferem todos os direitos necessários à preservação, e esses direitos transferidos devem ser documentados.
Evidência	Contratos, acordos de custódia; especificação(ões) de direitos transferidos para diferentes tipos de documento digital (se aplicável); declarações de política sobre os direitos de preservação necessários.
Seção	**A Infraestrutura organizacional**
Subseção	**A.5** Contratos, licenças e passivos
Requisito	**A.5.1.2** Ter especificado todos os aspectos apropriados de admissão, manutenção, acesso e retirada em acordos escritos com depositantes e outras partes relevantes.
Evidência	Acordos de submissão e de depósito e termos de doação executados adequadamente; procedimentos operacionais padrão (POP).
Seção	**A Infraestrutura organizacional**
Subseção	**A.5** Contratos, licenças e passivos
Requisito	**A.5.1.3** Ter políticas escritas que indiquem quando ele aceita a responsabilidade pela preservação dos documentos digitais de cada conjunto de documentos digitais recebidos.
Evidência	Acordos de submissão, termos de recolhimento, termos de doação; registros de confirmação de envio e recebimento do acervo.
Seção	**A Infraestrutura organizacional**
Subseção	**A.5** Contratos, licenças e passivos
Requisito	**A.5.1.4** Ter políticas em vigor para lidar com encargos e questões de propriedade/direitos.
Evidência	Licenças e permissões dos produtores dos documentos; citações de leis e regulamentos relevantes; políticas de respostas aos desafios; históricos documentados de respostas aos desafios; pareceres jurídicos; definição de direitos.
Seção	**A Infraestrutura organizacional**
Subseção	**A.5** Contratos, licenças e passivos

Requisito	**A.5.2** Rastrear e gerenciar os direitos de propriedade intelectual e as restrições ao uso dos documentos armazenados no repositório, conforme exigido pelo acordo de custódia, contrato ou licença.
Evidência	Uma declaração de política de preservação que defina e especifique os requisitos do repositório e o processo de gerenciamento de direitos de propriedade intelectual; acordos com depositantes; amostras de acordos e outros documentos que especifiquem e tratem dos direitos de propriedade intelectual; documentação sobre o monitoramento, ao longo do tempo, de alterações no status e posse de direitos de propriedade intelectual sobre os documentos digitais mantidos pelo repositório; resultados do monitoramento, metadados de captura.

B. Gerenciamento do documento digital

O gerenciamento dos documentos de um repositório digital confiável deve estar de acordo com o modelo de referência OAIS, que estabelece a formação de pacotes de informação envolvendo os documentos digitais (informação de conteúdo) e seus metadados (informação de representação).

A TRAC apresenta os requisitos para gerenciamento do documento no repositório digital, categorizados em seis grupos, com base nas funcionalidades, conforme detalhado a seguir.

B.1 Admissão: captura de documentos digitais

A admissão consiste na entrada dos documentos e seus metadados no repositório digital. Os requisitos de admissão variam dependendo do tipo de material, do contexto legal e da relação entre o produtor de documento e o repositório. Independentemente dessas variações, pode-se afirmar que a admissão se inicia com o recebimento de um SIP, que é convertido em AIP, e termina quando um AIP está seguro no repositório, incluindo a criação de cópias de segurança.

A seguir, apresentam-se requisitos gerais a serem cumpridos pelo repositório, cuja adequação deve ser avaliada de acordo com a missão e as necessidades de cada repositório.

Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.1** Identificar as propriedades do documento que serão preservadas (ex.: conteúdo, layout, tabela de cor, resolução da imagem, canais de som etc.).
Evidência	Acordos e contratos de admissão/submissão; termos de doação; definição de propriedades significativas; política de preservação, incluindo por escrito as propriedades, conforme estipulados nos acordos de admissão/submissão/custódia/recolhimento/transferência.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.1.1** Ter procedimento(s) para identificar as propriedades do documento que irá preservar.
Evidência	Acordos e contratos de admissão/submissão; termos de doação; definição de propriedades significativas; política de preservação, incluindo por escrito as propriedades, conforme estipulados nos acordos de admissão/submissão/custódia/recolhimento/transferência.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.1.2** Ter um registro das informações de conteúdo e das propriedades do documento que irá preservar.
Evidência	Política de preservação; manuais de processamento, metadados; logs, estratégias de preservação incorporadas a planos de ação.

Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.2** Especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão.
Evidência	Requisitos de transferência; acordos produtor-arquivo; planos, fluxos de trabalho, procedimentos e especificações de produção do AIP.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.3** Ter especificações adequadas que permitam o reconhecimento e a análise dos SIPs.
Evidência	Definições, especificações e informações de empacotamento dos SIPs; informações de representação para o conteúdo de dados do SIP, incluindo especificações documentadas de formatos, padrões de dados, e documentação da construção dos objetos.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.4** Ter mecanismos para verificar adequadamente a identidade do produtor de todos os documentos.
Evidência	Acordos de submissão/depósito, termos de doação todos juridicamente validados; metadados; logs de procedimentos de autenticação; evidência de medidas tecnológicas adequadas.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.5** Ter um processo de admissão que verifique cada SIP quanto à completude e correção.
Evidência	Política de preservação, plano de preservação, arquivos de logs do processo de submissão do sistema; listagem dos arquivos recebidos; procedimento operacional padrão (POP); diretório de arquivos.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.6** Ter o controle físico (controle completo dos bits) dos documentos transmitidos com cada SIP, a fim de preservá-los.
Evidência	Documentos que comprovem o nível de controle físico que o repositório realmente possui; base de dados ou catálogo de metadados listando os documentos digitais do repositório e seus metadados para validação de integridade (tamanho do arquivo, checksum, hash, localização, número de cópias etc.).
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.7** Fornecer ao produtor/depositante relatórios sobre o andamento dos procedimentos durante todo o processo de admissão.
Evidência	Acordos de submissão, termos de doação, acordos de depósito; documentação de fluxo de trabalho, procedimentos operacionais padrão (POP); relatórios, memorandos ou e-mails.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.1** Admissão: captura de documentos digitais
Requisito	**B.1.8** Ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação.
Evidência	Processo administrativo; e-mails; metadados; relatórios.

No caso de um repositório para documentos arquivísticos, a definição dos metadados deve observar o e-ARQ Brasil (nas fases corrente e intermediária) e a Nobrade (na fase permanente).

Para a admissão de documentos no repositório, no caso de transferência ou recolhimento, devem-se observar os procedimentos indicados na resolução n. 24, de 3 de agosto de 2006, do Conarq.

B.2 Admissão: criação do pacote de arquivamento

O repositório deve completar o processo de admissão criando um pacote de informação apropriado para arquivamento (AIP), com toda a informação recebida do produtor.

A fim de garantir que o pacote de informação recebido do produtor, e verificado pelo repositório, seja convertido para o formato de arquivamento (AIP) e armazenado para preservação de longo prazo, um repositório deve atender os seguintes requisitos:

Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.1** Ter, para cada AIP ou classe de AIPs preservados, uma definição associada que seja adequada para analisar o AIP e para necessidades de preservação de longo prazo.
Evidência	Metadados, definições e especificações do AIP.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.1.1** Ser capaz de identificar que definição se aplica a cada AIP.
Evidência	Documentação que vincule claramente cada AIP ou classe de AIPs à sua definição.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.1.2** Ter uma definição de cada AIP que seja adequada para preservação de longo prazo, permitindo a identificação e análise de todos os componentes necessários dentro daquele AIP.
Evidência	Demonstração do uso das definições para extrair informações de conteúdo e PDI (proveniência, direitos de acesso, contexto, referência e informações de fixidez) de AIPs. Deve-se notar que a proveniência de um documento digital, por exemplo, pode ser ampliada ao longo do tempo para refletir ações adicionais de preservação.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.2** Descrever como os AIPs são construídos a partir dos SIPs, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do AIP.
Evidência	Documentos que descrevem o processo; documentação da relação SIP-AIP; documentação clara de como os AIPs são derivados dos SIPs.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento

Requisito	**B.2.3** Documentar a disposição final de todos os SIPs.
Evidência	Documentos sobre a disposição final dos SIPs.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.3.1** Seguir procedimentos documentados se um SIP não for incorporado a um AIP ou descartado, e indicar por que o SIP não foi incorporado ou descartado.
Evidência	Logs de processamento do sistema, relatórios de descarte, acordos de submissão, termos de doação, sistema de rastreamento de proveniência; documentação da relação entre SIP e AIP; documentação clara de como os AIPs são derivados dos SIPs; documentação do padrão/processo a partir do qual ocorre a normalização; documentação resultado da normalização e como o AIP resultante é diferente do SIP.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.4** Atribuir aos AIPs identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por exemplo, Handle System, DOI, URN, PURL.
	B.2.4.1 Identificar de maneira única cada AIP dentro do repositório.
	B.2.4.1.1 Ter identificadores únicos.
	B.2.4.1.2 Atribuir e manter identificadores persistentes do AIP e seus componentes, de modo a ser único dentro do contexto do repositório.
	B.2.4.1.3 A documentação deve descrever quaisquer processos usados para mudanças em tais identificadores.
	B.2.4.1.4 Ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais de duplicações.
	B.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos do repositório agora e no futuro próximo, como o número de documentos sob sua custódia.
Evidência	Documentação que descreva a convenção de nomenclatura e a evidência física de sua aplicação (por exemplo, logs)
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.4.2** Ter um sistema confiável de serviços de vínculo para encontrar o objeto identificado de maneira única, independentemente de sua localização física.
Evidência	Documentação que descreva a convenção de nomenclatura e a evidência física de sua aplicação (por exemplo, logs)
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.5** Ter acesso às ferramentas e recursos necessários para fornecer informações de representação oficiais para todos os documentos digitais que contém.
	B.2.5.1 Ter acesso às ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos (por exemplo, PRONOM – base de dados com registro de formatos mantida pelo Arquivo Nacional do Reino Unido) e registros de outras informações de representação.
	B.2.5.2 Ter ferramentas ou métodos para determinar quais informações de representação são necessárias para tornar cada documento digital compreensível para a comunidade alvo.
	B.2.5.3 Ter acesso às informações de representação necessárias.
	B.2.5.4 Ter ferramentas ou métodos para garantir que as informações de representação necessárias sejam persistentemente associadas aos objetos de dados relevantes.

Evidência	Assinatura ou acesso a diretórios de informações de representação (incluindo diretórios de formatos); registros visíveis em diretórios locais (com vínculos persistentes com os documentos digitais); registros em bases de dados que incluam informações de representação e um vínculo persistente com os documentos digitais relevantes.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.6** Ter processos documentados para adquirir informações descritivas de preservação (PDI) para suas informações de conteúdo associadas e adquirir PDI de acordo com os processos documentados.
	B.2.6.1 Ter processos documentados para aquisição de PDI.
	B.2.6.2 Executar seus processos documentados para aquisição de PDI.
	B.2.6.3 Garantir que o PDI está persistentemente associado a informações de conteúdo relevantes.
Evidência	Procedimentos operacionais padrão (POP), manuais que descrevam os procedimentos de admissão; documentação visível sobre como o repositório adquire e gerencia a informação descritiva de preservação (PDI); criação de checksum ou hash, consulta à comunidade-alvo.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.7** Garantir que os documentos digitais contidos nos AIPs são compreensíveis para a comunidade-alvo, no momento da criação do AIP.
	B.2.7.1 Ter um processo documentado para testar a compreensibilidade dos documentos digitais dos AIPs para as comunidades-alvo no momento da sua criação.
	B.2.7.2 Executar o processo de teste para cada classe de informações de conteúdo dos AIPs.
	B.2.7.3 Transformar as informações de conteúdo do AIP até o nível exigido de compreensibilidade, se este falhar no teste de compreensibilidade.
Evidência	Procedimentos de teste a serem executados nos documentos digitais para garantir a compreensibilidade para a comunidade-alvo; registros de tais testes sendo realizados e avaliados; evidências de coleta ou identificação de informações de representação para preencher quaisquer lacunas de inteligibilidade que tenham sido encontradas; retenção de indivíduos com conhecimento técnico na disciplina.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.8** Verificar cada AIP quanto à integridade e exatidão no momento em que é criado.
Evidência	Descrição do procedimento que verifica se os AIPs estão completos e corretos; logs do procedimento.
Seção	**B Gerenciamento do documento digital**
Subseção	B.2 Admissão: criação do pacote de arquivamento
Requisito	**B.2.9** Ter um mecanismo independente para verificar a integridade do conjunto do seu acervo, ou seja, verificar que todos os documentos previstos foram, de fato, admitidos no repositório, justificando possíveis lacunas.
Evidência	Acordos, termos e contratos ente produtor e repositório; logs com datas de recebimento dos documentos; logs de verificações periódicas.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.2** Admissão: criação do pacote de arquivamento
Requisito	**B.2.10** Ter registros atualizados de ações e processos de administração que sejam relevantes para a criação de AIP.
Evidência	Documentação escrita das decisões e/ou ações realizadas, com carimbo do tempo; metadados de preservação registrados, armazenados e vinculados aos documentos pertinentes.

B.3 Planejamento da preservação

Um repositório digital deve fazer o planejamento da preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital, ser bem documentado e incluir:

Seção	**B Gerenciamento do documento digital**
Subseção	**B.3** Admissão: criação do pacote de arquivamento
Requisito	**B.3.1** Estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, por exemplo, a normalização de formatos.
Evidência	Plano de preservação; documentação indicando cada risco de preservação identificado e a estratégia para lidar com esse risco.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.3** Admissão: criação do pacote de arquivamento
Requisito	**B.3.2** Mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável (por exemplo, um formato de arquivo que esteja entrando em desuso, um suporte que esteja no final de sua vida útil).
Evidência	Teste de compreensibilidade, pesquisa sobre comunidade-alvo.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.3** Admissão: criação do pacote de arquivamento
Requisito	**B.3.2.1** Mecanismos para monitorar e notificar quando as informações de representação forem inadequadas para a comunidade designada compreender os acervos de dados.
Evidência	Inscrição em um serviço de diretório de informações de representação; inscrição em um serviço de vigilância tecnológica, pesquisas entre os membros da comunidade-alvo, processos de trabalho relevantes para tratar essas informações.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.3** Admissão: criação do pacote de arquivamento
Requisito	**B.3.3** Mecanismos de mudanças do plano de preservação como resultado do monitoramento.
Evidência	Planos de preservação vinculados à vigilância tecnológica formal ou informal; planejamento ou processos de preservação programados para intervalos mais curtos (por exemplo, não mais de cinco anos); prova de atualizações frequentes de políticas de preservação e planos de preservação; seções das políticas de preservação que tratem de como os planos podem ser atualizados e da frequência com que os planos devem ser revisados e reafirmados ou atualizados.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.3** Admissão: criação do pacote de arquivamento
Requisito	**B.3.3.1** Mecanismos para a criação, identificação ou recolhimento de qualquer informação de representação extra que seja necessária.
Evidência	Inscrição em um serviço de diretório de formatos; inscrição em um serviço de vigilância tecnológica; planos de preservação.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.3** Admissão: criação do pacote de arquivamento
Requisito	**B.3.4** Fornecimento de evidências sobre a eficácia do plano de preservação.
Evidência	Coleta de metadados de preservação apropriados; prova de usabilidade de documentos digitais mantidos dentro do sistema, selecionados aleatoriamente; histórico demonstrável de retenção de documentos digitais utilizáveis ao longo do tempo; pesquisas sobre a comunidade-alvo.

B.4 Armazenamento e preservação/manutenção do AIP

Um repositório deve atender a um conjunto de condições para garantir o bom desempenho da preservação de longo prazo dos AIPs. Tais condições são:

Seção	**B Gerenciamento do documento digital**
Subseção	**B.4** Armazenamento e preservação/manutenção do AIP
Requisito	**B.4.1** Ter especificações de como os AIPs são armazenados até o nível dos bits.
Evidência	Documentação do formato dos AIPs; descrições dos componentes de dados EAST e Data Entity Dictionary Specification Language (DEDSL).
Seção	**B Gerenciamento do documento digital**
Subseção	**B.4** Armazenamento e preservação/manutenção do AIP
Requisito	**B.4.1.1** Preservar as informações de conteúdo dos AIPs.
Evidência	Documentação dos procedimentos de fluxo de trabalho de preservação; documentação dos procedimentos de fluxo de trabalho; documentos da política de preservação que especifiquem o tratamento dos AIPs e sob que circunstâncias eles podem ser excluídos; capacidade de demonstrar a sequência de conversões de um AIP para qualquer documento digital específico ou grupo de objetos ingeridos; documentação que vincule os objetos admitidos aos AIPs atuais.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.4** Armazenamento e preservação/manutenção do AIP
Requisito	**B.4.1.2** Monitoramento constante da integridade dos AIPs, por meio do registro de metadados de fixidade e de logs de checagem dessa integridade (por exemplo, checksum).
Evidência	Documentação dos procedimentos de fluxo de trabalho de preservação; documentação dos procedimentos de fluxo de trabalho; documentos da política de preservação que especifiquem o tratamento dos AIPs e sob que circunstâncias eles podem ser excluídos; capacidade de demonstrar a sequência de conversões de um AIP para qualquer documento digital específico ou grupo de objetos ingeridos; documentação que vincule os objetos admitidos aos AIPs atuais.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.4** Armazenamento e preservação/manutenção do AIP
Requisito	**B.4.2** Ter registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIPs.
Evidência	Informações de fixidez (por exemplo, checksums) para cada documento digital/AIP admitido; logs de verificação de fixidez; documentação de como as informações de fixidez e os AIPs são mantidos separados; documentação de como os AIPs e as listagens de entrada são mantidos separados.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.4** Armazenamento e preservação/manutenção do AIP
Requisito	**B.4.2.1** Ter procedimentos para todas as ações realizadas em AIPs.
Evidência	Documentação escrita que descreva todas as ações que podem ser executadas em um AIP.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.4** Armazenamento e preservação/manutenção do AIP
Requisito	**B.4.2.2** Ser capaz de demonstrar que quaisquer ações realizadas sobre AIPs observaram a conformidade com a especificação dessas ações.
Evidência	Metadados de preservação registrados, armazenados e vinculados ao documento digital pertinente, e documentação dessa ação; auditorias procedimentais do repositório mostrando que todas as ações estão em conformidade com os processos documentados.

As migrações podem provocar alterações na forma e no conteúdo do documento, entretanto, no caso de documentos arquivísticos, não se admite a alteração de conteúdo. As migrações e quaisquer alterações da forma documental daí decorrentes devem ser registradas como metadados, a fim de apoiar a presunção de autenticidade do documento.

B.5 Gerenciamento de informação

Uma funcionalidade essencial de um repositório digital confiável é o gerenciamento da informação, aqui entendido como a gestão das informações descritivas (metadados) dos documentos admitidos no repositório. O principal objetivo desses metadados é apoiar o acesso e a recuperação dos documentos, e eles vão além das informações descritivas mais usuais (autor, título, data), envolvendo outras também úteis aos usuários, tais como o tamanho do arquivo disponível para download ou informação sobre a aplicação necessária para ler o arquivo. O gerenciamento da informação descritiva envolve os seguintes aspectos:

Seção	**B Gerenciamento do documento digital**
Subseção	**B.5** Gerenciamento de informação
Requisito	**B.5.1** Metadados mínimos que permitam a busca e localização dos documentos – esses metadados devem ser identificadores conhecidos pela comunidade-alvo de usuários (por exemplo, número de matrícula do servidor público, título de livro numa biblioteca, número de processo).
Evidência	Informações descritivas e de recuperação, metadados descritivos como Encoded Archival Description (EAD), Nobrade, ISAD(G), e outras documentações que descrevam o documento digital.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.5** Gerenciamento de informação
Requisito	**B.5.2** Captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao AIP correspondente.
Evidência	Metadados descritivos; identificador ou localizador único persistente, interno ou externo, associado ao AIP; documentação do sistema e arquitetura técnica; acordos com depositantes; documentação da política de metadados, incorporando detalhes dos requisitos de metadados e uma declaração descrevendo onde recai a responsabilidade por sua aquisição; documentação do fluxo de trabalho do processo.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.5** Gerenciamento de informação
Requisito	**B.5.3** Integridade referencial entre os AIPs e sua informação descritiva (metadados), ou seja, todo AIP deve ter uma informação descritiva, e toda informação descritiva deve apontar para um AIP.
Evidência	Metadados descritivos; identificador ou localizador único e persistente associado ao AIP; relação documentada entre o AIP e seus metadados; documentação do sistema e arquitetura técnica; documentação do fluxo de trabalho do processo.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.5** Gerenciamento de informação
Requisito	**B.5.3.1** Permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o AIP e seus metadados descritivos – nesse caso, o repositório deve ser capaz de restaurar a relação rompida.
Evidência	Log detalhando a manutenção contínua ou verificação da integridade dos dados e suas relações com as informações descritivas associadas, especialmente após o reparo ou modificação do AIP; informações descritivas legadas; persistência do identificador ou localizador; relação documentada entre AIP e suas informações descritivas; documentação do sistema e arquitetura técnica; documentação do fluxo de trabalho do processo.

B.6 Gerenciamento de acesso

O termo acesso possui vários sentidos, incluindo acesso por usuários ao sistema do repositório, por exemplo, segurança física e autenticação do usuário, e as diferentes fases de acesso aos documentos digitais (fazer uma solicitação, verificar os direitos do solicitante e preparar e enviar um pacote de informação para disseminação – DIP). Esta subseção trata de todos esses elementos e está relacionada à existência e implementação de políticas de acesso e à capacidade do repositório de fornecer documentos comprovadamente autênticos como DIPs.

Seção	**B Gerenciamento do documento digital**
Subseção	**B.6** Gerenciamento de acesso
Requisito	**B.6.1** Cumprir as políticas de acesso.
Evidência	Declarações de políticas que estejam disponíveis para as comunidades de usuários; informações sobre as autorizações do usuário (matrizes de autenticação); logs e trilhas de auditoria de solicitações de acesso; testes explícitos de alguns tipos de acesso.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.6** Gerenciamento de acesso
Requisito	**B.6.1.1** Registrar e revisar todas as falhas e anomalias de gestão de acesso.
Evidência	Logs de acesso, capacidade do sistema de usar ferramentas automatizadas de análise/monitoramento e gerar mensagens de problema/erro; anotações de revisões realizadas ou ações tomadas como resultado das revisões.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.6** Gerenciamento de acesso
Requisito	**B.6.2** Seguir políticas e procedimentos que possibilitem a disseminação de documentos digitais rastreáveis até os originais, com evidências que comprovem sua autenticidade.
Evidência	Documentos de desenho do sistema; instruções de trabalho (se os DIPs envolverem processamento manual); passo a passo do processo; produção de cópia de amostra com comprovação de autenticidade; documentação dos requisitos da comunidade para evidências de autenticidade.
Seção	**B Gerenciamento do documento digital**
Subseção	**B.6** Gerenciamento de acesso
Requisito	**B.6.2.1** Registrar e agir sobre os relatórios de problemas sobre erros nos dados ou respostas dos usuários.
Evidência	Documentos de desenho do sistema; instruções de trabalho (se os DIPs envolverem processamento manual); passo a passo do processo; registros de pedidos e produção de DIP; documentação de relatórios de erros e as ações tomadas.

C. Tecnologia, infraestrutura técnica e segurança

Esses requisitos não prescrevem hardware e software específicos para garantir a preservação de longo prazo dos AIPs, mas apenas descrevem as melhores práticas das áreas de gestão de dados e segurança, que devem ser atendidas por um repositório digital confiável.

O repositório deve adotar uma tecnologia de hardware e software apropriada para os serviços que presta, procedimentos para recebimento e monitoramento de notificações e para avaliação da necessidade de mudanças na tecnologia utilizada.

C.1 Infraestrutura de sistema

Um repositório deve possuir uma infraestrutura tecnológica robusta, de maneira a apoiar a confiabilidade dos AIPs nele mantidos. Para tanto, deve observar os seguintes aspectos:

Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1** Identificar e gerenciar os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema.
Evidência	Inventário de infraestrutura de componentes do sistema; avaliações periódicas de tecnologia; estimativas da vida útil dos componentes do sistema; exportação de registros autênticos para um sistema independente; uso de software fortemente apoiado pela comunidade (por exemplo, Apache, iRODS, Fedora); recriação de arquivos a partir de backups.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1** Empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Evidência	Relatórios periódicos de gerenciamento e avaliação de tecnologia. Comparação da tecnologia existente com cada nova avaliação.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.1** Ter tecnologias de hardware adequadas aos serviços que fornece às comunidades-alvo.
Evidência	Manutenção de tecnologia, expectativas e perfis de uso atualizados da comunidade-alvo; fornecimento de largura de banda adequada para suportar as demandas de admissão e uso; produção sistemática de feedback sobre a adequação de hardware e serviços; manutenção de um inventário atual de hardware.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.2** Ter procedimentos em vigor para monitorar e receber notificações quando mudanças na tecnologia de hardware forem necessárias.
Evidência	Manutenção de tecnologia, expectativas e perfis de uso atualizados da comunidade-alvo; fornecimento de largura de banda adequada para suportar as demandas de admissão e uso; produção sistemática de feedback sobre a adequação de hardware e serviços; manutenção de um inventário atual de hardware.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.3** Ter procedimentos em vigor para avaliar quando são necessárias mudanças no hardware atual.
Evidência	Procedimentos de avaliação em vigor; experiência documentada da equipe em cada subsistema de tecnologia.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.4** Ter procedimentos, compromisso e financiamento para substituir hardware quando as avaliações indicarem a necessidade de fazê-lo.
Evidência	Procedimentos de avaliação em vigor; experiência documentada da equipe em cada subsistema de tecnologia.

Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.5** Ter tecnologias de software adequadas aos serviços que fornece às suas comunidades-alvo.
Evidência	Manutenção de tecnologia, expectativas e perfis de uso da comunidade designada atualizados; fornecimento de software adequado para suportar as demandas de admissão e uso; obtenção sistemática de feedback sobre a adequação do software e do serviço; manutenção de um inventário de software atualizado.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.6** Ter procedimentos para monitorar e receber notificações quando mudanças de software forem necessárias.
Evidência	Auditorias de capacidade comparada com uso real; auditorias de taxas de erro observadas; auditorias de gargalos de desempenho que limitem a capacidade de atender aos requisitos de acesso da comunidade de usuários; documentação de avaliações de vigilância tecnológica; documentação de atualizações de software de fornecedores.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.7** Ter procedimentos em vigor para avaliar quando são necessárias mudanças no software atual.
Evidência	Procedimentos de avaliação em vigor; experiência documentada da equipe em cada subsistema de tecnologia de software.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.1.8** Ter procedimentos, compromisso e financiamento para substituir o software quando a avaliação indicar a necessidade de fazê-lo.
Evidência	Declaração de compromisso de fornecer os níveis de serviço previstos e contratados; evidências de ativos financeiros contínuos reservados para aquisição de software; demonstração da redução de custos, por meio do custo amortizado do novo sistema.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.2** Ter suporte de hardware e software adequados para funcionalidade de backup suficiente para preservar os documentos do repositório e recuperar as funções do repositório.
Evidência	Relatórios frequentes de backup; logs de auditoria/inventário de backups; validação de backups concluídos; plano, política e documentação de recuperação de desastres; exercícios contra incêndio; testes de backups; contratos de suporte para hardware e software de mecanismos de backup; preservação demonstrada de metadados do sistema, como controles de acesso, localização de réplicas, trilhas de auditoria e valores de checksum.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.3** Ter mecanismos efetivos para a detecção de corrupção ou perda de bits.
Evidência	Documentos que especifiquem os mecanismos usados para detecção e correção de erros de bits; análises de risco; relatórios de erros; análises de ameaças; análise periódica da integridade dos acervos do repositório.

Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.3.1** Registrar e relatar à sua administração todos os incidentes de corrupção ou perda de dados, e medidas que devem ser tomadas para reparar/substituir dados corrompidos ou perdidos.
Evidência	Procedimentos relacionados ao relato de incidentes aos administradores; registros de metadados de preservação (por exemplo, PDI); comparação de logs de erros com relatórios para a administração; procedimentos de expansão relacionados à perda de dados; rastreamento das origens de incidentes; ações de remediação tomadas para remover fontes de incidentes.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.4** Ter um processo para registrar e reagir à disponibilidade de novas atualizações de segurança, com base em uma avaliação de risco-benefício.
Evidência	Listagem de riscos (lista de todos os *patches* disponíveis e análise de documentação de risco); evidência de processos de atualização (por exemplo, daemon de gerenciamento de atualização do servidor); documentação relacionada à instalação de atualizações.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.5** Ter previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de hardware.
Evidência	Documentação de processos de migração; políticas relacionadas a suporte, manutenção e substituição de hardware; documentação dos ciclos de vida de suporte definidos pelo fabricante do hardware; políticas relacionadas à migração de documentos para sistemas de hardware alternativos.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.6** Ter identificado e documentado os processos críticos que afetam sua capacidade de cumprir suas responsabilidades obrigatórias.
Evidência	Matriz de rastreabilidade entre processos e requisitos obrigatórios.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.6.1** Ter documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias.
Evidência	Documentação do processo de gerenciamento de alterações; avaliação do risco associado a uma alteração de processo; análise do impacto esperado de uma alteração de processo; comparação de logs de alterações reais nos processos com análises do impacto e criticidade delas.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.1.6.2** Ter um processo para testar e avaliar o efeito das mudanças nos processos críticos do repositório.
Evidência	Procedimentos de teste documentados; documentação dos resultados dos testes anteriores e comprovação das alterações feitas em decorrência dos testes; análise do impacto de uma alteração de processo.

Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.2** Gerenciar o número e localização das cópias de todos os documentos digitais.
Evidência	Testes de recuperação aleatória; validação da existência do objeto para cada local registrado; validação de um local registrado para cada objeto em sistemas de armazenamento; informações de verificação de proveniência e fixidez; listagem de localização/log dos documentos digitais, comparado com o número e localização esperados de suas cópias.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.1** Infraestrutura de sistema
Requisito	**C.1.2.1** Ter mecanismos para garantir que qualquer cópia dos documentos digitais esteja sincronizada.
Evidência	Fluxos de trabalho de sincronização; análise sistemática de quanto tempo leva para as cópias serem sincronizadas; procedimentos/documentação de processos de sincronização.

C.1 Gestão de risco e segurança

A segurança do repositório não se limita a aspectos de tecnologia, mas abrange também instalações físicas e ações de pessoas. Os aspectos de segurança incluem:

Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.2** Gestão de risco e segurança
Requisito	**C.2.1** Análise sistemática de dados, sistemas, pessoas e instalação física.
Evidência	Emprego de práticas e certificações da série ISO 27000.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.2** Gestão de risco e segurança
Requisito	**C.2.2** Adoção de procedimentos de controle para tratar adequadamente as necessidades de segurança.
Evidência	O repositório emprega os códigos de prática encontrados na série de padrões ISO 27000; lista de controle do sistema; análises de risco, ameaça ou controle; e adição de controles com base na detecção e avaliação contínua de riscos. O repositório mantém a certificação ISO/IEC 27002.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.2** Gestão de risco e segurança
Requisito	**C.2.3** Delineamento de funções, responsabilidades e autorizações relativas à implementação de mudanças no sistema.
Evidência	O repositório emprega os códigos de prática encontrados na série de padrões ISO 27000; organograma; documentação de autorização do sistema. O repositório mantém a certificação ISO/IEC 27002.
Seção	**C Tecnologia, infraestrutura técnica e segurança**
Subseção	**C.2** Gestão de risco e segurança
Requisito	**C.2.4** Plano de prevenção de desastres e de reparação, que inclua, ao menos, um backup, offsite, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.
Evidência	O repositório emprega os códigos de prática encontrados na série de padrões ISO 27000; planos de desastre e recuperação; informações sobre e prova de pelo menos uma cópia offsite de informações preservadas; plano de continuidade do serviço; documentação ligando funções com atividades; dados geológicos, geográficos ou meteorológicos locais ou avaliações de ameaças. O repositório mantém a certificação ISO/IEC 27002.

D. Princípios

A seguir serão apresentados os princípios a serem cumpridos por um repositório digital de documentos arquivísticos.

Princípio	**D.1** A responsabilidade pelo projeto, implantação, manutenção e governança de um repositório digital de documentos arquivísticos deve ser compartilhada por profissionais de arquivo, de tecnologia da informação e da administração da instituição, de forma a se cumprirem os requisitos tecnológicos, os procedimentos do tratamento arquivístico e a disponibilidade de recursos. A instituição de um comitê ou comissão de governança de caráter permanente com competências e responsabilidades definidas por portaria ou instrumento equivalente. A equipe deve ser multidisciplinar e presidida por profissional de arquivo.	
Princípio	**D.2** Um repositório digital para documentos arquivísticos tem que ser capaz de organizar e recuperar os documentos, de forma a manter a relação orgânica entre eles. Nesse sentido, deve apoiar a organização hierárquica dos documentos digitais, a partir de um plano de classificação de documentos, e a descrição multinível, de acordo com a norma internacional para descrição arquivística: Norma Geral Internacional de Descrição Arquivística, ISAD(G) e Norma Brasileira de Descrição Arquivística (Nobrade).	
Princípio	**D.3** Princípios de preservação digital	
	A preservação digital tem que garantir o acesso de longo prazo a documentos arquivísticos autênticos, o que implica na adoção dos seguintes princípios:	
Princípio	**D.3.1** Focar especificamente em documentos arquivísticos e não em objetos digitais de forma genérica.	
	D.3.2 Focar em documentos arquivísticos digitais autênticos.	
	D.3.3 Reconhecer que a preservação digital é um processo contínuo, que começa na concepção do documento.	
	D.3.4 Reconhecer que a autenticidade dos documentos arquivísticos digitais tem por base os procedimentos de gestão e preservação, e a confiança tanto no repositório como no órgão responsável pela guarda desses documentos.	**Obs**.: ver resolução n. 37, de 19 de dezembro de 2012, do Conarq, que aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais.
	D.3.5 Arbitrar o que se considera como documento original, uma vez que a preservação digital implica a necessidade de conversão de formatos e atualização de suportes.	
	D.3.6 Reconhecer que a elaboração de manuais e os procedimentos de preservação desempenhados pelo repositório digital apoiam a presunção de autenticidade desses documentos.	
	D.3.7 Reconhecer que o registro, em metadados, das intervenções de preservação em cada documento apoia a presunção de autenticidade desses documentos.	
	D.3.8 Reconhecer que a autenticidade dos documentos digitais deve ser avaliada e presumida no momento de sua submissão ao repositório.	**Obs**.: ver resolução n. 24, de 3 de agosto de 2006, do Conarq, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas.
	D.3.9 Reconhecer que o repositório digital é responsável pela manutenção permanente da autenticidade dos documentos a ele submetidos.	
	D.3.10 Distinguir, claramente, a autenticidade e a autenticação de documentos, considerando que a primeira é a qualidade de o documento ser verdadeiro e a segunda é uma declaração dessa qualidade, feita, em dado momento, por pessoa autorizada.	

Princípio	D.4 Independência dos repositórios
	Um repositório digital deve ter independência. Isso significa que seu funcionamento e o acesso aos documentos não podem depender das aplicações que funcionam em conjunto com ele. Por exemplo, em uma aplicação para arquivos correntes e intermediários, deve ser possível acessar os documentos independentemente do Sigad, isto é, diretamente no repositório, desde que isso seja feito de forma controlada, para não ameaçar a autenticidade dos documentos no repositório. É bom esclarecer que o acesso direto aos documentos no repositório não exclui a necessidade de um Sigad para apoiar a gestão arquivística.
Princípio	**D.5 Interoperabilidade**
	Um repositório digital deve estar em conformidade com as normas e padrões estabelecidos, de forma a possibilitar níveis de interoperabilidade com outros repositórios digitais e sistemas informatizados que tratam de documentos arquivísticos. Podem ser citados como exemplos dessas normas e padrões: o Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH) para coleta de registros de metadados em repositórios digitais; o Metadata Encoding and Transmission Standard (METS) para a codificação de metadados descritivos, administrativos e estruturais; o Encoded Archival Description (EAD) para a codificação de metadados descritivos de documentos arquivísticos; e os Padrões de Interoperabilidade de Governo Eletrônico – e-PING,19 no caso dos órgãos e entidades do governo federal.

19 Informações disponíveis em: http://www.gov.br/governodigital/pt-br/governanca-de-dados/padroes-de-interoperabilidade.

ARQUIVO NACIONAL

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO