UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL
EM PATRIMÔNIO CULTURAL

Henrique Machado dos Santos

AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS: UMA ANÁLISE DAS NORMAS ISO 14721 E ISO 16363

Santa Maria, RS
2018

Henrique Machado dos Santos

AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS: UMA ANÁLISE DAS NORMAS ISO 14721 E ISO 16363

Dissertação apresentada ao Curso de Pós-Graduação Profissional em Patrimônio Cultural, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Patrimônio Cultural**.

Orientador: Profº Drº. Daniel Flores

Santa Maria, RS
2018

Santos, Henrique Machado
Auditoria de repositórios arquivísticos digitais confiáveis: uma convergência entre as normas ISO 14721 e ISO 16363 / Henrique Machado Santos.- 2018.
284 p.; 30 cm

Orientador: Daniel Flores
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Patrimônio Cultural, RS, 2018

1. Patrimônio cultural 2. Documento digital 3. Arquivologia 4. Preservação digital 5. Repositório digital I. Flores, Daniel II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.

Endereço: rua das Acácias, Nº 340, Bairro Caiçara, Agudo, RS. CEP: 96540-000

E-mail: henrique.hms.br Fone: (55) 996371426

Henrique Machado dos Santos

CRITÉRIOS PARA AUDITORIA E CERTIFICAÇÃO DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Dissertação apresentada ao Curso de Pós-Graduação Profissional em Patrimônio Cultural, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Patrimônio Cultural**.

Aprovado em 05 de março de 2018:

Daniel Flores, Drª (UFSM)
(Presidente/Orientador)

Gustavo Zanini Kantorski, Drº (UFSM)

Rafael Port Rocha, Drº (UFRGS)

Gilberto Fladimar Rodrigues Viana, Drº (UFSM)
(Suplente)

Santa Maria, RS
2018

DEDICATÓRIA

Para meus pais:

Alberi Guedes dos Santos (*in memorian*)
Ana Maria Machado

Dia dos pais (13/08/2017).

AGRADECIMENTOS

A Universidade Federal de Santa Maria, pelo ensino gratuito e de qualidade;

Aos professores e funcionários do Programa de Pós-Graduação Profissional em Patrimônio Cultural, respectivamente, pelos ensinamentos proporcionados e serviços prestados;

Ao meu orientador, professor Daniel Flores, pela amizade, confiança e incentivo;

Aos membros da comissão avaliadora, Gustavo Zanini Kantorski, Rafael Port Rocha e Gilberto Fladimar Rodrigues Viana, pelas dicas e sugestões que certamente vem a contribuir com este trabalho;

Aos professores do Curso de Arquivologia da UFSM, que até hoje mantém uma relação de amizade e incentivo;

Aos colegas de mestrado pela boa convivência e união durante essa trajetória;

A meu pai (*in memorian*), por ter me apoiado até o último instante de sua vida;

A minha mãe por ter me apoiado em todos os momentos, inclusive nos mais difíceis;

Aos meus ex-colegas de serviço do MMT Advogados Associados, pelo apoio e amizade. Com estes tive o prazer de compartilhar duas grandes realizações: a aprovação no mestrado, e uma nomeação em concurso público;

Aos meus atuais colegas de trabalho da Coordenação de Arquivo Geral da Universidade Federal do Rio Grande, pelo acolhimento, incentivo e força prestada;

Aos meus familiares em geral, por todo o incentivando prestado;

Aos meus amigos, conhecidos e colegas arquivistas, sempre presentes, seja pessoalmente, seja através das redes sociais. Tenho muito a agradecer pelo incentivo de cada pequena vitória conquistada e por manter amizades saudáveis e que foram capazes de acrescentar muito em minha vida até o momento.

O saber humano se espalha para todos os lados, a perder de vista, de modo que nenhum indivíduo pode saber sequer a milésima parte daquilo que é digno de ser sabido.
(Arthur Schopenhauer)

Esta, porém, é a minha doutrina: quem quiser um dia aprender a voar deve primeiro aprender a ficar de pé e a caminhar e correr e escalar e dançar: não se pode aprender a voar voando!
(Friedrich Nietzsche)

Estamos na era do primitivismo digital. Tudo que fazemos agora terá um impacto nos registros que serão acessados no futuro. Porém, parte dessa história corre o perigo de se perder em sequências de bits, estruturadas em bytes sem leitura no futuro. É a obsolescência tecnológica. Para cuidar dela, usamos técnicas de preservação digital que poderão, daqui a alguns anos, ajudar nossos descendentes a entenderem os dias de hoje.
(Charlley Luz)

O documento arquivístico constitui o registro de ações humanas independentemente da forma como se apresenta e da base em que se encontra afixado.
(Rosely Curi Rondinelli)

RESUMO

AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS: UMA ANÁLISE DAS NORMAS ISO 14721 E ISO 16363

AUTOR: Henrique Machado dos Santos
ORIENTADOR: Daniel Flores

Este estudo tem por objetivo contextualizar e discutir a aplicabilidade das normas OAIS – ISO 14721:2012 e ACTDR – ISO 16363:2012 no âmbito dos repositórios arquivísticos digitais confiáveis. Para isto, analisa-se inicialmente o modelo funcional OAIS no contexto da Arquivística, enfatizando as perspectivas de preservação e garantia de acesso a documentos autênticos no longo prazo. Posteriormente, o padrão de auditoria ACTDR é analisado vislumbrando a sua aplicabilidade aos repositórios arquivísticos digitais em conformidade com o OAIS. A metodologia consiste em uma pesquisa de natureza aplicada, na qual a coleta de dados é realizada por meio de fichamentos, os quais são planificados através de um instrumento de banco de dados. A coleta de dados parte, essencialmente, de um levantamento documental, contemplando normas e recomendações às quais compõe o núcleo deste estudo. E em caráter complementar, utiliza-se o levantamento bibliográfico, composto por materiais previamente publicados, como livros, teses, dissertações e artigos científicos recuperados pela ferramenta de busca *Google Scholar*. A análise do OAIS demonstra que há conformidade teórica com a Arquivística, embora não esteja explícito, é possível moldar um repositório arquivístico com base em seus requisitos. Com isto, um repositório em conformidade com o OAIS poderá contemplar princípios como, proveniência e unicidade, além de se enquadrar no contexto das sete funções arquivísticas. O modelo funcional OAIS conceitua estruturas de pacotes e objetos de informação, os quais contemplam propriedades fundamentais à preservação, manutenção da autenticidade e garantia de acesso aos documentos digitais. Logo, o OAIS é considerado um pré-requisito na implementação de um repositório arquivístico digital confiável. Em um segundo momento, o padrão de auditoria ACTDR é analisado para explicitar aspectos potencialmente arquivísticos que estão implícitos, assim, seu detalhamento fornece suporte ao processo de auditoria de repositórios arquivísticos digitais confiáveis. O padrão ACTDR se divide em três seções nas quais estão subdivididos os requisitos relacionados a políticas institucionais de preservação digital, gerenciamento dos objetos digitais armazenados e a gestão de segurança e risco do repositório digital. Dentre as contribuições deste estudo, ressalta-se que a implementação de um repositório arquivístico digital confiável deverá, inicialmente, considerar o modelo de referência OAIS, e, em um segundo momento, este repositório deve ser auditado pelo padrão ACTDR. Caso o repositório atinja os níveis de confiabilidade requeridos na auditoria, procede-se a certificação do mesmo, através do órgão competente para tal. Por fim, a complementação deste estudo consiste na elaboração de um produto, o "manual para auditoria de repositórios arquivísticos digitais confiáveis", estabelecendo assim, um diálogo entre o OAIS e ACTDR, além de considerar os aspectos arquivísticos pertinentes na preservação de longo prazo. Este manual sintetiza os conhecimentos discutidos para servir como orientação aos arquivistas que atuam no âmbito dos repositórios arquivísticos digitais.

Palavras-chave: Patrimônio cultural. Documento digital. Arquivologia. Preservação digital. Repositório digital.

ABSTRACT

AUDIT OF TRUSTWORTHY DIGITAL ARCHIVAL REPOSITORIES: AN ANALYSIS OF STANDARDS ISO 14721 AND ISO 16363

AUTHOR: Henrique Machado dos Santos
ADVISOR: Daniel Flores

This study aims to contextualize and discuss the applicability of OAIS - ISO 14721: 2012 and ACTDR - ISO 16363: 2012 standards in the context of trustworthy digital archival repositories. For this, the OAIS functional model is analyzed initially in the context of Archives, emphasizing the perspectives of preservation and guarantee of access to authentic documents in the long term. Subsequently, the ACTDR audit standard is analyzed by looking at its applicability to OAIS-compliant digital archival repositories. The methodology consists of a research of an applied nature, in which the data collection is carried out by means of records, which are planned through a database instrument. The data collection is based essentially on a documentary survey, contemplating norms and recommendations to which it composes the nucleus of this study. And in a complementary way, a bibliographic survey is used, consisting of previously published materials such as books, theses, dissertations and scientific articles retrieved by the Google Scholar search tool. The OAIS analysis demonstrates that there is theoretical compliance with Archival, although it is not explicit, it is possible to shape an archival repository based on its requirements. With this, an OAIS-compliant repository can contemplate principles such as provenance and uniqueness, as well as fit into the context of the seven archival functions. The OAIS functional model conceptualizes packet structures and information objects, which include fundamental properties for preservation, maintenance of authenticity and guarantee of access to digital documents. Therefore, OAIS is considered a prerequisite in the implementation of a trustworthy digital archival repository. In a second moment, the ACTDR audit pattern is analyzed to make explicit the potentially archival aspects that are implicit, so its detailing supports the auditing process of trustworthy digital archival repositories. The ACTDR standard is divided into three sections in which the requirements related to institutional policies of digital preservation, management of stored digital objects and the management of security and risk of the digital repository are subdivided. Among the contributions of this study, it is emphasized that the implementation of a trustworthy digital archival repository should initially consider the OAIS reference model, and, in a second moment, this repository should be audited by the ACTDR standard. In case the repository reaches the levels of reliability required in the audit, it is certified by the appropriate body. Finally, the complement of this study consists of the elaboration of a product, the "Manual for Auditing Reliable Digital Archival Repositories", thus establishing a dialogue between OAIS and ACTDR, in addition to considering archival aspects pertinent to long-term preservation. This manual synthesizes the knowledge discussed to serve as guidance to archivists working within digital archival repositories.

Keywords: Cultural heritage. Digital record. Archival Science. Digital preservation. Digital repository.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ACTDR	*Audit and Certification of Trustworthy Digital Repositories*
AIP	*Archival Information Package*
AIC	*Archive Information Collection*
AIU	*Archival Information Unit*
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCSDS	*Consultative Committee for Space Data System*
CD	*Compact Disc*
CODEARQ	Cadastro Nacional de Entidades Custodiadoras de Acervos Arquivísticos
CONARQ	Conselho Nacional de Arquivos
CRL	*The Center for Research Libraries*
DCC	*Digital Curation Centre*
DIP	*Dissemination Information Package*
DPE	*DigitalPreservationEurope*
DRAMBORA	*Digital Repository Audit Method Based on Risk Assessment*
DVD	*Digital Versatile Disc*
INTERPARES	*International Research on Permanent Authentic Records in Electronic Systems*
ISO	*International Organization for Standardization*
LAI	Lei de acesso à informação
MoReq	*Model Requirements for the Management of Electronic Records*
NBR	Norma Brasileira Recomendada
NESTOR	*Network of Expertise in long-term STORage*
NOBRADE	Norma Brasileira de Descrição Arquivística
OAIS	*Open Archival Information System*
PDI	*Preservation Description Information*
RDC-Arq	Repositório Arquivístico Digital Conviável
RLG	*Research Libraries Group*
SAAI	Sistema Aberto de Arquivamento de Informação
SINAR	Sistema Nacional de Arquivos
SIP	*Submission Information Package*
TRAC	*Trustworthy Repository Audit & Certification: Criteria and Checklist*

SUMÁRIO

1 INTRODUÇÃO

Tendo em vista a constante evolução das tecnologias da informação e consequente proliferação de documentos digitais, pode-se dizer que a Arquivística vivencia um período de reformulação. Nesse sentido, as práticas de gestão e preservação do patrimônio digital ganham relevância devido ao grande volume de documentos digitais produzidos.

A preservação digital vem se configurando como um dos principais desafios da Arquivística contemporânea. Produzem-se cada vez mais documentos digitais, e esta produção acelerada é inversamente proporcional às práticas de preservação em longo prazo. Tal fato vem se caracterizando como uma ameaça à memória digital das sociedades contemporâneas, que muito dependem das tecnologias e dos documentos digitais; tanto para continuar evoluindo, quanto para disponibilizar conhecimentos para as futuras gerações.

No cenário atual, já existem metodologias, como por exemplo, a implementação de estratégias, padrões de metadados e repositórios, que visam minimizar os efeitos da obsolescência tecnológica. Tais ações têm o objetivo de preservar e proporcionar o acesso em longo prazo aos documentos arquivísticos digitais, de modo que o repositório digital irá gerenciar a implementação das estratégias e padrões de metadados.

Entretanto, o fato dessa temática ser recente atribui dúvidas com relação à confiança depositada pelos usuários potenciais; visto que, as instituições de memória tradicionais como arquivos, bibliotecas e museus, demoraram um tempo considerável para ganhar a confiança do público. Logo, a demanda por documentos digitais é uma transformação que ainda precisa de um tempo para ser assimilada pelo público, bem como pelos profissionais da área; e para estes, compete agora, a preservação de documentos analógicos e digitais. Mesmo assim, em um contexto no qual não há metodologias consagradas para preservação digital será necessário implementar estratégias e repositórios, visto que estas ações são os primeiros passos para atingir os níveis de confiança desejada.

A delimitação do tema do presente trabalho consiste na preservação de documentos arquivísticos digitais em longo prazo em um repositório arquivístico digital confiável (RDC-Arq). Ressalta-se aqui, a questão da confiabilidade devido ao

comprometimento das instituições de memória em demonstrar que o patrimônio documental custodiado é autêntico.

Nesse sentido, as práticas de auditoria dos repositórios consistem em alternativas pertinentes na busca da confiabilidade. Por meio de auditorias periódicas será possível verificar as vulnerabilidades dos repositórios e das políticas de preservação, e assim buscar soluções que melhorem os níveis de qualidade. E posteriormente, as atividades de certificação atuarão como um complemento frente à auditoria, demostrando que um determinado repositório digital atingiu um determinado nível de confiabilidade.

A literatura técnica de preservação digital define o *Open Archival Information System* (OAIS) como o padrão para implementação de repositórios digitais, visto que se tornou a norma ISO 14721:2012, a qual foi traduzida para o Brasil sob a recomendação ABNT/NBR 15472:2007. Ressalta-se que mesmo estando em conformidade com uma norma ISO, os repositórios digitais precisam ser auditados e certificados para agregar confiabilidade.

No âmbito da auditoria de repositórios digitais, observa-se que há algumas iniciativas, dentre elas: *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC) (RLG/NARA, 2007), *Audit And Certification of Trustworthy Digital Repositories* (ACTDR) (CCSDS, 2011), *Catalogue of Criteria for Trusted Digital Repositories* da *Network of Expertise in long-term STORage* (NESTOR) (NESTOR, 2006) e *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) (DCC/DPE, 2007).

Considerando o contexto apresentado, observa-se que as atividades de auditoria e certificação são fundamentais para adicionar confiabilidade às instituições que fazem a custódia de documentos arquivísticos digitais. Assim, pode-se definir que o problema da pesquisa consiste em: analisar a aplicabilidade do modelo OAIS e o padrão de auditoria ACTDR no contexto da Arquivística, tendo em vista a implementação de um RDC-Arq.

1.1 JUSTIFICATIVA

O estudo sobre a auditoria de RDC-Arq's se faz necessário em virtude da escassez de estudos que abordem esta temática, sejam eles teses, dissertações ou artigos científicos. Observa-se que diversos estudos vêm discutindo aspectos

relacionados às estratégias de preservação[1] e os repositórios digitais[2], entretanto há pouco avanço com relação às atividades de auditoria e certificação na busca por um RDC-Arq.

A constante evolução das tecnologias da informação e a consequente demanda por documentos digitais vêm estimulando a implementação de repositórios digitais. Da mesma forma, ainda não há a confiança esperada pela comunidade designada e pelos usuários potenciais, e estima-se que esta seja atingida através de procedimentos de auditoria e certificação; exercendo assim, um papel renovador no que tange a preservação digital em longo prazo.

Analisar os padrões de auditoria permitirá verificar o padrão recomendável, que contemple os principais critérios para auditar e certificar repositórios digitais que seguem o modelo funcional OAIS. Considerando o caráter genérico de aplicabilidade do OAIS, pode-se dizer que a compilação de tais critérios observados constitui um instrumento de abrangência considerável: que pode auxiliar diretamente no caso dos RDC-Arq's, além de fornecer contribuições para os demais tipos de repositórios digitais, como por exemplo, temáticos, dados de pesquisa, biblioteconômicos, etc.

1.2 OBJETIVOS

A seguir será apresentado o objetivo geral e os objetivos específicos deste estudo.

1.2.1 Objetivo Geral

Desenvolver uma análise sistemática do modelo OAIS e o do padrão ACTDR, no âmbito da Arquivística, para auxiliar no desenvolvimento de um RDC-Arq, tendo em vista o preparo para futura certificação.

1.2.2 Objetivos Específicos:

[1] A implementação das estratégias de migração, emulação, encapsulamento, refrescamento e

[2] Brasil (2014), Fernal e Vechiato (2013), Ferreira (2006), Lopes (2008), Márdero Arellano (2008), Márdero Arellano e Leite (2009), Ramalho et al. (2007), Santos e Flores (2015c), Saramago (2004), Sayão (2010), e Thomaz (2007).

- Avaliar a aplicabilidade do modelo funcional OAIS no contexto da Arquivística, com ênfase na preservação e garantia de acesso a documentos autênticos no longo prazo;
- Analisar o padrão ACTDR na auditoria de um RDC-Arq em conformidade com o OAIS;
- Compilar o produto deste estudo na forma de um “manual para auditoria de repositórios arquivísticos digitais confiáveis”, para estabelecer um diálogo entre o OAIS, a Arquivística e o ACTDR.

1.3 ESTRUTURA DE APRESENTAÇÃO

Após realizar a introdução da pesquisa, delimitando tema e problema, e perpassar por justificativa, objetivo geral e objetivos específicos; prossegue-se o seu aprofundamento, conforme os padrões do texto dissertativo-argumentativo.

O próximo capítulo contém a “revisão de literatura” compreende o levantamento dos materiais publicados e, em caráter elucidativo, possui fundamentos básicos similares aos “referenciais teóricos” por se tratar de um tema relativamente recente; visto que a primeira versão do OAIS foi publicada no ano de 2002.

Posteriormente, é apresentado o capítulo “metodologia”, a qual irá classificar a pesquisa com relação à área do conhecimento, à finalidade e aos métodos. Além disso, apresentar as etapas da investigação, as técnicas de coleta de dados e o modo de planificação dos dados obtidos.

Após estabelecer as bases introdutórias e os fundamentos teóricos e metodológicos, procede-se ao capítulo “análise e discussão dos resultados”. Neste, discutem-se aspetos do OAIS com relação a sua aplicabilidade na Arquivística, mais precisamente, quanto à preservação de documentos arquivísticos digitais. Na sequência da discussão, tem-se a análise do padrão ACTDR. Assim, a aplicabilidade de seus critérios no âmbito do RDC-Arq é discutida, e posteriormente, concatenada na forma de um “manual para auditoria de repositórios arquivísticos digitais confiáveis” o qual é o produto final deste estudo.

E por fim, será apresentado o capítulo “conclusão”, que retoma o atingimento dos objetivos propostos, e faz apontamentos gerais sobre o tema. Desta forma, são

perpassados os aspectos mais pertinentes do OAIS e do ACTDR para elaborar o produto, que é um manual de auditoria de RDC-Arq's voltado para arquivistas.

Desta forma, após perpassar pela delimitação do tema, identificar de um problema, justificar a realização deste estudo e propor objetivos, encerra-se o capítulo de "introdução". O próximo capítulo, "revisão de literatura" apresenta as bases teóricas necessárias para fundamentar e direcionar os objetivos.

2 REVISÃO DE LITERATURA

Neste capítulo são apresentados os fundamentos teóricos que fornecem as bases para o desenvolvimento da pesquisa, bem como um breve apanhado sobre a preservação digital no qual se contextualiza as atividades de auditoria de repositórios digitais. Desta forma, é perpassada a ideia do documento arquivístico digital como parte integrante do patrimônio cultural, e posteriormente descrevem-se aspectos pertinentes à sua preservação em longo prazo.

2.1 PATRIMÔNIO: BREVE CONTEXTUALIZAÇÃO

O conceito de patrimônio é muito amplo e vai além de questões relacionadas à acumulação de riqueza proporcionada pelo sistema capitalista. Em uma perspectiva social e humana, o patrimônio pode ser dividido em três categorias: histórico, cultural e natural.

O patrimônio histórico consiste no conjunto de bens que representam a história de uma sociedade, para isto, ele utiliza de aspectos da arquitetura da época, obras de arte, documentos em geral e objetos que mantenham uma forte relação com o contexto histórico.

> A expressão [patrimônio histórico] designa um bem destinado ao usufruto de uma comunidade que se ampliou a dimensões planetárias, constituído pela acumulação contínua de uma diversidade de objetos que se congregam por seu passado comum: obras e obras-primas das belas-artes e das artes aplicadas, trabalhos e produtos de todos os saberes e savoir-faire dos seres humanos (CHOAY, 2006, p. 11).

Seguindo a linha de pensamento de Choay (2006), observa-se que o patrimônio histórico auxilia na compreensão da identidade tendo importante influência na manutenção dos usos e dos costumes populares da sociedade.

O patrimônio cultural é representado pelo conjunto de bens materiais e imateriais. O patrimônio material está relacionado aos objetos concretos, mais precisamente, àqueles que atuam como fontes de informações aos indivíduos. Já o patrimônio imaterial é composto pelo conjunto de manifestações sociais as quais são transmitidas, recriadas e modificadas de forma assistemática ao longo do tempo. Por consequência, ambos representam a memória, a identidade e a História dos

costumes de uma determinada sociedade. Logo, é possível conscientizar os indivíduos, por meio da aquisição de conhecimentos que auxiliem na compreensão de sua história local.

Memória e identidade se concentram em lugares os quais desafiam o passar do tempo e assim são reconhecidos (CANDAU, 2014). Logo, a possibilidade de registrar e arquivar memórias proporciona a imortalidade das pessoas (ABREU, 1996). Desta forma, a preservação de registros documentais que contextualizem as diferentes representações do patrimônio irá corroborar para a sua compreensão e consequentemente, para a preservação de sua lembrança às gerações futuras.

O patrimônio natural, por sua vez, consiste na relação entre o homem e o meio ambiente, mais precisamente no que se refere à fauna e a flora. Observa-se que este ambiente possui uma relação com os indivíduos que nele vivem, havendo assim uma interação que influencia o cotidiano das sociedades.

2.1.1 Desdobramentos patrimoniais

O patrimônio pode configurar diferentes expressões culturais, representado na forma de prédios, documentos, monumentos, entre outros. No caso dos prédios históricos deve-se ressaltar que as ações do conservadorismo representam um grande entrave para os tombamentos. Tal dificuldade pode ser explicada pelo fato de que sempre haverá uma oposição frente aos interesses capitalistas do setor imobiliário, desta forma, uma possível solução seria se adaptar a este sistema e mensurar um nível de intervenção permitido, o qual não descaracterize os prédios históricos (VELHO, 2007).

É valido ressaltar que a preservação de edifícios tombados como patrimônio é uma questão muito sensível, pois a definição do nível de intervenção mais flexível poderá descaracterizá-lo, da mesma forma, que um nível mais rigoroso poderá dificultar qualquer reforma em sua estrutura fazendo ruir e se perder com o tempo devido ao excesso de restrições.

Outra questão pertinente a ser destacada é que há um aumento do conjunto de patrimônio, que pode ser motivado pelo aumento da produção de registros, impactando assim, no aumento das coleções e acervos arquivísticos. Tal fato é uma característica da sociedade contemporânea que demanda grandes volumes de

conteúdos, e da mesma forma, surge a consciência e o dever de disponibilizar e difundir estes conteúdos.

O patrimônio não existe apenas para representar ideias e valores abstratos, e assim ser compreendido, ele vai além, constrói e forma as pessoas (GONÇALVES, 2009). Desta forma, o patrimônio molda os indivíduos conforme as características culturais do meio em que vivem, tendo influência em sua cultura, seus costumes, linguagens, crenças e vestimentas.

> [...] a elaboração do patrimônio segue o movimento das memórias e acompanha a construção das identidades: seu campo se expande quando as memórias se tornam mais numerosas; seus contornos se definem ao mesmo tempo em que as identidades colocam, sempre de maneira provisória, seus referenciais e suas fronteiras; pode assim retroceder quando ligada a identidades fugazes ou que os indivíduos buscam dela se afastar. O patrimônio é menos um conteúdo que uma prática de memória obedecendo a um projeto de afirmação de si mesma. Esse projeto está destinado a permanecer sempre inacabado; ele pode mesmo se esgotar na esperança de chegar a uma memória total (CANDAU, 2014, p. 163-164).

Seguindo a linha de pensamento de Candau (2014), o patrimônio nunca estará completo, sempre haverá um novo item ou aspecto a ser incorporado, e consequentemente, tem-se um constante crescimento patrimonial. Observa-se que, na medida em que o patrimônio se expande o desafio de preservar se torna maior, visto que haverá maior amplitude temporal e diversidade de objetos.

2.1.2 Os lugares de memória e a identidade cultural

Os indivíduos que vivem em sociedade ocupam posições diferenciadas, e assim compartilham das mesmas crenças e visões de mundo, sendo válido ressaltar, que por vezes estes indivíduos se encontram em lugares sociais diferentes. Logo, é necessário perceber os diferentes pontos de vistas que os indivíduos têm em relação ao mundo (ABREU, 1996). Assim, as diferentes visões e condições sociais atuam como variáveis no processo de identidade cultural, possibilitando que um mesmo país possa ter diversas expressões culturais.

Neste ponto, observa-se a importância das instituições de memória, como arquivos, bibliotecas e museus. Abreu (1996) destaca o papel do museu, o qual salvaguarda as memórias individuais ou de grupos os quais se vinculam a uma

construção da história nacional. Tem-se aqui uma série de lembranças determinadas pessoas que são relevantes para a sociedade.

2.1.3 O Arquivo no âmbito do patrimônio cultural

Com o surgimento da escrita, a memória se separa dos indivíduos e começa a estar disponível para ser consultada e comparada. Trata-se de uma memória objetiva, impessoal, vindo a constituir uma verdade independente dos sujeitos. Desta forma, o conhecimento é separado da identidade pessoal, seja do indivíduo ou da comunidade. O conhecimento deixa de ser aquilo que é útil no dia a dia, e passa a ser aquilo que está registrado, tornando-se suscetível à avaliação. A escrita captura a memória social por intermédio de uma rede de signos, a qual lhe confere um significado (LÉVY, 2010). Na medida em que as sociedades passadas evoluíram em sua organização houve paralelamente, o desenvolvimento de uma consciência em relação ao valor dos documentos como meio de registro de suas diversas atividades. Tal fato resultou no surgimento dos arquivos com o objetivo de guardar os tesouros culturais da época (PAES, 2004).

> Através da escrita, o poder estatal comanda tanto os signos quanto os homens, fixando-os em uma função, designando-os para um território, ordenando-os sobre uma superfície unificada. Através dos anais, arquivos administrativos, leis, regulamentos e contas, o Estado tenta de todas as maneiras congelar, programar, repensar ou estocar seu futuro e seu passado (LÉVY, 2010, p. 88).

Atualmente, os documentos custodiados pelos Arquivos integram com o patrimônio cultural brasileiro, além de possuírem tutela jurídica, conforme ressaltado pelo artigo nº 216 da Constituição Federal de 1988:

> Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:
> I - as formas de expressão;
> II - os modos de criar, fazer e viver;
> III - as criações científicas, artísticas e tecnológicas;
> IV - as obras, objetos, documentos, edificações e demais espaços destinados às manifestações artístico-culturais;
> V - os conjuntos urbanos e sítios de valor histórico, paisagístico, artístico, arqueológico, paleontológico, ecológico e científico. (BRASIL, 1988)

A Constituição Federal inicia uma preocupação com a preservação dos documentos, embora não explicite se estes registros são arquivísticos, biblioteconômicos ou museológicos, ressalta-se sua importância como um marco na preservação do patrimônio documental.

Após cumprirem o seu valor imediato na administração, e caso seja identificado valor mediato (interesse probatório, informativo, social e/ou histórico), os documentos passam a ser dotados de um valor secundário; e por esta razão são preservados em caráter permanente. Os documentos arquivísticos “saem da Administração” e passam pelo crivo da avaliação para “entrar na História”.

> [...] o documento de valor permanente é um bem cultural móvel, componente do patrimônio cultural nacional. Como tal, ele tem direitos assegurados à sua integridade física e, tal como outras modalidades de bens culturais, recebe o amparo legal quanto ao seu domicílio, guarda e proteção dentro do meio administrativo, jurídico e social que lhe deu origem, função e sentido (BELLOTTO, 2014, p. 92).

Tais “direitos assegurados” estão implícitos na Lei nº 8.159, de 8 de janeiro de 1991. Em suas disposições gerais, mais precisamente no artigo primeiro, define que: “É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação” (BRASIL, 1991). Esta lei é um importante instrumento jurídico para proteção dos Arquivos brasileiros, de modo que seus documentos não possam ser eliminados de forma arbitrária e indiscriminada. Deste modo, adiciona responsabilidade e prestígio ao trabalho dos profissionais do Arquivo; assim, os documentos arquivísticos representam questões de interesse social, além de possuir um resguardo legal.

Observa-se que a justificativa do tratamento dos arquivos para fins culturais, patrimoniais e/ou de investigação, tem base na sua qualidade de testemunhos (ROUSSEAU; COUTURE, 1998). Sendo válido ressaltar o caráter imparcial dos documentos de arquivo, visto que são gerados para satisfazer atos administrativos de uma determinada organização.

Um último aspecto a ser destacado no âmbito dos acervos é a questão da evolução dos documentos arquivísticos. O avanço das tecnologias da informação e comunicação, e a demanda social por estas ferramentas impulsionou a produção da informação em meio digital, desta forma, o correu o advento do documento

arquivístico digital. Pode-se apontar que a presença da informação digital nos arquivos desencadeou um processo de reformulação de conceitos na área, vindo a modificar o campo de atuação do arquivista.

Ressalta-se que os documentos digitais não são uma exclusividade da Arquivologia, pois já há informação digital sendo preservada, por exemplo, nos museus e nas bibliotecas. Mesmo assim, faz-se uma ressalva visto que cada ambiente (arquivo, biblioteca e museu) possui uma sistemática de gestão, preservação e acesso aos materiais custodiados. Mesmo assim, os referenciais teóricos e as soluções para armazenar estes materiais poderão ser compartilhados de modo que cada área adapte ao seu contexto teórico.

> Novas maneiras de pensar e de conviver estão sendo elaboradas no mundo das telecomunicações e da informática. As relações entre os homens, o trabalho, a própria inteligência dependem, na verdade, da metamorfose incessante de dispositivos informacionais de todos os tipos. Escrita, leitura, visão, audição, criação, aprendizagem são capturados por uma informática cada vez mais avançada. Não se pode mais conceber a pesquisa científica sem uma aparelhagem complexa que redistribui as antigas divisões entre experiência e teoria (LÉVY, 2010, p. 7).

Na medida em que as sociedades vão evoluindo, novas tecnologias vão surgindo e deixando seu legado histórico. Desta forma, há diferentes “marcos históricos” com significados muito particulares e pertinentes ao seu contexto.

2.2 DOCUMENTO ARQUIVÍSTICO DIGITAL

O documento digital pode ser definido como aquele acessado e interpretado por meio de um sistema computacional, (BRASIL, 2011; 2012), armazenado em suporte magnético, óptico ou óptico-magnético, sendo formado por uma sequência de *bits* a qual é lida indiretamente pelas plataformas de *hardware* e *software* (INNARELLI, 2012). E para ser considerado um documento arquivístico digital, deverá ainda ser produzido ou recebido por uma atividade orgânica (BRASIL, 2011; 2012).

Atualmente, uma parcela significativa de documentos arquivísticos está sendo produzida exclusivamente em formato digital (BRASIL, 2004a; 2004b; INNARELLI, 2011; INTERPARES, 2007b; THOMAZ, 2005; 2006), de modo que estes registros ganham relevância como fonte de informação (INNARELLI, 2009). Tal fato é

impulsionado pelas vantagens que o meio digital proporciona como, por exemplo, a facilidade de acesso e a economia de espaço físico. Contudo, a ausência de procedimentos adequados de segurança e de preservação, acarretam incertezas quanto a sua confiabilidade, autenticidade e acesso futuro. Tais entraves podem desqualificar o seu valor como prova das atividades (ROCHA; SILVA, 2007).

Em resumo, os documentos arquivísticos em meio digital necessitam de um tratamento diferenciado se comparados aos documentos analógicos. Tal aspecto reforça a necessidade de intervenção humana, por meio das atividades de preservação digital.

2.3 PRESERVAÇÃO DIGITAL

A preservação de documentos arquivísticos consiste em garantir a autenticidade das informações registradas no suporte, a fim de possibilitar o acesso contínuo aos seus conteúdos e funcionalidades no longo prazo (BRASIL, 2004b). Para isto, a informação, contida no documento, deverá ser interpretada no futuro por uma plataforma tecnológica diferente da qual foi utilizada no momento de sua criação (BRASIL, 2004a; FERREIRA, 2006). Observa-se aqui, um pertinente entrave visto que não há como saber antecipadamente, quais serão as tecnologias utilizadas no futuro, tampouco como será o seu funcionamento.

Para que os documentos digitais possam atingir a longevidade, o estudo da preservação digital deverá ser abordado de forma interdisciplinar (INNARELLI, 2011), contemplando políticas de preservação, as quais irão descrever claramente, como, por exemplo, as estratégias de preservação digital a serem aplicadas. (FERREIRA, 2006).

A complexidade e a fragilidade dos documentos digitais levam ao entendimento de que a preservação digital não é e nunca será resolvida pela própria tecnologia (INNARELLI, 2011). A implementação de políticas de preservação será considerada a iniciativa mais eficaz para preservar e garantir o acesso em longo prazo (MÁRDERO ARELLANO, 2004). Esta política deverá identificar os riscos a fim de evitá-los ou minimizá-los, e contemplar a gestão de segurança seguindo padrões amplamente aceitos. Além disso, será preciso estabelecer um plano de ação para garantir efetivamente, as condições de acesso necessárias no longo prazo (CASANOVAS, 2008).

Em síntese, a preservação digital consiste em garantir o acesso contínuo em longo prazo, objetivando a manutenção da autenticidade dos documentos digitais. Estes documentos deverão ser corretamente interpretados por plataformas de *hardware* e *software* diferentes das quais foram originados. Sendo assim, entende-se a preservação digital como uma atividade que transcende o tempo, a plataforma tecnológica e o suporte de armazenamento.

2.3.1 Estratégias de preservação digital

A preservação digital é composta por procedimentos de ordem estrutural e operacional. Os procedimentos estruturais são os investimentos iniciais como, por exemplo, definições de normas, adoção de padrões e a infraestrutura. Já os de ordem operacional são as atividades aplicadas para a preservação física, lógica e intelectual dos documentos digitais (MÁRDERO ARELLANO, 2004; THOMAZ, 2004). Os procedimentos estruturais compreendem as políticas de preservação, incluindo normas e procedimentos de segurança. Já os procedimentos operacionais compreendem intervenções diretas em nível de *hardware*, *software*, suporte e na própria sequência de *bits* do documento.

Uma estratégia de preservação digital pode ser entendida com um conjunto de objetivos e métodos para efetuar a manutenção em longo prazo dos documentos digitais, contemplando seus objetos digitais e suas informações relacionadas. Assim será possível reproduzir documentos arquivísticos digitais com caráter de autenticidade (WEBB, 2003). Porém, nenhuma estratégia se mostrou eficaz a ponto de ser aplicada genericamente (BRASIL, 2004b; FERREIRA, 2006), o que torna necessário o desenvolvimento de diversas investigações.

Em síntese, as estratégias de preservação digital, de ordem operacional, deverão efetuar a “manutenção” dos documentos digitais, contemplando os seus diversos componentes digitais. A implementação de tais estratégias visa minimizar os problemas causados pela obsolescência tecnológica, como por exemplo, dificuldades de leitura, incompatibilidade de versões, e até mesmo, a perda de informações relacionadas aos documentos.

2.3.2 Autenticidade (integridade[3] e identidade[4])

A preocupação com a preservação da autenticidade dos documentos digitais deve-se a necessidade de garantir que o patrimônio documental custodiado é autêntico e permanecerá íntegro no decorrer do tempo (CORRÊA, 2010). Esta preocupação é manifestada pelo Conselho Nacional de Arquivos (2012, p. 1), órgão vinculado ao Arquivo Nacional do Brasil, conforme o seu documento "Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais", segundo o qual:

> Os documentos arquivísticos digitais apresentam dificuldades adicionais para presunção de autenticidade em razão de serem facilmente duplicados, distribuídos, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes (BRASIL, 2012, p.1).

A questão da autenticidade está diretamente relacionada ao processo de criação, manutenção e custódia dos documentos arquivísticos (RONDINELLI, 2005), e é ameaçada pelos efeitos da obsolescência tecnológica. Além disto, há riscos relacionados à sua transmissão através do tempo em que são custodiados e do espaço onde o aparato tecnológico utilizado para sua preservação e acesso for acondicionado (BRASIL, 2012).

Os documentos arquivísticos digitais necessitam de um tratamento diferenciado, pois possuem características próprias em relação a sua comprovação de autenticidade (SOUSA, 2007), além disto, são vulneráveis à fragilidade implícita de seus objetos digitais, são de fácil adulteração e estão sujeitos aos ciclos de obsolescência tecnológica cada vez mais acelerados (BRASIL, 2014; 2015). Este conjunto de complexidades implícitas ao registro binário, aliado às especificidades tecnológicas para acessar os documentos, demonstram que a preservação e

---

[3] Qualidade daqueles documentos que se encontram completos e que não sofreram quaisquer tipos de corrupção ou alteração não autorizada e nem documentada (BRASIL, 2011). O conteúdo e os dados são considerados inalterados quando forem idênticos ao valor e à apresentação do conteúdo e dos dados da primeira manifestação salva do material (INTERPARES, 2007b). Transmitindo exatamente a mesma mensagem que levou à sua produção para atingir seus objetivos (BRASIL, 2012). A integridade da informação está associada e dependente dos recursos de segurança relacionadas à tecnologia da informação utilizadas no processamento, armazenamento e transmissão (DE SORDI, 2008).

[4] Conjunto dos atributos de um documento arquivístico que o caracterizam como único, capaz de identificar e distinguir um determinado documento arquivístico dos outros. Dentre estes atributos podem ser considerados, por exemplo: data, autor, destinatário, assunto, número identificador, número de protocolo (BRASIL, 2012; INTERPARES, 2007b).

garantia de acesso a documentos arquivísticos digitais autênticos é o desafio à Arquivologia do século XXI.

Os documentos arquivísticos digitais devem ter a sua autenticidade preservada ao longo do tempo, desde a sua produção até o momento de sua transferência ou recolhimento aos arquivos permanentes (INNARELLI, 2009). No meio digital, os problemas relacionados com a autenticidade são semelhantes aos do meio analógico. Porém, a simplicidade com que se podem realizar alterações, a rapidez com que estas podem ser disseminadas e a dificuldade em detectá-las tornam o problema mais complexo (FERREIRA, 2006).

Para preservar documentos digitais autênticos, será necessário manter o registro do conjunto de processos que garantem o seu acesso contínuo, confiabilidade e integridade (MÁRDERO ARELLANO, 2008). Ou seja, os procedimentos aos quais os documentos foram submetidos durante a sua custódia deverão ser registrados na forma de metadados. Além disso, o público e os especialistas devem ter acesso aos procedimentos utilizados pelo preservador, para evidenciar a maturidade do serviço de preservação de digital, e consequentemente, gerar confiança.

2.3.3 Confiabilidade

Dentre os desafios apresentados pelos documentos digitais é possível citar a produção de documentos confiáveis, a manutenção de sua autenticidade e o acesso contínuo em longo prazo (ROCHA; SILVA, 2007). A ausência de confiabilidade acaba por ofuscar os investimentos e os esforços realizados para manutenção da autenticidade. Logo, é preciso que as instituições que custodiam materiais digitais definam boas práticas de preservação digital.

Para agregar confiabilidade, será preciso manter uma cadeia de custódia ininterrupta, na qual os documentos devem estar inseridos desde a sua produção até a sua transferência e/ou recolhimento para o responsável por sua preservação em longo prazo (BRASIL, 2012). Caso esta cadeia de custódia seja interrompida, isto será o suficiente para gerar dúvidas em relação à autenticidade do documento, (BRASIL, 2012; INTERPARES, 2007a) em virtude de sua vulnerabilidade no que tange a manipulação/falsificação de informações.

A autenticidade dos documentos armazenados está relacionada à confiabilidade do sistema de gestão documental. Para isto, os documentos devem ser produzidos, tramitados, avaliados e preservados por meio de métodos confiáveis. Logo, o foco da manutenção da autenticidade não deve estar limitado aos arquivos permanentes, visto que tal questão deve ser considerada desde a produção. Desta forma, os documentos autênticos devem ser produzidos e armazenados por meio de sistemas confiáveis e, posterirormente, serem preservados por sistemas confiáveis. A autenticidade é uma qualidade que deve ser preservada, sendo assim, questões relacionadas à confiabilidade devem ser consideradas desde a produção documental. Conforme o Conselho Nacional de Arquivos (2011) do Arquivo Nacional do Brasil:

> A confiabilidade está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados. Dificilmente pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável (BRASIL, 2011, p.21).

Caso os documentos não sejam produzidos de forma confiável, não haverá como garantir a sua presunção de autenticidade. A confiabilidade depende da manutenção de uma cadeia de custódia ininterrupta, e antes de estar focada na preservação, deve garantir a produção de documentos autênticos.

A confiabilidade não pode ser entendida como um status de “confiável” e “não confiável”, e sim como uma variável que depende do contexto tecnológico onde está situado o acervo. Conforme De Sordi (2008) a informação confiável é aquela a qual os usuários conferem credibilidade, embora seja uma informação que não possua veracidade absolutamente comprovada, a informação confiável é uma informação em que se acredita (DE SORDI, 2008). No caso da informação registrada/documentada, a confiabilidade dependerá da conformidade dos documentos digitais com os princípios da Arquivologia e da Diplomática. A criação de um ambiente confiável para a preservação de documentos digitais implica em estabelecer métodos de preservação que satisfaçam exigências do público pesquisador.

Neste sentido, é preciso implementar *softwares* e políticas de gestão e preservação de documentos digitais, que visem o aumento da confiabilidade do

sistema. Com o tempo, estas iniciativas atingirão os níveis de confiança desejados pelo público alvo.

2.3.4 Repositório arquivístico digital confiável (RDC-Arq)

Os documentos arquivísticos possuem um ciclo de vida o qual é composto por três fases distintas: corrente, intermediária e permanente. A fase corrente compreende documentos consultados frequentemente, os quais são considerados essenciais à Administração, devendo permanecer acessíveis (PAES, 2004; ROUSSEAU; COUTURE, 1998).

A fase intermediária compreende os documentos que deixaram de possuir uso frequente e aguardam o cumprimento de prazos (razões legais, administrativas ou financeiras) para posteriormente após avaliação, serem eliminados ou recolhidos ao arquivo permanente (PAES, 2004; ROUSSEAU; COUTURE, 1998). O arquivo intermediário é, teoricamente, entendido como uma extensão do arquivo corrente (LOPES, 1997).

Desta forma, arquivo corrente e arquivo intermediário constituem o ambiente de gestão documental, o qual está relacionado ao processo de produção e tramitação dos documentos. Para isto, para documentos arquivísticos digitais, será necessário um conjunto de *softwares* para auxiliar no processo de avaliação e recolhimento destes registros ao ambiente de preservação.

A fase permanente compreende documentos remanescentes do processo de avaliação, os quais são preservados por razões além do seu uso administrativo, em especial culturais (SCHELLENBERG, 2006). Tais documentos já perderam o valor administrativo, e são preservados em consideração ao seu valor histórico, e assim, constituem fontes de pesquisa, testemunho e informação (PAES, 2004).

Desta forma, há dois ambientes claramente distintos: o ambiente de gestão, composto por arquivo corrente e arquivo intermediário; e o ambiente de preservação e acesso, composto pelo arquivo permanente. Cada ambiente terá suas peculiaridades e juntos compõem a cadeia de custódia que abrange o ciclo de vida dos documentos arquivísticos.

Ressalta-se que um dos primeiros procedimentos para a preservação de objetos digitais deverá ser a transferência destes para um repositório digital (MÁRDERO ARELLANO, 2008). Para este, será designado o compromisso com a

preservação, o gerenciamento e o acesso contínuo em longo prazo de documentos arquivísticos digitais autênticos (BRASIL, 2014; 2015).

Tradicionalmente, as bibliotecas, os arquivos e os museus são encarregados pela guarda do patrimônio cultural por serem instituições que adquiriram ao longo do tempo, a confiança necessária para armazenar materiais de tal valor. Estas instituições são tidas como confiáveis para preservar tais registros nas melhores condições, bem como fornecer o acesso para as futuras gerações (THOMAZ, 2007). Logo, pode-se dizer que a confiança é adquirida com o passar do tempo, mediante demonstração de competência para tal; no caso dos documentos digitais, será necessário comprovar a eficácia do repositório digital em questão, tornando-se então, um RDC-Arq.

É fundamental que o repositório digital facilite a implementação das políticas de preservação e das estratégias que serão utilizadas (FERREIRA, 2006). Desta forma, um RDC-Arq deverá ser capaz de atender aos procedimentos arquivísticos e aos requisitos de confiabilidade (BRASIL, 2014; 2015). Tal confiança se desenvolve em diversos níveis, havendo um mínimo necessário que são três níveis: produtores, consumidores e fornecedores. Logo, é preciso verificar se os produtores estão enviando as informações corretas, se os consumidores estão recebendo as informações corretas, e se os fornecedores estão prestando serviços adequados (THOMAZ, 2007). Estas são responsabilidades obrigatórias para um repositório digital em conformidade com o OAIS, de modo que possa atingir os seus propósitos de aquisição, preservação e disponibilização de conteúdos à comunidade designada.

A confiabilidade deve ser considerada nas medidas de segurança, desde a construção do RDC-Arq para garantir que os materiais armazenados permanecerão autênticos no logo prazo (MÁRDERO ARELLANO, 2008). Deste modo, será preciso seguir padrões e procedimentos amplamente aceitos pela comunidade[5], demonstrando assim, que os documentos arquivísticos digitais permanecem autênticos.

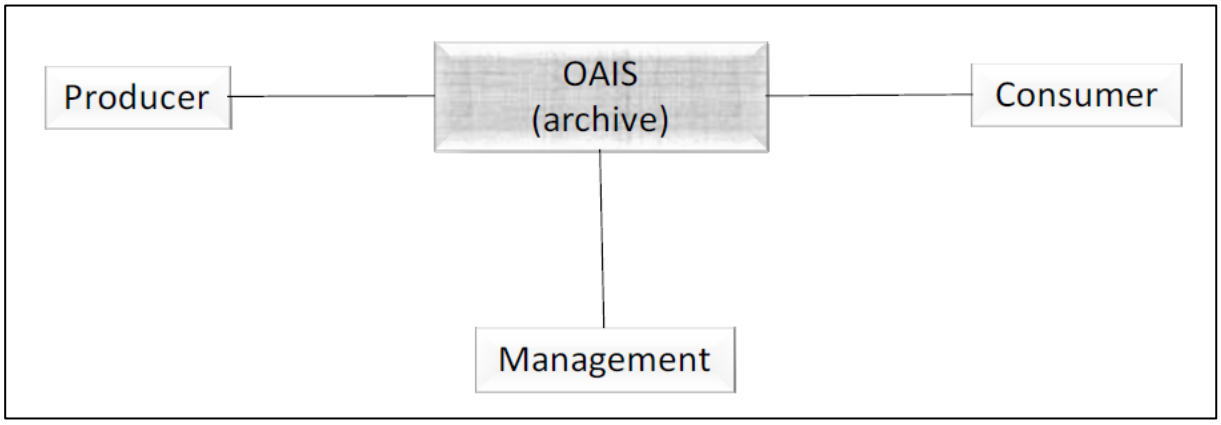
[5] Isto inclui a comunidade de preservação digital e a comunidade de usuários designados.

2.3.5 O modelo de referência *Open Archival Information System*

A implementação de repositórios arquivísticos digitais deverá seguir normas definidas previamente. Neste caso, o Conarq comenta que a norma mais importante da área é o OAIS – ISO 14721:2012 (BRASIL, 2014; 2015). Esta norma oferece uma referência sólida para os termos, conceitos e fluxos de informações que circunscrevem um repositório OAIS, porém não prescreve sua implementação (SAYÃO, 2010).

A “Figura 1 – Os três atores do ambiente OAIS”, apresenta uma visão resumida contendo: produtor, administrados e consumidor, os quais constituem o ambiente de relação direta como o Arquivo (OAIS).

Figura 1 – Os três atores do ambiente OAIS



Fonte: (CCSDS, 2012, p. 2-2).

Conforme a “Figura 1” há três entidades relacionadas ao OAIS. Inicialmente, a entidade produtor (*producer*) representa o responsável pelos documentos de valor primário (arquivo corrente e intermediário), os quais serão submetidos à avaliação, e posteriormente, recolhidos ao OAIS (arquivo permanente) para preservação em longo prazo. Ressalta-se que a entidade produtor (*producer*) é externa ao repositório OAIS, constituindo dois ambientes informatizados distintos e com responsabilidades próprias; podendo acarretar alteração na cadeia de custódia documental.

A entidade administrador (*management*) é responsável por definir as políticas de preservação digital, que englobam questões de normatização, como os padrões de formatos e as estratégias de preservação a serem implementadas. Além de

definir as políticas de aquisição de conteúdo (acordos, licenças), definição da comunidade designada e as tecnologias que serão utilizadas.

Por fim, o material de caráter ostensivo submetido pelo produtor (*producer*), e preservado no ambiente OAIS pelo administrador (*management*), poderá ser acessado pelo consumidor (*consumer*), o qual representa uma entidade externa ao repositório. Ressalta-se que é preciso proporcionar condições de acesso ao consumidor (*consumer*), bem como demonstrar que os materiais custodiados são preservados por métodos confiáveis.

A literatura técnica sobre preservação digital aponta que a conformidade dos repositórios digitais com o modelo OAIS adicionará confiança nas ações de preservação. O fato de o OAIS ser apenas um modelo conceitual, possibilita a sua implementação utilizando uma variabilidade de repositórios, bem como é possível escolher um padrão entre diversos padrões de metadados. Além disso, é possível escolher os *softwares* responsáveis pelas estratégias de preservação, como por exemplo, migrações, conversões e emulações. Desta forma, o acesso em longo prazo dependerá da eficácia destas ferramentas que executam as estratégias, por isto é de extrema importância que exista uma avaliação criteriosa e uma verificação constante destas ferramentas.

Conforme Lopes (2008), para garantir o acesso contínuo à informação no longo prazo torna-se indispensável à criação de repositórios digitais, tendo o auxílio de *softwares* que lhes permitam um melhor controle dos processos relacionados à manutenção dos documentos digitais. No entanto, é necessário ter em mente o modelo de referência OAIS durante a implementação do repositório (LOPES, 2008). Além disso, deve existir em simultâneo, um modelo de informação onde se encontram descritos os requisitos de metadados para a preservação em longo prazo (SARAMAGO, 2004).

Implementar de um arquivo em concordância com os modelos de funcionalidade e estrutura da informação do OAIS é um pré-requisito para se estabelecer os repositórios confiáveis, garantindo a preservação em longo prazo (MÁRDERO ARELLANO, 2008). Deste modo, estima-se que com modelo OAIS, as instituições arquivísticas passarão a entender com maior clareza os conceitos arquivísticos necessários para a preservação (THOMAZ, 2006).

A definição de um repositório digital confiável deverá considerar os termos do OAIS, além de ser submetido a processos de auditoria e certificação. A sincronia

entre estas definições proporcionará um ambiente confiável para a preservação em longo prazo. Logo, tomam-se estes conceitos com base para a recomendação de qualquer repositório digital para preservar documentos autênticos. Para fins desta investigação, cabe explorar a aplicabilidade do OAIS em arquivos, para que forneça subsídios teóricos para a implementação de um RDC-Arq.

2.3.6 Auditoria de repositórios digitais

O processo de auditoria é essencial para avaliar a confiabilidade dos métodos de preservação empenhados pelos repositórios digitais. Em um primeiro momento, verifica-se a conformidade do repositório digital com o modelo OAIS e com requisitos de ordem tecnológica e organizacional pré-estabelecidos.

As atividades de certificação estão diretamente relacionadas com as de auditoria, sendo executadas *a posteriori* como um complemento capaz de mensurar a confiabilidade dos repositórios digitais. Inicialmente uma auditoria é realizada, seguindo um determinado modelo, e assim, fornecendo um determinado conjunto de dados capaz de quantificar as potencialidades e as vulnerabilidades do repositório. Após a interpretação destes dados, o repositório digital poderá ser certificado como "repositório digital confiável".

A certificação dos repositórios digitais precisa ser realizada por uma organização competente para tal e devidamente registrada nos termos legais deste serviço. Desta forma, os requisitos para exercer tal atividade variam de acordo com a legislação de cada país.

Observa-se que o processo de auditoria deve seguir um determinado padrão reconhecido. Dentre estes, serão abordados os seguintes modelos: TRAC[6] (RLG/NARA, 2007), ACTDR[7] (CCSDS, 2011), NESTOR[8] (NESTOR, 2006) e DRAMBORA[9] (DCC/DPE, 2007).

[6] *Trustworthy Repository Audit & Certification: Criteria and Checklist.*
[7] *Audit And Certification of Trustworthy Digital Repositories.*
[8] *Catalogue of Criteria for Trusted Digital Repositories* da *Network of Expertise in long-term STORage.*
[9] *Digital Repository Audit Method Based on Risk Assessment*

2.3.6.1 TRAC

Em 2003, o *Research Libraries Group* (RLG) e o *National Archives and Records Administration* (NARA) criaram uma força-tarefa conjunta a RLG-NARA para certificação de repositórios digitais. O objetivo consistiu em desenvolver critérios para identificar os repositórios digitais confiáveis, e que forneçam acesso aos materiais digitais. Dessa forma, foram produzidos critérios para delinear um processo de certificação aplicável a uma gama de repositórios digitais, dentre eles, arquivos, bibliotecas e serviços de armazenamento digital (RLG/NARA, 2007).

O TRAC possui um conjunto de critérios para a certificação de repositórios digitais, oferecendo ferramentas para auditoria, avaliação e certificação potencial dos repositórios. Desta forma, estabelece a documentação exigida (contratos, licenças, políticas de preservação, planejamento, planos de sucessão) para realizar a auditoria. Além de estabelecer metodologias adequadas para determinar a pertinência e a sustentabilidade dos repositórios digitais (SAYÃO, 2010).

Este modelo tem por objetivo identificar, com base em seus critérios, se os repositórios digitais são capazes de realizar o armazenamento e a migração de forma confiável, além de garantir o acesso aos documentos digitais. O principal desafio consistiu na produção e esquematização de um processo genérico para auditoria e certificação de repositórios digitais (RLG/NARA, 2007).

Conforme o próprio documento, o TRAC engloba as principais características necessárias para que o repositório digital seja considerado confiável. Tais características podem ser comprovadas pelas ações de certificação.

Observa-se que os critérios do TRAC são divididos em três seções, que são: infraestrutura organizacional (*organizational infrastructure*), gerenciamento de objetos digitais (*digital object management*) e tecnologias, infraestrutura técnica e segurança (*technologies, technical infrastructure, & security*).

A seção, **infraestrutura organizacional** (*organizational infrastructure*), compreende aspectos relacionados à governança e viabilidade organizacional (g*overnance & organizational viability*), estrutura organizacional e pessoal (*organizational structure & staffing*), responsabilidade processual e políticas (*procedural accountability & policy framework*), sustentabilidade financeira (*financial sustainability*) e contratos, licenças e passivos (*contracts, licenses, & liabilities*).

Posteriormente, a seção **gerenciamento de objetos digitais** (*digital object management*) compreende aspectos relacionados à aquisição de conteúdo (*ingest: acquisition of content*), criação do pacote para arquivamento (*ingest: creation of the archivable package*), plano da preservação (*preservation planning*), preservação e manutenção dos AIP's (*archival storage & preservation/maintenance of AIPs*), gestão da informação (*information management*), e gestão de acesso (*access management*).

E por fim, a seção **tecnologias, infraestrutura técnica e segurança** (*technologies, technical infrastructure, & security*) compreende aspectos relacionados à infraestrutura do sistema (*system infrastructure*), tecnologias apropriadas (*appropriate technologies*) e segurança (s*ecurity*).

Destaca-se que o TRAC consiste na principal ferramenta utilizada pelo CRL (*The Center for Research Libraries*) para auditoria e certificação de repositórios digitais. Sua versão final foi revisada pelo CRL e pelo RLG (*Research Libraries Group*) após a realização conjunta de testes de auditorias em diversos repositórios digitais durante o período de 2005-2006. A versão final do TRAC foi publicada em 2007 pelo CRL e pelo RLG. Posteriormente, os critérios presentes no TRAC foram base para o desenvolvimento do ACTDR, o qual é outro documento que auxilia no processo para auditoria de repositórios digitais.

2.3.6.2 ACTDR

Este documento tem por objetivo definir um conjunto de práticas recomendadas em conformidade com o modelo de referência OAIS, a fim de fundamentar o processo de auditoria e certificação. Este documento é destinado principalmente aos administradores de repositórios e demais profissionais que prestam o serviço de auditoria, tendo por finalidade mensurar os níveis de confiabilidade de qualquer repositório digital (CCSDS, 2011). O ACTDR possibilita avaliar o repositório digital com relação à sua infraestrutura organizacional, sustentabilidade financeira, gerenciamento dos objetos digitais e gestão de riscos.

Observa-se que o ACTDR tem por objetivo realizar um processo contínuo de auditoria, julgando as áreas que necessitam ser melhoradas. Isto porque o *status* de confiança não é atingido em uma única vez, consiste em um ciclo regular de auditoria e certificação. Como consequência, a divulgação dos resultados da

auditoria ao público irá gerar maior confiança sobre o processo como um todo (CCSDS, 2011).

O padrão ACTDR segue essencialmente a base do TRAC, sendo composto por três seções primárias: infraestrutura organizacional (*organizational infrastructure*), gestão de objetos digitais (*digital object management*), e infraestrutura e segurança da gestão de riscos (*infrastructure and security risk management*). Esta prática recomendada define um processo de auditoria para avaliar a confiabilidade dos repositórios digitais, tornou-se a norma ISO 16363:2012 em 2012.

2.3.6.3 NESTOR

A primeira versão do *NESTOR CRITERIA* foi publicado em dezembro de 2006 pelo *nestor Working Group Trusted Repositories – Certification*. Seu objetivo inicial consiste em ser implementado na Alemanha, entretanto, já é discutido e padronizado internacionalmente, figurando entre os principais modelos que orientam a auditoria de repositórios digitais. Já em novembro de 2009 é a segunda versão do modelo é publicada.

Este documento consiste em um catálogo de critérios atuais que são destinados, principalmente, para as organizações que tem a missão de preservar a memória (arquivos, bibliotecas e museus). Desta forma, atua como um manual, o qual orienta a elaboração, o planejamento e a implementação de um repositório digital confiável no longo prazo. Este catálogo tem por finalidade fornecer orientações para instituições no âmbito da administração de arquivos, prestadores de serviços comerciais e não comerciais, e de serviços de terceiros (NESTOR, 2006; 2009).

2.3.6.4 DRAMBORA

Este documento apresenta um conjunto de ferramentas para auditoria de repositórios digitais, destinado em facilitar a auditoria interna. O DRAMBORA fornece aos administradores do repositório digital, a possibilidade de avaliar as suas qualidades, identificar as vulnerabilidades, e reconhecer suas potencialidades (DCC/DPE, 2007).

O DRAMBORA surgiu a partir do trabalho conjunto entre *Digital Curation Centre* (DCC) e *DigitalPreservationEurope* (DPE), formando assim, o grupo de trabalho DCC/DPE. Inicialmente, o trabalho do grupo DCC/DPE teve como objetivo proporcionar uma abordagem complementar em associação com os esforços dos projetos TRAC e Nestor. Desta forma, em um primeiro momento, procede-se a auditoria interna com o DRAMBORA para identificar e mitigar os riscos; e posteriormente, executa-se a auditoria com o TRAC ou Nestor, para então avaliar a confiabilidade do repositório e certifica-lo como "confiável" caso atinja os níveis desejados.

Com o DRAMBORA é possível obter um catálogo de riscos pertinentes, além de definir a probabilidade e o impacto potencial dos riscos identificados, e assim, propor medidas para prevenção, mitigação e tratamento. A análise de riscos possibilita que as organizações identifiquem e aloquem recursos para minimizar os riscos presentes nas suas atividades consideradas de maior prioridade.

O processo prepara as organizações para atender aos requisitos de avaliação subsequente, ou seja, a auditoria externa. Logo, realizar a auditoria interna com o DRAMBORA equivalente ao trabalho preparatório antes de uma auditoria externa. Além disso, os resultados de obtidos com o DRAMBORA podem fornecer evidências aos auditores externos, demonstrando assim, compromisso com a preservação de longo prazo (DCC/DPE, 2007).

2.3.7 Características dos padrões de auditoria

Os padrões PARA auditoria de repositórios digitais apresentam uma base fundamental para desenvolver tais atividades. Cada um destes estudos abarca uma série de requisitos para adicionar confiabilidade à preservação de longo prazo. Desta forma, entre TRAC, ACTRD, NESTOR e DRAMBORA há considerações quanto a sua aplicabilidade e a própria pertinência do padrão.

O primeiro padrão a surgir foi TRAC, criado em 2003, e sendo revisado pela força tarefa RLG-NARA até 2007, no qual é publicada a sua versão final. Este estudo é continuado no documento ACTDR. Dessa forma, o ACTDR torna-se o sucessor/substituto dos critérios do TRAC em virtude de sua descontinuidade. Os avanços dos estudos em preservação digital farão com que o TRAC, naturalmente,

torne-se ultrapassado com os anos, visto que o conteúdo deste documento é definitivo.

Criado em 2011 pelo CCSDS, o ACTDR surgiu como uma continuidade do padrão TRAC, e logo, em 2012 tornou-se a ISO 16363:2012. No âmbito do CCSDS, o ACTRD está inserido em um processo de constante revisão, o que reforça a pertinência deste modelo, além disso, enquanto norma ISO o documento também estará sujeito às revisões realizadas/solicitadas pelo comitê da ISO.

Outro padrão existente, o NESTOR, originado em 2006 trouxe um proposta inicial para ser implementado na Alemanha, se limitando de certa forma, a um determinado contexto geopolítico. Posteriormente o projeto ganhou relevância sendo aplicado fora deste país, com uma tendência de caráter genérico em seus requisitos, não limitando à realidade alemã. Mesmo assim, o NESTOR ainda carece de reconhecimento enquanto norma ISO, o NESTOR é um estudo promissor e que influenciou e foi influenciado por outros padrões como o TRAC e DRAMBORA.

Em um comparativo com os demais padrões para auditoria, o DRAMBORA diferencia-se por se tratar de um padrão indicado para auditoria interna. Ou seja, trata-se de um instrumento para uso interno da organização, entretanto, isto não minimiza a pertinência de sua estrutura, visto que este documento apresenta uma série de requisitos pertinentes para mitigar riscos. Desta forma, o DRAMBORA pode ser implementado em um repositório digital paralelamente a outro padrão.

Tendo em vista o exposto, este estudo procede à análise do padrão ACTDR, que se tornou a ISO 16363:2012. A escolha toma por base os seguintes argumentos:

- O TRAC está finalizado e o ACTDR é sua continuação;
- O NESTOR ainda carece de reconhecimento pela ISO;
- O DRAMBORA se limita a auditoria interna;
- O ACTDR tornou-se ISO e é revisado constantemente;
- O ACTDR possui caráter de implementação genérico não se limitando a contextos geopolíticos;
- E o ACTDR pode ser usado para auditoria externa.

Por fim, este capítulo apresentou uma revisão dos conceitos básicos que perpassaram o patrimônio cultural, a Arquivística e a preservação digital; além disso,

a revisão de literatura permitiu escolher o padrão de auditoria ACTDR para posterior análise e discussão. A seguir, o capítulo, “metodologia” classifica e descreve as etapas e as técnicas de pesquisa realizadas para atingir os objetivos propostos.

3 METODOLOGIA

Este capítulo descreve os procedimentos metodológicos utilizados para a realização do presente estudo. A seguir serão descritas as especificidades da pesquisa, dentre elas: a classificação, as etapas, a coleta de dados e a planificação dos dados coletados.

3.1 CLASSIFICAÇÃO DA PESQUISA

Conforme Gil (2010), esta pesquisa pode ser classificada em relação a sua área do conhecimento, sua finalidade e seus métodos.

3.1.1 Área do conhecimento

Com relação às áreas do conhecimento definidas então pela CAPES[10] é possível situar quatro níveis hierárquicos de classificação: grande área[11], área[12], subárea[13] e especialidades[14]. Deste modo está pesquisa está essencialmente classificada nos seguintes níveis:

- Grande área: Comunicação e Informação[15] (Código 6.00.00.00-7);
- Área: Ciência da Informação (Código: 6.07.00.00-9);
- Subárea: Arquivologia (Código: 6.07.03.00-8);
- Especialidade: Organização de Arquivos (Código: 6.07.03.01-6).

[10] De acordo com a nova classificação atualizada e publicada pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) em 31 de janeiro de 2017. Disponível em: <http://www.capes.gov.br/images/documentos/documentos_diversos_2017/TabelaAreasConhecimento_072012_atualizada_2017_v2.pdf>.

[11] "Aglomeração de diversas áreas do conhecimento, em virtude da afinidade de seus objetos, métodos cognitivos e recursos instrumentais refletindo contextos sociopolíticos específicos" (CAPES, 2017).

[12] "Conjunto de conhecimentos inter-relacionados, coletivamente construído, reunido segundo a natureza do objeto de investigação com finalidades de ensino, pesquisa e aplicações práticas" (CAPES, 2017).

[13] "Segmentação da área do conhecimento (ou área básica) estabelecida em função do objeto de estudo e de procedimentos metodológicos reconhecidos e amplamente utilizados" (CAPES, 2017).

[14] "Caracterização temática da atividade de pesquisa e ensino. Uma mesma especialidade pode ser enquadrada em diferentes grandes áreas, áreas básicas e subáreas" (CAPES, 2017).

[15] Antiga "Ciências Sociais Aplicadas".

Pelo fato da presente pesquisa relacionar-se com ferramentas informáticas, abordar aspectos de gestão e visar à salvaguarda da memória; ainda poderá manter relações interdisciplinares com outras áreas como: Administração (Código: 6.02.00.00-6), Ciência da Computação (Código: 1.03.00.00-7) e História (Código: 7.05.00.00-2). Observa-se ainda, que diversas outras relações poderiam surgir conforme a ênfase da abordagem da pesquisa.

3.1.2 Finalidade

Com relação a sua finalidade, essa é uma pesquisa de natureza aplicada, pois tem por objetivo gerar conhecimentos para aplicação prática de modo que sejam conduzidos à solução de problemas específicos (SILVA; MENEZES, 2005). Os problemas são identificados no âmbito da sociedade em que o pesquisador vivencia, logo, a pesquisa aplicada é capaz de contribuir para a ampliação do conhecimento científico, bem como gerar novas questões que necessitem de investigação (GIL, 2010).

Sua abordagem é qualitativa, pois conforme Silva e Menezes (2005) a pesquisa qualitativa considera que:

> [...] há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. [...] Não requer o uso de métodos e técnicas estatísticas. O ambiente natural é a fonte direta para coleta de dados e o pesquisador é o instrumento-chave (SILVA; MENEZES, 2005, p.20).

3.1.3 Métodos

Os métodos utilizados nesta pesquisa são classificados como bibliográfico e documental. Inicialmente parte-se, da análise documental do modelo funcional OAIS e de um padrão de auditoria escolhido, e posteriormente, recebe apoio da pesquisa bibliográfica para concatenar conhecimento de natureza Arquivística.

3.1.3.1 Documental

A pesquisa documental, contemplando normas e recomendações. As quais,

segundo o entendimento de Gil (2010), se enquadram na categoria de documento, pois o material consultado é interno à organização que o produziu; já a fonte bibliográfica é obtida em bibliotecas e bases de dados (GIL, 2010). Desta forma, são analisados, fundamentalmente, os seguintes documentos:

- ABNT/NBR 15472:2007. Sistemas espaciais de dados e informações – Modelo de referência para um sistema aberto de arquivamento de informação;
- *Audit and Certification of Trustworthy Digital Repositories*;
- *Digital Repository Audit Method Based on Risk Assessment*;
- *ISO 14721:2012. Space data and information transfer systems – Open archival information system – Reference model*;
- *ISO 16363:2012. Space data and information transfer systems – Audit and Certification of Trustworthy Digital Repositories;*
- *Nestor working group on trusted repositiories certification*. *Catalogue of Criteria for Trusted Digital Repositories* da *Network of Expertise in long-term STORage;*
- *Reference Model for an Open Archival Information System*;
- *Trustworthy Repository Audit & Certification: Criteria and Checklist.*

Além das normas e recomendações, a pesquisa documental recebe apoio de outros materiais como leis brasileiras e diretrizes do Conselho Nacional de Arquivos do Brasil, além da pesquisa bibliográfica.

3.1.3.2 Bibliográfico

A pesquisa bibliográfica parte do levantamento de materiais previamente publicados, realizando uma revisão de caráter assistemático com ênfase nos trabalhos publicados nos últimos quinze anos, período no qual as discussões sobre a preservação digital foram acentuadas. Dentre as fontes bibliográficas, podem-se citar: livros, teses, dissertações e artigos científicos recuperados pela ferramenta de pesquisa *Google Scholar* (GIL, 2010; LUNA, 1997; SILVA; MENEZES, 2005), a qual possui acesso a artigos indexados em diversas bases de dados.

3.2 ETAPAS DA PESQUISA

Para o atingimento dos objetivos definiram-se as seguintes etapas:

- Analisar e apresentar aspectos arquivísticos presentes nas especificações do modelo OAIS;
- Analisar o ACTDR e apresentar os aspectos pertinentes para auditoria de um RDC-Arq;
- Elaborar um manual de procedimentos para auditoria com base no ACTDR, considerando um RDC-Arq em conformidade com o OAIS.

3.3 COLETA DE DADOS

A coleta de dados é realizada através de fichamentos que identificam: autores, editoras, endereços eletrônicos, os títulos das obras e demais informações juntamente aos seus respectivos resumos. Os fichamentos são aplicados tanto na pesquisa bibliográfica, quanto na documental.

Desta forma, o fichamento dos materiais consiste em analisar os materiais na íntegra, e selecionar aspectos que se julgar pertinente para posterior incorporação neste estudo. O uso de fichamentos facilita localizar os dados coletados com precisão, minimizando os riscos de erro ao referenciar os dados citados.

3.4 PLANIFICAÇÃO DOS DADOS COLETADOS

A planificação dos dados da pesquisa tem como instrumento de apresentação um banco de dados elaborado em *Microsoft Access* (Ver Apêndice A – Modelo de fichamento para coleta e tabulação de dados). Este banco de dados, o qual já se encontra concluído, pois teve seu desenvolvimento preconizado em um estudo anterior. Este estudo se refere à Monografia de Graduação[16] do autor que foi apresentada em dezembro de 2014. Com esta ferramenta obtém-se o controle dos materiais fichados, evitando assim, a duplicação, a perda e os riscos de erro ao referenciar os materiais, além de melhorar a precisão da busca e a recuperação da informação.

[16] SANTOS. H. M. **Estratégias de Preservação Digital para Acervos Arquivísticos**. Monografia (Graduação em Arquivologia) 90 p., Universidade Federal de Santa Maria, Santa Maria, 2014.

Parte dos dados coletados contribuiu para a redação de um artigo científico, o qual foi submetido para uma revista da área de ciência da informação. No presente momento um artigo submetido, que abarca o capítulo de "revisão de literatura" já se encontra publicado na revista argentina *Palabra Clave*[17]. Os demais capítulos serão posteriormente submetidos para revistas da área de ciência da informação. O critério para escolha das revistas considera o *qualis* definido pela CAPES (preferência por A1, A2, B1 e B2), o enquadramento dossiê temático (quando houver), e as bases de dados e catálogos nos quais as revistas estão indexadas.

Por fim, este capítulo descreveu as técnicas de pesquisa utilizadas para analisar e discutir o modelo OAIS e o padrão de auditoria ACTDR para elaborar de um manual de autoria de RDC-Arq's. A seguir, o capítulo "análise e discussão dos resultados" explora a conformidade de OAIS com a Arquivística, assim como a pertinência dos critérios de auditoria do ACTDR para a elaboração do manual.

[17] Disponível em: <http://www.palabraclave.fahce.unlp.edu.ar/article/view/PCe029>.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Nesta seção, realiza-se a análise e a discussão necessárias para o atingimento dos objetivos específicos, respeitando os procedimentos metodológicos definidos na seção anterior. Primeiramente, aborda-se o modelo funcional OAIS – ISO 14721:2012. Posteriormente, dentre os padrões de auditoria levantados é analisado o ACTDR – ISO 16363:2012. E por fim, é elaborado o produto deste estudo, um manual que sistematiza um conjunto de requisitos para auditoria de RDC-Arq's.

4.1 OAIS – ISO 14721:2012

Ao se considerar a possibilidade de implementação do modelo funcional OAIS na preservação de documentos arquivísticos digitais autênticos em longo prazo, será necessária uma análise que identifique as consonâncias e as dissonâncias com a Arquivística. Com isto, será possível mensurar as contribuições deste modelo na implementação de um RDC-Arq.

4.1.1 Conceitos

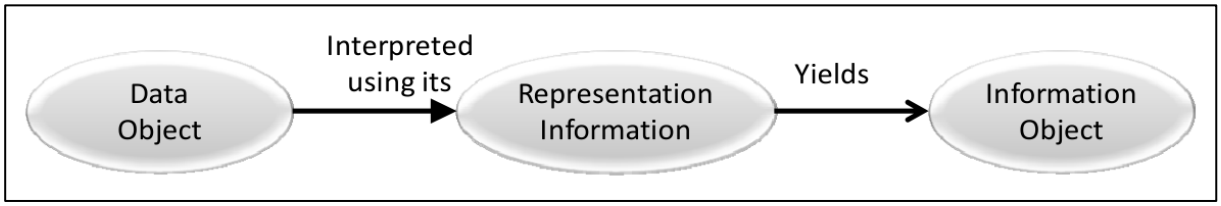
O modelo OAIS consiste em uma descrição de alto nível dos tipos de informação recebidos e armazenados no contexto global de um sistema de depósito digital (SARAMAGO, 2004). Inicialmente o modelo funcional OAIS define uma série de conceitos elementares para a sua compreensão. Desta forma, realiza-se uma análise sobre conceitos como: o objeto de dados; o pacote de informação; as variações do pacote de informação; e as interações externas no OAIS de alto nível. Por meio da análise destes conceitos busca-se elucidar uma visão de alto nível do modelo, para posteriormente, detalhar seu funcionamento em níveis mais densos.

4.1.1.1 Objeto de dados

Inicialmente, o objeto de dados (*data object*) pode ser expresso como um objeto físico ou como um objeto digital, ambos associados com a sua respectiva informação de representação (*representation information*). No caso do objeto digital,

a informação de representação será responsável por adicionar significado a sua sequência de *bits* (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Desta forma, o objeto de dados é interpretado com o auxílio da informação de representação, o que irá resultar no objeto de informação (*information object*). Tal processo pode ser observado na "Figura 2 – Obter informação através dos dados".

Figura 2 – Obter informação através dos dados



Fonte: (CCSDS, 2012, p. 2-4).

Neste processo, observa-se que a preservação do objeto de informação requer uma clara identificação e compreensão, do objeto de dados e de sua respectiva informação de representação. No caso da informação digital, o OAIS deve identificar claramente, os *bits* e qual é a sua informação de representação relacionada. Tal aspecto é uma peculiaridade da informação digital, e representa um desafio significativo para sua preservação (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Há de se ressaltar uma complicação adicional, que é a natureza recursiva da informação de representação, que são os seus próprios dados e sua própria informação de representação, os quais normalmente levam a uma rede de objetos de informação da representação. Desta forma, há dois caminhos a serem escolhidos por um Arquivo OAIS: compreender a base de dados de conhecimento da sua comunidade designada[18] para contemplar a informação de representação[19] mínima necessária; ou manter a maior quantidade de informações de representação que permita a compreensão por uma comunidade maior de consumidores com uma base de conhecimento menos especializado, o que é equivalente a expansão da definição

[18] Corresponde aos usuários potenciais do arquivo, desta forma, devem-se atender as diversas necessidades que estes demandem, a fim de cumprir com as solicitações de acesso.
[19] Os usuários integrantes das comunidades designadas terão diferentes necessidades para acessar e interpretar corretamente os conteúdos, para sito, é preciso inserir informação de representação suficiente para atender tais necessidades.

da comunidade designada (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

No ambiente digital há uma complexidade adicional que vai além da própria complexidade dos objetos digitais, ou seja, o conhecimento sobre os objetos e sobre as ferramentas necessárias para acessá-lo e interpretá-lo corretamente. Este é mais um entrave no processo de preservação digital de longo prazo, visto que o *hardware*, o *software* e o conhecimento específico estão em constante mudança.

A recursividade da informação digital, e a necessidade de se desenvolver redes de objetos de informação de representação criam um ponto de tomada de decisão importante, que é a delimitação da informação de representação. Neste ponto será preciso avaliar a abrangência e a pertinência do material custodiado para escolher entre os dois caminhos possíveis, que são: armazenar a informação de representação mínima necessária; ou manter a maior quantidade de informação de representação.

A escolha entre preservar a quantidade mínima necessária ou o máximo possível da informação de representação, deve considerar também os custos envolvidos para a sua preservação de longo prazo. Estes são aspectos que deverão ser considerados na sustentabilidade do repositório digital, e se opõem de certa forma, à garantia de condições de acesso e de correta interpretação dos objetos digitais. Observa-se que não se podem armazenar todas as informações, no entanto, é preciso discernir o que será necessário para que haja uma comunidade significativa de usuários/consumidores capazes de interpretar os registros preservados.

Além do mais, a base de conhecimentos da comunidade designada[20] poderá sofrer transformações, e assim, será preciso atualizar as informações de representação fornecidas a fim de assegurar a compreensão continuada (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Este processo proposto no modelo OAIS converge com as práticas de gestão do conhecimento, no qual: a informação de representação é atualizada conforme necessário, e atua como uma base de instruções para interpretar o objeto de dados e convertê-lo posteriormente em objeto de informação.

[20] O conhecimento tácito que os usuários de uma determinada comunidade detêm sobre as tecnologias, bem como sua capacidade de acessar e interpretar corretamente os conteúdos desejados.

Outra alternativa será usar um *software* como informação de representação para então acessar o objeto de informação, logo, este *software* será incorporado na rede de objetos de informação de representação. No entanto, este *software* não deve ser usado como justificativa para evitar identificação e a reunião de uma informação de representação facilmente compreensível a qual define o objeto de informação. Tal fato se justifica, pois será mais difícil preservar um *software* do que para preservar a informação em formato digital ou em papel (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Utilizar um *software* como informação de representação não deve ser entendida como um meio para se evitar a inserção de informações textuais relacionadas ao objeto. O simples fato de se inserir um *software* junto ao objeto de dados não garante a sua correta interpretação, visto que será preciso descrever os procedimentos de uso deste *software*; além disto, o *software* se tornará obsoleto e assim, haverá dificuldades para sua utilização no futuro.

O uso de um *software* denota a dependência da longevidade de uma determinada tecnologia, muito específica, o que poderá comprometer o processo de preservação digital no longo prazo. É possível frisar outros entraves quanto ao uso de um *software* como informação de representação, dentre eles:

- O custo de armazenamento;
- O custo relacionado a licenças de uso;
- A obsolescência do conhecimento para manuseio;
- E a obsolescência das plataformas de *hardware* e *software*.

Desta forma, defende-se a posição manifestada pelo modelo OAIS, de que o *software* **pode** ser inserido, mas não deve ser uma alternativa frente à inserção de informações relacionadas em meio digital ou analógico. A proposição do OAIS evita prejuízos ao acesso e a correta interpretação dos documentos arquivísticos digitais, visto que a informação de representação possuiu um subconjunto de outras informações de representação (recursividade) que permitem a sua própria interpretação. Além do mais, interpretar uma informação digital é mais simples do que interpretar um *software*[21].

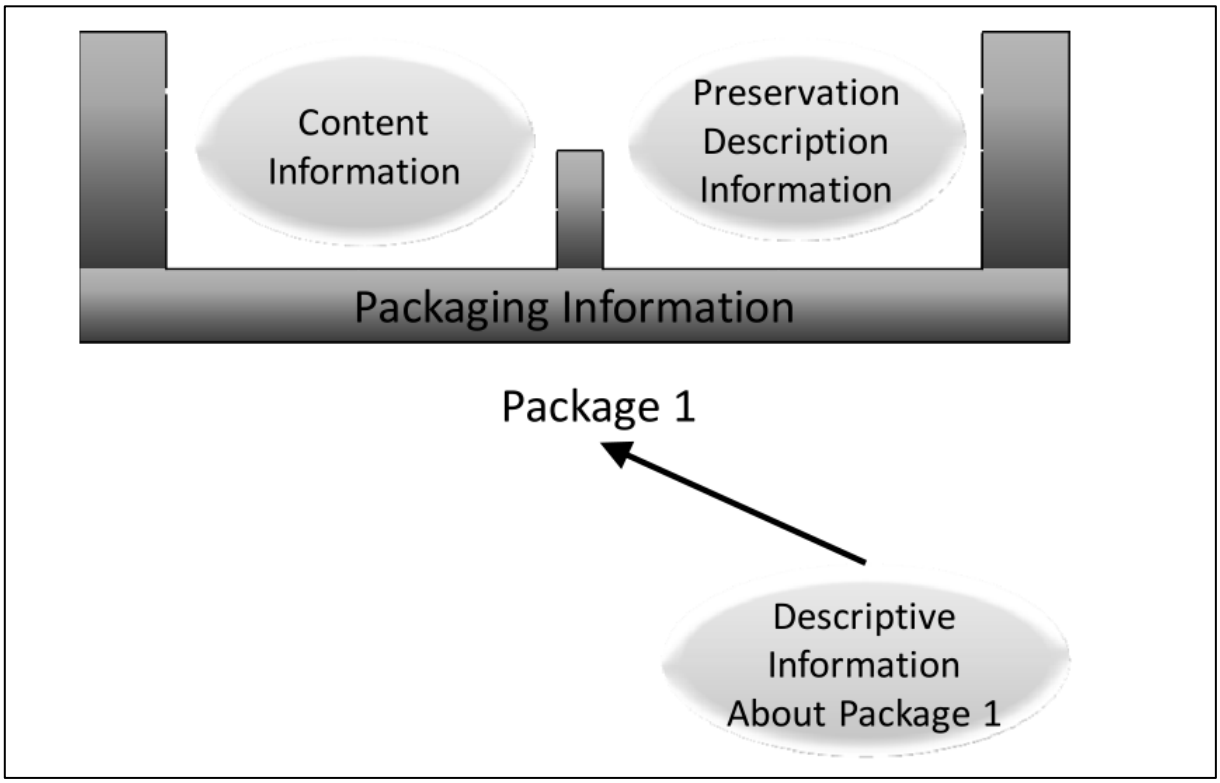
[21] Caso opte-se por utilizar um *software* como informação de representação será realizada a estratégia de encapsulamento. Assim, o *software* será encapsulado e anexado ao objeto de dados, sua sequência de *bits* permanecerá inalterada.

O ideal será inserir as informações de representação necessárias para a correta interpretação dos conteúdos. O *software* não deve ser entendido como um sinônimo de informação de representação, mas pode ser utilizado como alternativa, mesmo assim, deve-se é preciso considerar o seu potencial de obsolescência.

4.1.1.2 Pacote de informação

Um pacote de informação é um recipiente conceitual composto por dois tipos de informações: informações do conteúdo (*content information*) e informação descritiva de preservação (*preservation description information - PDI*). A informação de conteúdo e a PDI são encapsuladas e identificadas pela informação de empacotamento (*packaging information*). O pacote resultante é detectável em virtude da informação de descrição (*descriptive information*) inserida (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Tal esquema pode ser observado a seguir na “Figura 3 – Conceitos e relações do pacote de informação”:

Figura 3 – Conceitos e relações do pacote de informação



Fonte: (CCSDS, 2012, p. 2-6).

Na figura 3, tem-se um pacote genérico, denominado “Package 1”. Neste esquema são identificados os seguintes elementos: informação de conteúdo (*content information*), informação descritiva de preservação (*preservation description information*), informação de empacotamento (*packaging information*) e informação descritiva do “pacote 1” (*descriptive information – About Package 1*).

A **informação de conteúdo** (*content information*) é entendida como a informação que se deseja preservar, ou seja, ela é o conteúdo do objeto de dados (objeto físico e/ou objeto digital), juntamente com sua informação de representação necessária para tornar o conteúdo do objeto de dados compreensível a sua comunidade designada (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Conforme o modelo OAIS, a **informação descritiva de preservação** (*preservation description information - PDI*), a qual descreve a informação de conteúdo, é dividida em cinco tipos de informações de preservação (proveniência, contexto, referência, fixidez e direitos de acesso) apresentadas a seguir:

- A informação de proveniência descreve a fonte da informação de conteúdo, que teve a custódia desde a sua origem, juntamente com o seu histórico (incluindo modificações);
- A informação de contexto descreve como as informações de conteúdo se referem a outras informações fora do pacote de informação;
- A informação de referência fornece um ou mais identificadores, ou sistemas de identificadores, pelo qual a informação de conteúdo pode ser identificada exclusivamente;
- A informação de fixidez fornece proteção às informações de conteúdo para que não haja uma alteração não registrada;
- E a informação de direitos de acesso fornece as condições de acesso, incluindo a preservação, distribuição e uso de informação de conteúdo. Isto inclui concessão de permissões para operações de preservação, licenciamento para distribuição do conteúdo, e demais especificações relacionadas à aplicação de direitos e controle de acesso.

Ainda na figura 3, observa-se que a **informação de empacotamento** é responsável por ligar e relacionar logicamente as informações de conteúdo (*content*

information) e as informações descritivas de preservação (*preservation description information*). E por fim, a **informação descritiva** (*descriptive information*) é usada para descobrir qual pacote tem as informações de conteúdo desejadas. Esta descrição poderá ser, por exemplo, um título descritivo do pacote de informação, ou conjunto inteiro de atributos pesquisáveis em um catálogo.

Desta forma, o pacote de informação visa reunir o objeto de dados e a informação de representação necessária para representar corretamente o objeto de informação, e paralelamente, fornecer subsídios para sua preservação. A arquitetura lógica do pacote de informação fornece evidências para a preservação de documentos arquivísticos em longo prazo. Além disso, contempla aspectos pertinentes quanto ao processo de recuperação da informação e a correta interpretação dos documentos digitais pela comunidade designada.

4.1.1.3 Variações do pacote de informação

Dentro do OAIS irão existir três tipos de pacote de informação, que são: Pacote de Informação de Submissão (*Submission Information Package*), Pacote de Informação de Arquivamento (*Archival Information Package*) e Pacote de Informação de Difusão (*Dissemination Information Package*).

O *Submission Information Package* (SIP) é enviado pelo produtor para o OAIS, ressaltando que sua forma e conteúdo detalhado normalmente são negociados entre o produtor e o administrador OAIS. Na maioria dos casos, este pacote terá alguma informação de conteúdo e alguma PDI. A relação do SIP com o *Archival Information Package* (AIP) pode ser complexa, visto que são possíveis as seguintes transformações:

- Um SIP será transformado em um AIP;
- Um AIP será resultará de vários SIP's produzidos em diferentes épocas por um produtor ou mais produtores;
- Um SIP resultando vários AIP's;
- E muitos SIP's de uma ou mais fontes sendo totalmente desagregados e recombinados em formas diferentes para produzir muitos AIP's.

Mesmo no caso de um SIP ser transformado em um AIP, poderá haver uma série de recombinações na estrutura do SIP, pois as informações de

empacotamento estarão presentes de alguma forma, e isto irá alterar o pacote. Dentro do OAIS um ou mais SIP's podem ser transformados em um ou mais AIP's para a preservação. E os AIP's resultantes possuirão um conjunto completo de PDI para as informações de conteúdo associadas; além disso, os AIP's também poderão conter um conjunto de outros AIP's (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Os pacotes de informação SIP sofrerão alguma transformação independente do nível de complexidade. Tal fato se sustenta, por exemplo, no mais simples dos casos, pela necessidade de inserir a informação de empacotamento. Além disso, tem-se a seguinte premissa lógica: um ou mais SIP's poderão ser transformados em um ou mais AIP's, uma relação de muitos para muitos. Na fase de submissão e arquivamento dos pacotes de informação, observa-se uma mutabilidade de certa forma previsível e perfeitamente aceitável, visto que busca organizar as informações no ambiente OAIS.

As informações sobre os pacotes AIP estarão de acordo com normas internas do OAIS, podendo variar, uma vez que são geridas neste ambiente. Após uma solicitação, o OAIS retorna a totalidade ou uma parte do AIP como resposta ao consumidor. Este material será enviado na forma de um Pacote de Disseminação de Informação, o *Dissemination Information Package* (DIP), propriamente dito. O pacote DIP também poderá incluir coleções de AIP's, as quais podem ou não conter uma PDI completa (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

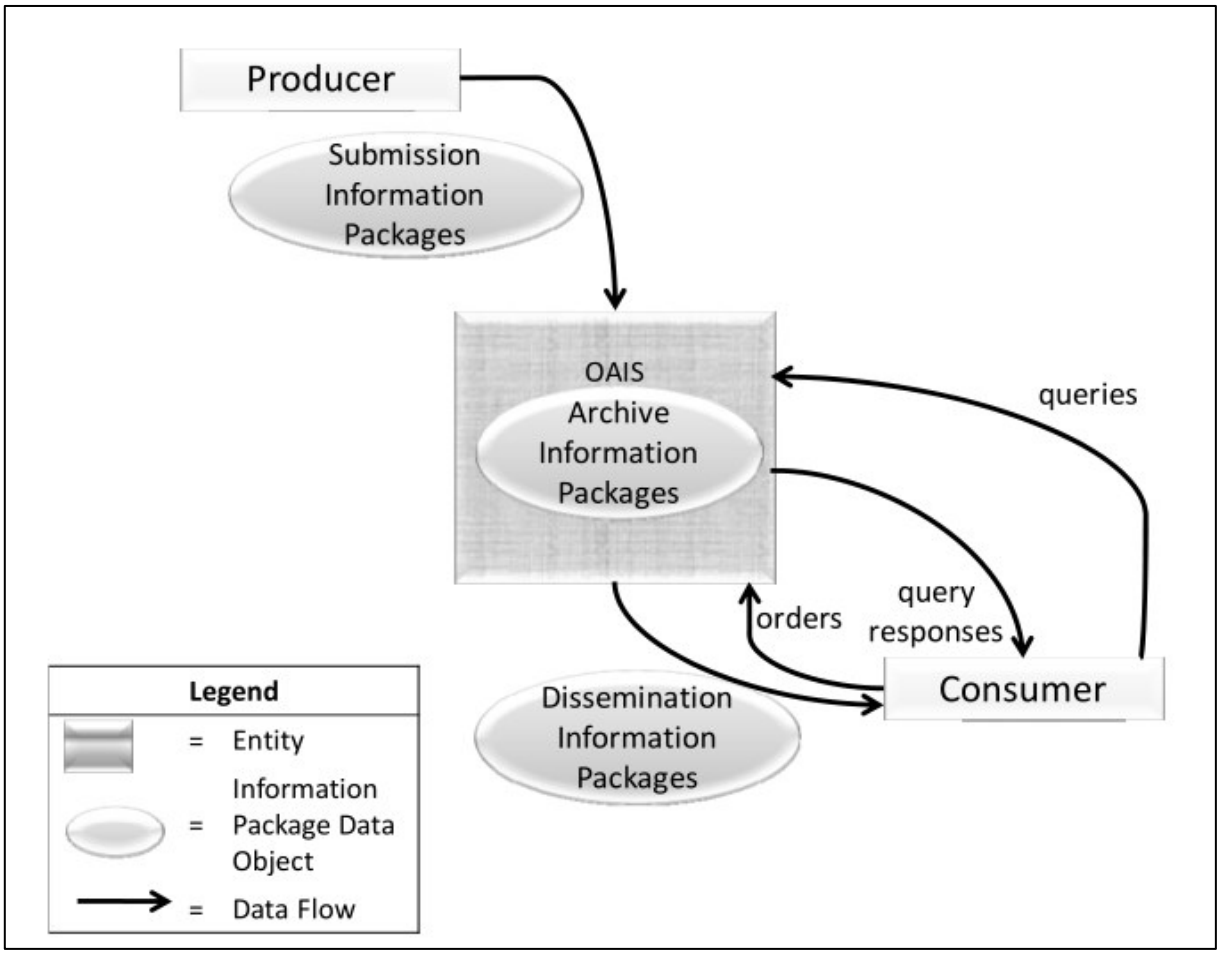
Há de se considerar que o OAIS tem suas próprias normas internas para realizar a organização, o gerenciamento e promover o acesso à informação. Desta forma, após uma solicitação feita pelo consumidor, o OAIS irá retornar um resultado com base em suas normas internas, previamente definidas. Tal questão irá influenciar diretamente no que tange a presença de coleções de AIP's relacionados, bem como a presença da informação de descrição de preservação.

Por fim, o OAIS ressalta que as informações sobre os pacotes devem estar presentes de alguma forma para que o consumidor possa distinguir claramente a informação solicitada. Além disso, a informação de empacotamento poderá assumir diversas formas dependendo dos requisitos tecnológicos das mídias de disseminação e de consumo. Estes são posicionamentos fundamentais para a efetividade do modelo, visto que a informação digital que deverá ser adaptada para o consumidor poder acessá-la e interpretá-la corretamente.

4.1.1.4 Interações externas no OAIS de alto nível

Fora do ambiente OAIS há duas entidades a serem consideradas, que são o produtor (*producer*) e o consumidor (*consumer*). Estas entidades exercem funções elementares no que tange a origem e a finalidade dos processos de preservação digital. A seguir, a "Figura 4 – Fluxos de dados externos do OAIS" apresenta resumidamente, os principais fluxos de informação.

Figura 4 – Fluxos de dados externos do OAIS



Fonte: (CCSDS, 2012, p. 2-8).

Conforme apresentado na figura 4, o produtor (*producer*) envia um fluxo de dados, contendo o pacote SIP ao repositório OAIS. Posteriormente, no ambiente OAIS ocorre a sua transformação em AIP para o arquivamento de longo prazo. E por

fim, o consumidor (*consumer*), o qual representa a comunidade designada, poderá fazer consultas/solicitações (*query responses/orders*) ao OAIS e obter o pacote DIP com os respectivos resultados de suas solicitações.

O primeiro contato entre o OAIS e o produtor consiste no pedido para que o OAIS preserve os materiais digitais criados pelo produtor. Este contato pode ser uma iniciativa tomada pela gestão do OAIS ou pelo produtor. Após isto, o produtor estabelece um acordo de submissão com o OAIS, o qual identifica os SIP's a serem apresentados, observa-se que estes SIP's podem abranger qualquer período de tempo para submissão (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Quanto aos acordos de submissão, há de se destacar três possíveis situações:

- O acordo será um requisito obrigatório para fornecer informações ao OAIS;
- Haverá oferta voluntária do produtor de informações para o OAIS;
- Haverá pagamentos ao produtor em troca de informações ofertadas ao OAIS.

Com relação às diversas interações entre o consumidor e o repositório OAIS, destaca-se que além das consultas (*queries*) o consumidor poderá estabelecer um acordo de solicitações (*orders*) com o OAIS para obter informações, as quais poderão existir atualmente no Arquivo ou esperar admissão no futuro (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Observa-se que este procedimento identifica os interesses dos consumidores constituindo uma comunidade designada de forma automática prevendo os consumidores potenciais da informação.

Por fim, é preciso considerar a função do administrador (*management*) que ao passo em que interage com o ambiente externo (produtor e consumidor), também possui atribuições relacionadas a diversos aspectos do OAIS. Dentre as principais atribuições do administrador podem ser consideradas:

- A busca de financiamentos para o repositório;
- Realizar uma constante revisão para avaliar a desempenho OAIS em seu progresso e os riscos no qual é exposto;
- Determinar políticas de preços para os serviços do OAIS;
- Oferecer soluções para conflitos envolvendo produtores, consumidores e a própria administração interna do OAIS;
- E fornecer suporte para o OAIS a fim de estabelecer procedimentos que asseguram sua utilização em esferas de influência.

O administrador do OAIS terá um papel fundamental no que tange à longevidade, desempenho, normatização, realização de acordos (de submissão e de solicitação) e demais questões relacionadas. O administrador atua no epicentro do repositório: requerendo a ingestão de pacotes de informação com determinada qualidade; definindo ações para preservar estes materiais em longo prazo; provendo o seu acesso; além de fornecer suporte para sua utilização.

4.1.2 Responsabilidades

Dentre as especificações do modelo OAIS observa-se um conjunto de responsabilidades a serem consideradas, que podem ser divididas em: responsabilidades obrigatórias e exemplos de mecanismos que possam realizar estas funções (mecanismos de apoio).

4.1.2.1 Responsabilidades obrigatórias

Conforme o próprio modelo funcional OAIS há uma série de responsabilidades obrigatórias a serem atendidas. Desta forma, um repositório digital deverá ser capaz de:

- Negociar e aceitar informações adequadas junto ao produtor;
- Obter o controle das informações fornecidas a fim de possibilitar a sua preservação em longo prazo;
- Participar do processo de definição da comunidade designada, e definir sua base de conhecimento, de modo que esta seja capaz de entender as informações fornecidas;
- Garantir que a comunidade designada é capaz de compreender as informações preservadas sem a necessidade de recursos especiais ou do auxílio dos produtores;
- Seguir políticas e procedimentos previamente documentados assegurando que a informação é preservada de maneira confiável, estando imune a questões como a exclusão de itens, a menos que permitido como parte de uma estratégia aprovada;

- Tornar a informação preservada disponível para a comunidade designada, permitindo disseminá-la como cópia ou rastreável (apontando para o objeto de dados originalmente submetido junto com os demais elementos que comprovam a sua autenticidade).

As responsabilidades obrigatórias correspondem aos propósitos do repositório digital, ou seja, se relaciona a aquisição da informação digital, bem como busca resguardar os direitos para realizar a sua preservação em longo prazo. Além disso, outras questões podem ser destacadas como a definição de quem será a comunidade designada, e garantir que esta seja capaz de interpretar as informações preservadas sem a necessidade de se recorrer a métodos complexos e específicos.

Em resumo, as responsabilidades irão nortear o que será preservado; definir o direito de preservar; manter procedimentos preservados para a preservação; e ter definido quem irá usufruir deste material. Neste ponto, o modelo OAIS subentende a necessidade de assegurar a posse da informação digital, bem como conhecer previamente, a existência de uma comunidade potencialmente interessada na preservação e garantia de acesso desta informação.

4.1.2.2 Mecanismos de apoio

Os mecanismos de apoio correspondem a possíveis exemplos para realização das responsabilidades obrigatórias. No entanto, salienta-se que nem todos esses mecanismos serão, necessariamente, aplicáveis ao OAIS.

4.1.2.2.1 Negociar e aceitar informações

Um OAIS deverá obter informação descritiva, a qual seja suficiente para auxiliar a comunidade designada a encontrar as informações de conteúdo de seu interesse. Além disso, é preciso garantir que a informação preservada segue todas as normas internas do repositório OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

É preciso vislumbrar o acesso logo na fase da submissão dos documentos digitais, pois desta forma será possível obter informações de interesse junto ao produtor, como por exemplo, a informação descritiva, a qual será muito útil ao

consumidor. De maneira geral, este procedimento enriquece as informações relacionadas aos documentos digitais, podendo auxiliar tanto no processo de preservação quanto na precisão da busca e acesso a informação.

4.1.2.2.2 Obter controle para a preservação

No momento da aquisição da informação por parte do OAIS é preciso garantir um acordo de transferência legalmente válido, especificando claramente, a transferência dos direitos de propriedade intelectual; as concessões de direitos ao OAIS; ou quaisquer outras limitações impostas pelo detentor de direitos. Após a definição desse acordo, o OAIS deve garantir a conformidade destes com suas ações posteriores de preservação e disponibilização (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O controle é um ponto crucial para as atividades desenvolvidas *a posteriori*, pois é preciso definir os direitos que o repositório terá sobre a documentação adquirida. Tais direitos irão implicar diretamente no tratamento que os documentos digitais poderão receber.

Nos casos em que o repositório OAIS não obter controle para gerenciar os direitos da propriedade intelectual será necessário que o acordo especifique o nível de envolvimento que o titular de direito terá nos processo de gestão, preservação e/ou disseminação das informações. Em geral, será preferível que o repositório negocie um acordo que especifique os requisitos da custódia, de modo que o OAIS mantenha a conformidade com esses requisitos, mas sem a participação ativa do titular do direito nos procedimentos de tratamento da informação (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Quando o gerenciamento da propriedade intelectual não for negociado pelo OAIS frente ao produtor, será fundamental um acordo que autorize o repositório a realizar os procedimentos de preservação. Isto implica em questões como a alteração do conteúdo binário, como, por exemplo, no caso de uma migração ou mesmo na inserção de metadados. Além disto, ressalta-se que a questão da disseminação também será regida pelo acordo de direitos. Em resumo, o acordo de direitos é o meio pelo qual se define os possíveis usos da documentação custodiada.

Quanto à preservação de longo prazo, observa-se que um repositório OAIS deverá assumir controle suficiente sobre as informações de conteúdo e sobre as informações de preservação; visto que as informações de empacotamento são criadas internamente no OAIS e mantém-se sob seu controle (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Desta forma, conforme o OAIS, os possíveis problemas em assumir o controle da informação de conteúdo e da informação de preservação, podem ser divididos em três categorias relacionadas: implicações de direitos autorais, propriedade intelectual e outras restrições legais ao uso; autoridade para modificar as informações de representação; e acordos com organizações externas.

a) **Implicações de direitos autorais, propriedade intelectual e outras restrições legais ao uso**: um Arquivo deve respeitar todas as restrições legais aplicáveis. Estes entraves ocorrem quando o OAIS age como custodiador, de modo que o OAIS compreenda os conceitos de direitos de propriedade intelectual, tais como direitos autorais e quaisquer outras leis aplicáveis antes de aceitar a submissão de materiais com direitos autorais. Sendo assim, um repositório OAIS pode definir orientações para a submissão de informações e regras de difusão e de redistribuição das informações quando necessário;
b) **Autoridade para modificar as informações de conteúdo**: mesmo que a informação de fixidez dentro da PDI de um AIP garanta que os *bits* relacionados à informação de conteúdo não tenham sido alterados poderá haver um momento no qual a própria comunidade designada de consumidores demande novos formatos para a representação das informações de conteúdo. Os *bits* da informação de conteúdo podem ser integralmente documentados em formatos impressos, logo, teoricamente, a informação não foi perdida, no entanto tornou-se inacessível. Além disso, o OAIS precisa de permissão[22] para migrar as informações de conteúdo para novos formatos de representação. E ao exercer o papel de custodiador será

[22] A informação poderá ser alterada com a finalidade de facilitar o processo de preservação. Isto implica em, por exemplo, converter formatos ou migrar para novas versões. Para sito, devem ser definidas as principais características dos objetos digitais, essas serão as suas propriedades significativas, e determinarão o mínimo necessário para sua compreensão e presunção de autenticidade. Deste modo, as propriedades significativas devem ser mantidas durante todo o processo de preservação, pois são essenciais ao objeto digital.

necessária uma autorização adicional para fazer tais alterações. Nos casos das informações que possuam *copyright* o OAIS deverá negociar a permissão para fazer as alterações necessárias a fim de cumprir seus objetivos de preservação em longo prazo, de modo que não altere as propriedades significativas dos objetos digitais. Para isto, o OAIS poderá incorporar especialistas externos a fim de garantir que a informação custodiada não será perdida. O ideal para esta situação será manter os AIP's originais (totalmente descritos) e os novos AIP's;

c) **Acordos com organizações externas**: Um repositório OAIS pode estabelecer vários contratos com organizações externas para auxiliar nas atividades de preservação em longo prazo. Logo, os acordos com organizações externas devem ser monitorados a fim de garantir o seu cumprimento e avaliar a sua importância no processo de preservação (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Em linhas gerais, um repositório OAIS precisa obter as permissões necessárias para efetivar as atividades de preservação em longo prazo. Neste sentido, é preciso atentar para questões como os direitos de propriedade, restrições de uso, alteração da informação de conteúdo e a busca de acordos que visem a melhoria dos procedimentos de preservação digital. Obter o controle necessário para as informações a serem preservadas é entendido como uma importante iniciativa para garantir a manutenção dos documentos digitais.

Tendo em vista o horizonte da Arquivística, observa-se que a questão da aquisição de direitos ou licenças de uso converge com uma das funções apontadas por Rousseau e Couture (1998), a aquisição. Há uma série de questões a serem consideradas pelo antigo custodiador e pelo preservador (novo custodiador), e tais questões se tornam ainda mais complexas ao se tratar de documentos arquivísticos em meio digital.

4.1.2.2.3 Determinar a comunidade designada

No momento da submissão da informação de conteúdo, juntamente com a PDI relacionada, será preciso determinar quais são os consumidores esperados ou comunidades designadas. Tal procedimento é necessário para determinar se a

informação será compreensível (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O modelo OAIS trata a comunidade designada como um conjunto identificado de usuários potenciais capazes de entender um conjunto específico de informações. Assim, a comunidade designada pode ser composta por várias comunidades de usuários. O arquivo definirá a comunidade designada, e esta definição, poderá mudar com o tempo (CCSDS, 2012; ISO 14721:2012). No entanto, no âmbito da Arquivística, esta distinção de público não ocorre de forma rígida. O acesso à informação preservada é oferecido para quaisquer usuários que tenham interesse na informação de conteúdo. A visão arquivística da comunidade designada corresponde ao arquivo e seus usuários potenciais, ou seja, não há restrição de público. Logo, o objetivo é atender o maior número possível de usuários interessados, de modo que estes sejam capazes de interpretar corretamente as informações preservadas.

Esta sistemática pode evitar problemas futuros quanto a correta interpretação das informações de conteúdo, logo, deverá considerar a base de conhecimento da comunidade designada e manter uma rotina de atualização do AIP; principalmente, de suas informações de representação. Em termos genéricos de custódia, a definição da comunidade designada, bem como a identificação de possíveis usuários da informação pode ser considerada pelo OAIS, como um dos sentidos da preservação dos documentos digitais. Caso não haja interesse do público externo não haveria razão para se preservar um determinado conteúdo.

Entretanto, no contexto da Arquivística só há uma fase para a seleção dos materiais a serem preservados, a qual corresponde a função de “avaliação” enfatizada por Rousseau e Couture (1998). Observa-se neste ponto, que a avaliação considera critérios previamente definidos, logo, a comunidade designada consisteem um critério visto que os documentos serão preservados para os usuários acessarem. Desta forma, a avaliação considera valores probatórios, sociais, culturais e de informação, vislumbrado a utilização destes documentos no longo prazo.

A função de avaliação está localizada em uma fase que antecede a submissão de SIP’s ao repositório digital OAIS, o qual atua como um Arquivo Permanente. Desta forma, os documentos digitais são submetidos ao OAIS em virtude de seu caráter permanente, ou seja, durante o processo de avaliação foi verificada a necessidade de preservar determinados documentos, em virtude da presença de valor social, histórico e/ou informativo. Logo não há, por parte do

Arquivo, seleção posterior dos materiais que continuarão sendo preservados; todos deverão ser preservados.

Este apontamento não se configura como uma divergência entre o modelo OAIS e a Arquivística, e sim como uma adaptação que surge em virtude do caráter genérico do OAIS. A questão do interesse por determinados documentos arquivísticos pode variar conforme a época, e estas questões devem ser consideradas pelo arquivista na fase de avaliação dos documentos a fim de prever possível interesse sobre os documentos. Em resumo, a determinação da comunidade designada pelo OAIS deve ser considerada na fase da avaliação, desta forma, os documentos arquivísticos digitais remanescentes serão submetidos ao repositório OAIS e preservados em longo prazo.

4.1.2.2.4 Garantir a correta interpretação das informações

Uma comunidade designada, geralmente interpreta a informação de conteúdo e a PDI relacionada de forma subjetiva. No entanto, é preciso que o Arquivo defina esse grau de transmissão para maximizar a preservação de informação. A informação de conteúdo e a PDI precisam de informações de representação adequadas para então se tornarem compreensíveis de uma forma independente para a comunidade designada. Como consequência haverá vários objetos de informações de representação envolvidos (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O modelo OAIS prevê que a informação de conteúdo poderá assumir diferentes significados para a comunidade designada, isto é, uma interpretação subjetiva que seguirá a base de conhecimento de cada indivíduo. Logicamente, este é um entrave que não poderá ser eliminado, mesmo assim, o OAIS poderá buscar alternativas para minimizar estas divergências. A inserção dos objetos de informação de representação atua como um meio para amenizar as diferenças entre as bases de conhecimento dos membros das comunidades designadas e demais indivíduos, para que a informação de conteúdo expresse o mesmo sentido.

As bases de conhecimento evoluem ao longo do tempo de modo que aspectos importantes da informação podem não ser mais facilmente compreensíveis. Tal problema poderá ocorrer até mesmo nos casos em que um conjunto de informações for determinado para ser compreensível para uma

determinada comunidade designada. Logo, o OAIS pode melhorar a qualidade da informação de representação associada a fim de facilitar, para a comunidade designada, a compreensão das informações de conteúdo (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Conforme destacado por Lévy (2010), para que as informações tenham sentido, é essencial fazer associações, ligar a informação em uma rede para construir sentido.

> A operação elementar da atividade interpretativa é a associação; dar sentido a um texto é o mesmo que ligá-lo, conectá-lo a outros textos, e portanto é o mesmo que construir um hipertexto. É sabido que pessoas diferentes irão atribuir sentidos por vezes opostos a uma mensagem idêntica. Isto porque, se por um lado o texto é o mesmo para cada um, por outro o hipertexto pode diferir completamente. O que conta é a rede de relações pela qual a mensagem será capturada, a rede semiótica que o interpretante usará para captá-la. [...] Para que as coletividades compartilhem um mesmo sentido, portanto, não basta que cada um de seus membros receba a mesma mensagem (LÉVY, 2010, p. 72).

Desta forma, será interessante que um repositório OAIS aplique ações para monitorar as comunidades designadas, de modo a verificar se as informações preservadas são de fácil compreensão. Este é um processo complexo, pois as bases de conhecimento das comunidades designadas mudam o tempo todo, o que força a uma verificação sistemática.

Nos casos em que houver escassez de informação de representação, pode-se utilizar um *software* para acessar a informações do conteúdo. Entretanto, a manutenção de um *software* específico no longo prazo ainda não tem sido eficaz com relação aos custos relacionados, até mesmo pela sua aplicação que é restrita. A dependência do *software* para acessar a informação de conteúdo configura um grande risco de perda das informações; como também, para a compreensão do conteúdo no caso de mudanças nas plataformas de *hardware* e *software*, gerando possíveis incompatibilidades[23] (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Em geral, o caráter recursivo da informação em meio digital e a necessidade de garantir a correta interpretação da informação de conteúdo, adicionam mais um

[23] Este é um problema que não pode ser detectado a menos que haja um controle para validação. Uma alternativa é empregar um emulador para manter um ambiente estável para uso de *softwares* de aplicação específica. Uma das principais preocupações com esta abordagem é a necessidade de atualizar e efetuar manutenção do emulador no longo prazo. É preciso garantir que os documentos emulados não sofreram manipulação, além de manter um custo viável para os processos (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

nível de complexidade ao processo de preservação em longo prazo. Tal complexidade se relaciona diretamente ao processo de recuperação da informação tendo impacto direto nas responsabilidades a serem consideradas por um OAIS.

4.1.2.2.5 Estabelecer políticas e procedimentos de preservação

É essencial que o OAIS documente e siga as políticas e os procedimentos utilizados para preservar os pacotes AIP. Dentre estas definições, observa-se que os AIP's nunca devem ser excluídos de um OAIS salvo a exceção caso seja parte de uma política aprovada. Além disso, as migrações que alteram qualquer informação de conteúdo ou PDI devem ser monitoradas e a PDI atualizada consequentemente (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Considerando que o contexto no qual o repositório digital está inserido é a fase permanente, logo, o OAIS não deve permitir a exclusão de documentos. A necessidade de proceder a exclusão de documentos do OAIS passa a ser entendida com uma exceção, ou seja, um procedimento que é adotado caso um determinado pacote AIP não deva ser armazenado pelo repositório. No entanto, este procedimento de exclusão de AIP's não pode ser realizado de maneira rotineira, e sim para casos especiais amparados por uma política de segurança. Um exemplo prático seria um erro na submissão, de modo que ocorresse o envio equivocado de um pacote AIP contendo documentos que não possuem caráter arquivístico ou documentos arquivísticos que não possuem valor secundário (guarda permanente). Desta forma, o procedimento correto seria a exclusão do AIP equivocado seguido pela submissão do AIP correto.

Dentro do escopo das políticas de preservação digital, é preciso estabelecer um plano de uso da tecnologia no longo prazo, o qual é atualizado conforme a evolução das plataformas. Este procedimento é essencial para evitar custos elevados de manutenção do sistema, bem como as substituições de sistemas em caráter de emergência as quais ocasionam alterações na representação dos dados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

As políticas de preservação digital do OAIS devem considerar o contexto tecnológico no qual o repositório digital está inserido. Desta forma, o monitoramento constante das tendências de *hardware* e *software* surge como uma alternativa para prevenir e minimizar os riscos de perda de informações. Atuando com uma política

preventiva, o OAIS poderá evitar prejuízos tanto de ordem financeira, quanto à informação digital.

Outra questão a ser considerada pelo Arquivo nas políticas de preservação é a formalização[24] de um plano de sucessão para os seguintes casos: se o Arquivo cessar as suas atividades; se ocorrer mudança da administração; ou se ocorrer interrupção do financiamento (CCSDS, 2012; ISO 14721:2012). Estas são questões essenciais que afetam profundamente as atividades de preservação no longo prazo e que devem ser pensadas *a priori* antes mesmo da implementação de um repositório digital que segue o modelo OAIS.

4.1.2.2.6 Disponibilizar a informação

Um repositório OAIS tem por função tornar a informação de conteúdo de seus AIP's disponíveis â comunidade designada. Neste sentido, haverá certa pressão por um acesso mais eficaz o qual deve ser equilibrado com os requisitos de preservação observando as limitações impostas pelos de recursos disponíveis (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A questão do equilíbrio entre preservação e acesso pode ser delineada na relação entre os pacotes AIP e DIP. O pacote AIP se restringe à preservação, reunindo todo o material necessário para a correta interpretação dos documentos digitais, já o DIP se concentra nas questões de acesso, facilitando a precisão da busca de uma determinada informação.

Entretanto, há um contraponto a ser considerado: o AIP precisa reunir as informações necessárias para a correta representação, e dentre esta reunião de componentes digitais pode haver níveis de complexidade consideráveis, como, por exemplo, um determinado *software* que realiza a interpretação da informação de conteúdo, e que não pode ser suprimido ou substituído no DIP. Por isso, é preciso que a preservação vislumbre o acesso desde suas fases iniciais.

Ressalta-se que determinados AIP's podem ter acesso restrito, de modo que somente as suas restrições de acesso podem ser divulgadas aos consumidores em caráter de informação. Quando for o caso, as políticas de acesso e as restrições do OAIS devem ser previamente publicadas para garantir a proteção dos direitos de

[24] Documentação oficial, aprovada pelas políticas internas, que explicite os procedimentos de sucessão do repositório.

todos os envolvidos. Por padrão, o pacote DIP pode ser distribuído pelos mais diversos meios de comunicação, seja por meio da *internet* ou por mídias físicas (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Em se tratando de documentos arquivísticos, há uma ressalva quanto ao acesso em virtude de seu possível caráter sigiloso. No contexto brasileiro, ocorreram transformações tendo em vista a Lei de Acesso à Informação (LAI)[25]. Assim, a "cultura do sigilo" foi alterada, obtendo-se assim, a "cultura do acesso", logo, todos os documentos são previamente acessíveis (ostensivos), e o sigilo das exceções deve ser explicitamente justificado. Desta forma, observa-se que, o modelo OAIS, através da entidade funcional de acesso (*access*), pode contribuir com a LAI; a qual corrobora com o novo paradigma da finalidade da Arquivística, que é preconizar o acesso aos documentos do arquivo.

Com a LAI, os indivíduos possuem direito de acesso aos documentos e informações a ele relacionados. A lei traz o direito de acesso como regra geral, já o sigilo passa a ser entendido como uma exceção. Quanto ao sigilo, este deverá ser definido previamente e justificado de acordo com a definição do nível de sigilo (reservado, secreto ou ultrassecreto) (BRASIL, 2011).

Desta forma, caso um AIP possua informações de caráter sigiloso, haverá restrições de acesso na informação de conteúdo do pacote DIP, o qual irá fornecer acesso somente ao conteúdo ostensivo. Tais considerações devem ser negociadas entre o administrador e o consumidor, assim o OAIS poderá cumprir legalmente a restrição e o direito de acesso à informação.

4.1.3 Visão detalhada do modelo funcional OAIS

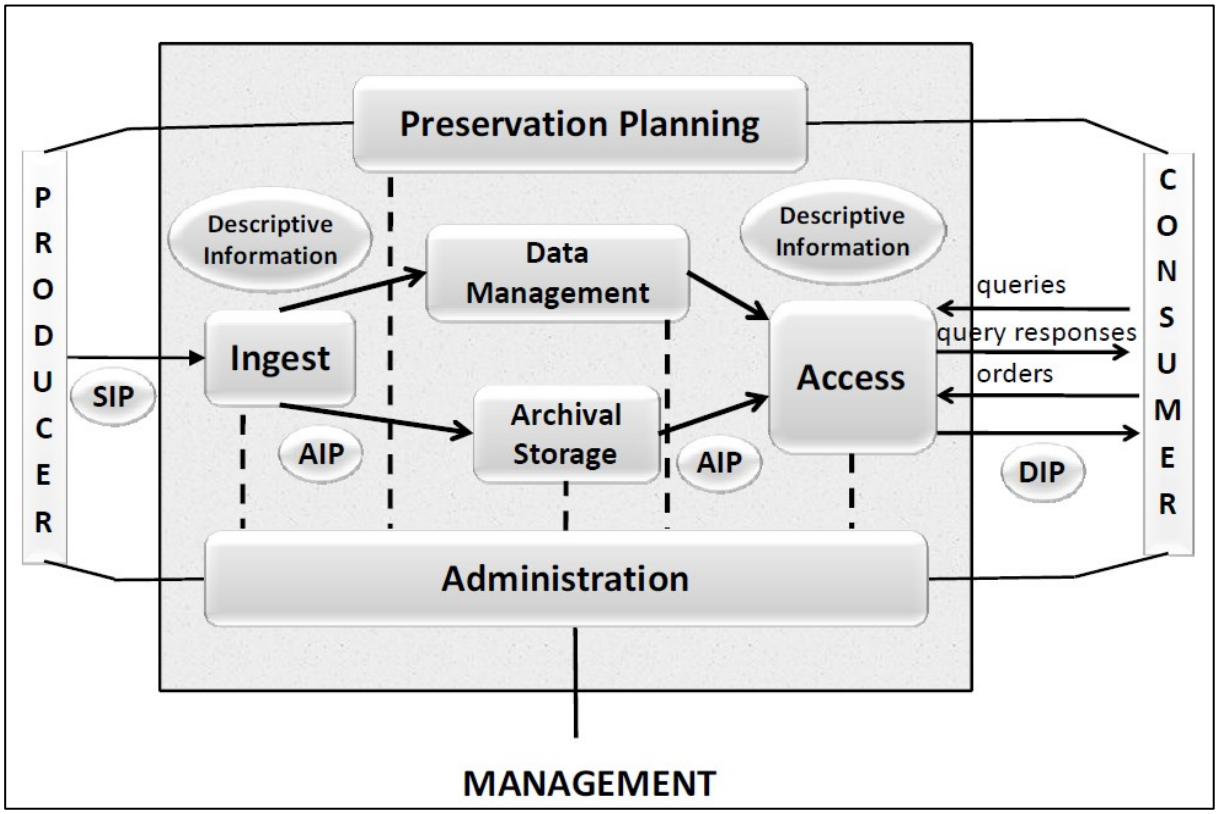
Os pacotes de informação (SIP, AIP e DIP) os quais perpassam os agentes (produtor, administrador e consumidor) interagem por intermédio de um conjunto complexo que agrega: entidades funcionais e serviços de apoio. De modo que a interação entre estas partes (pacotes de informação, agentes, entidades funcionais e serviços de apoio) irá possibilitar a efetividade do repositório OAIS.

[25] Lei nº 12.527, de 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

4.1.3.1 Entidades funcionais

Dentro do ambiente OAIS há seis entidades funcionais, que são: admissão (*ingest*), armazenamento arquivístico (*archival storage*), gestão de dados (*data management*), administração (*administration*), plano de preservação (*preservation planning*) e acesso (*access*). Neste ambiente, perpassam os pacotes de informação (SIP, AIP e DIP) nos quais são inseridas as informações descritivas (*descriptive information*) referentes às suas respectivas informação de conteúdo. A seguir, a "Figura 5 – Entidades funcionais do OAIS" apresenta uma esquematização simplificada da relação entre indivíduos, entidades funcionais e pacotes de informação.

Figura 5 – Entidades funcionais do OAIS



Fonte: (CCSDS, 2012, p. 4-1).

Conforme o OAIS, as entidades funcionais são entendidas da seguinte forma:

a) **Admissão (*ingest*)**: oferece serviços e processos para aceitar os SIP's dos produtores (ou de componentes internos sob controle da administração) e preparar os conteúdos para o seu armazenamento e para gestão de dados. Os processos internos desta entidade funcional se resumem em: receber SIP's, verificar a qualidade destes SIP's; e gerar AIP's em conformidade com os padrões de formatação de dados e padrões de documentação; extrair informações descritivas das AIP's para inclusão no banco de dados e coordenar as atualizações nas entidades funcionais de armazenamento arquivístico (*archival storage*) e de gestão de dados (*data management*);
b) **Armazenamento arquivístico (*archival storage*)**: fornece os serviços e processos para o armazenamento, manutenção e recuperação dos AIP's. Os processos internos desta entidade se resumem em: receber os AIP's da entidade de admissão e adicioná-los a área de armazenamento permanente; gerenciar sua hierarquia de armazenamento; refrescar as mídias em que os AIP's estão armazenados; executar rotinas de verificação de erros; ter capacidade de recuperação de desastres; e fornecer AIP's à entidade de acesso para cumprir as solicitações dos consumidores;
c) **Gestão de dados (*data management*)**: fornece os serviços e processos para incluir, manter e acessar tanto as informações descritivas, quanto os dados administrativos utilizados para gerenciar o OAIS. Os processos internos desta entidade se resumem em: administrar as funções de banco de dados do arquivo; atualizar o banco de dados; processar consultas sobre os seus dados e elaborar relatórios a partir dos resultados;
d) **Administração (*administration*)**: fornece os serviços e processos para o funcionamento global do sistema. Os processos internos desta entidade se resumem em: solicitar e negociar acordos de submissão com os produtores; realizar auditoria nas submissões para garantir que elas respeitem as normas de Arquivo; manter o gerenciamento das configurações de *hardware* e *software* do sistema; oferecer processos de engenharia de sistema para monitorar e melhorar as operações de arquivo; realizar um relatório das migrações/atualizações dos conteúdos; estabelece e mantém normas e políticas do OAIS; fornece suporte ao cliente; e ativa as solicitações armazenados;

e) **Planejamento da preservação (*preservation planning*)**: fornece serviços e processos para monitorar o ambiente do OAIS e prover recomendações para garantir que a informação armazenada no OAIS seja acessada e corretamente interpretada pela comunidade designada no longo prazo; mesmo que o ambiente de computação original se torne obsoleto. Os processos internos desta entidade se resumem em: avaliar os conteúdos do OAIS e recomendar atualizações periódicas de informação arquivada; desenvolver recomendações para padrões e políticas de arquivamento; fornecer relatórios periódicos de análise de risco e monitorar as mudanças no ambiente tecnológico, nos requisitos de serviço e na base de conhecimento da comunidade designada; desenvolver modelos para pacotes de informação, oferecendo assistência para adaptá-los na forma de SIP's e AIP's para submissões específicas; desenvolver planos de migração detalhados, protótipos de *software* e planos de teste a fim de permitir a implementação das metas de migração definidas pela entidade de administração;
f) **Acesso (*access*)**: oferece a serviços e processos necessários para dar suporte aos consumidores para determinação da existência, descrição, localização e disponibilização das informações armazenadas, permitindo que os consumidores solicitem e recebam produtos de informação. Os processos internos desta entidade se resumem em: realizar a comunicação com os consumidores a fim de receber solicitações; aplicar mecanismos de controle para limitar o acesso às informações protegidas; coordenar a execução das solicitações para serem concluídas com sucesso; gerar DIP's e entrega-los aos consumidores.

4.1.3.2 Detalhamento das entidades funcionais

Cada uma das seis entidades funcionais do OAIS possui um conjunto de processos internos que corroboram para o funcionamento do sistema como um todo. Além disso, há uma série de serviços de apoio essenciais ao OAIS. A seguir são detalhados os serviços de apoio, e posteriormente, o funcionamento e os processos internos das entidades funcionais do OAIS.

4.1.3.2.1 Serviços de apoio

Os serviços de apoio do OAIS são compostos por três categorias: serviços de sistema operacional, serviços de rede e serviços de segurança.

Dentre os serviços de um sistema operacional há serviços essenciais para operar e administrar a plataforma de aplicações e fornecer uma interface de interação entre o *software* e a plataforma de aplicação. Esses serviços incluem questões como:

- Operações de núcleo (*Kernel*), para oferece serviços de baixo-nível;
- Comandos e utilitários, para auxiliar nas atividades de operar o sistema;
- Extensão em tempo real, para definir interfaces de sistema e de aplicações;
- Gerenciamento do sistema, para definir e gerenciar a alocação, o acesso, e demais configurações do sistema;
- Serviços de segurança do sistema operacional, para especificar o controle de acesso aos dados, funções, recursos de *hardware* e *software*, e processo de usuários.

Os serviços de rede fornecem recursos e mecanismos para apoiar as aplicações distribuídas, as quais requerem acesso aos dados e a interoperabilidade de aplicações em ambientes de rede heterogênea. Esses serviços compreendem:

- A comunicação de dados, que envolve a interface, o programa de aplicação e especificações de protocolo para transmissão segura através das redes de comunicação;
- Acesso transparente aos arquivos de dados, disponibilizados em qualquer ponto da rede;
- Suporte para computador pessoal, ou seja, proporcionar interoperabilidade com outros sistemas operacionais;
- Serviços de chamada de procedimento remoto, que envolvem especificações para estender a chamada de processamento local para um ambiente distribuído;
- Serviços de segurança de rede envolvem acesso, autenticação, confidencialidade, integridade e controles de não repúdio, além de gerenciar

as comunicações entre os emissores e receptores de informação de uma determinada rede.

Os serviços de segurança fornecem recursos e mecanismos para proteger as informações e os tratamentos restritos no sistema de informação. O nível de proteção adequado é determinado com base no valor que a informação tem para os usuários finais da aplicação considerando as ameaças relacionadas a ela. Esses serviços incluem:

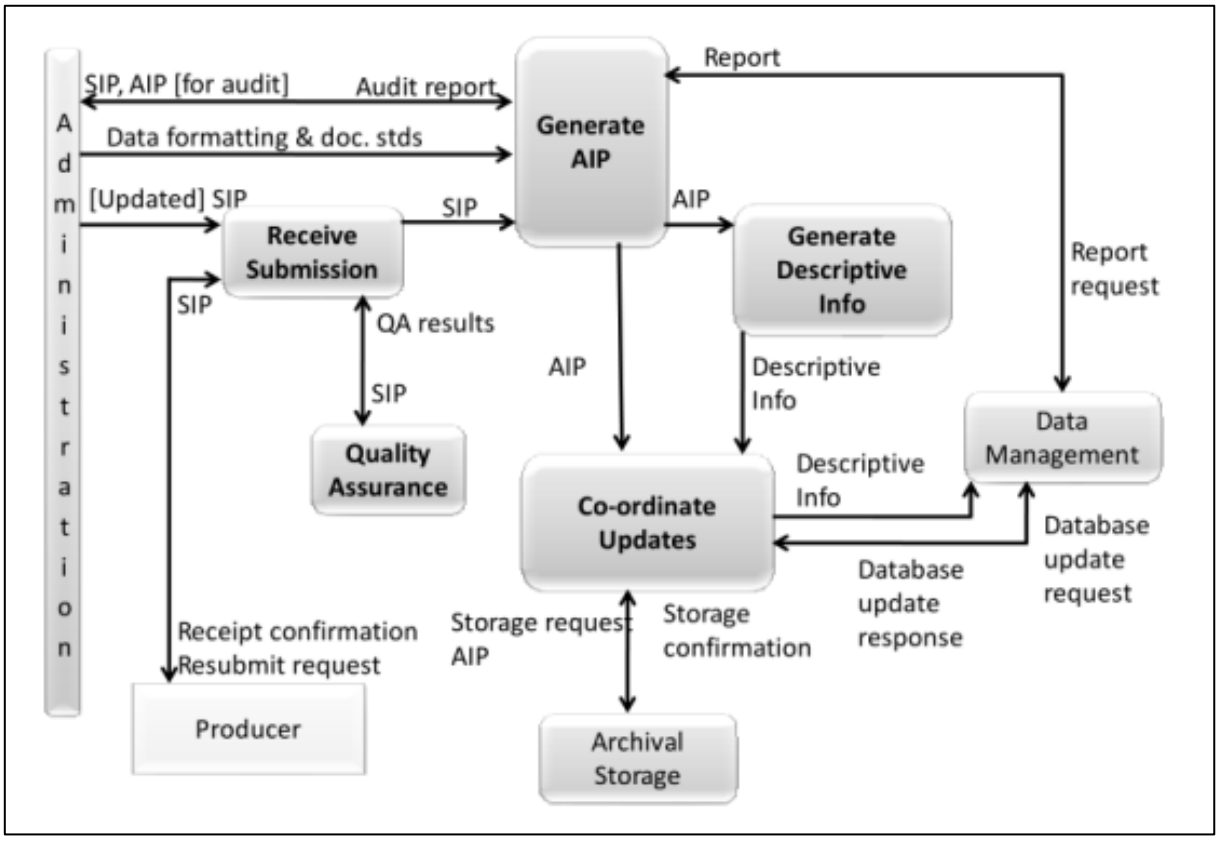
- Identificação/autenticação, para confirmar a identidade de quem requer uso do sistema;
- Controle de acesso, para prevenir o uso não autorizado, compreende permissões de acesso para leitura, gravação e eliminação de dados, além da execução de procedimentos;
- Integridade de dados, para garantir que os dados do sistema não serão alterados ou excluídos de forma não autorizada;
- Confidencialidade de dados, para garantir que os dados do sistema não serão disponibilizados ou revelados a indivíduos ou processos computacionais que não tenham sido autorizados;
- Não repúdio, impede que as entidades envolvidas em um intercâmbio de informação neguem seu envolvimento. Desta forma, evita que emissor e receptor neguem, respectivamente, o envio e o recebimento dos dados ou de seu conteúdo.

4.1.3.2.2 Admissão (*ingest*)

A entidade de admissão é composta por cinco processos que são: recebimento da submissão (*receive submission*), garantia da qualidade (*quality assurance*), geração do AIP (*generate AIP*), geração da informação descritiva (*generate descriptive info*) e coordenação de atualizações (*co-ordinate updates*). A entidade de admissão possui ainda relação com outras quatro entidades que são: produtor (*producer*), administração (*administration*), armazenamento arquivístico (*archival storage*) e gestão de dados (*data management*); ressaltando que a entidade produtor está situada fora do ambiente OAIS. A seguir a “Figura 6 –

Detalhamento da entidade de admissão" apresenta os diversos fluxos de informação da entidade.

Figura 6 – Detalhamento da entidade de admissão



Fonte: (CCSDS, 2012, p. 4-5).

O processo de **recebimento da submissão** (*receive submission*) oferece capacidade de armazenamento ou dispositivos adequados para receber um SIP do produtor. Os SIP's digitais podem ser entregues via transferência eletrônica, carregados a partir de uma mídia submetida ao Arquivo ou simplesmente montados no sistema de arquivos dados para acesso. Já os SIP's analógicos, provavelmente serão entregues por meio de processos convencionais de transporte (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Além disso, o processo de recebimento da submissão (*receive submission*) pode representar uma transferência legal de custódia das informações de conteúdo do SIP, e exigir a adição de controles especiais de acesso sobre o conteúdo. Este processo fornece uma confirmação de recebimento (*receipt confirmation*) de um SIP

para o produtor (*producer*), e ainda pode incluir uma solicitação de nova submissão (*resubmit request*) do SIP caso houver erros no envio (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Os documentos arquivísticos digitais, então submetidos via pacote de informação, são transmitidos de um determinado ambiente informatizado para um novo ambiente. Neste procedimento, os documentos armazenados no sistema de gestão, e que já passaram pelo crivo da avaliação, são recolhidos ao OAIS para a guarda de longo prazo. Observa-se que poderá haver a alteração da cadeia de custódia documental, uma vez que produtor e OAIS podem ser instituições ou pessoas diferentes.

O processo de **garantia da qualidade** (*quality assurance*) irá validar (*QA results*) o sucesso da transferência do SIP para a área de armazenamento temporário. No caso das submissões digitais, esses mecanismos podem incluir verificações de redundância cíclica; ou somas de verificação associados com cada arquivo de dados; ou ainda, o uso de registros de *logs* do sistema para registrar e identificar quaisquer erros na transferência de arquivos de dados ou de leitura/gravação de mídia (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Tal procedimento é essencial e permite identificar erros a fim de refazer o processo de submissão.

Em seguida, o processo de **geração do AIP** (*generate AIP*) transforma um ou mais SIP's em um ou mais AIP's em conformidade com os padrões de formatação de dados e padrões de documentação. Isto pode envolver conversões dos formatos de arquivo de dados, conversões de representação dos dados ou reorganização da informação de conteúdo nos SIP's. O processo de geração do AIP pode emitir solicitações de relatórios para a entidade de gestão de dados (*data management*) para obter relatórios de informação necessários para produzir informação descritiva que complementa o AIP. O processo de geração de AIP (*generate AIP*) envia o SIP ou o AIP para a entidade de administração (*administration*) onde será feita a auditoria, após, a entidade de administração (*administration*) retorna um relatório desta auditoria[26] (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

[26] Como resultado do relatório de auditoria, por exemplo, a administração pode solicitar a reunião de mais informações de representação para garantir que a informação de conteúdo seja compreensível e utilizável pela comunidade designada (CCSDS, 2012; ISO 14721:2012).

Observa-se que a transformação do SIP em AIP deve realizada em consonância com padrões previamente definidos. A informação de conteúdo estará inicialmente no SIGAD, de modo que todo o processo de gestão será realizado até que esta informação seja avaliada e, consequentemente, transferida/recolhida ao repositório OAIS na forma de pacote SIP. Posteriormente, o OAIS irá aceitar o pacote SIP, caso esteja em conformidade com suas políticas previamente definidas, e assim, transformá-lo em AIP para preservação de longo prazo. Desta forma, ressalta-se a importância da definição de políticas de preservação digital que prevejam questões como os formatos de arquivo e os padrões de metadados a serem utilizados nos ambientes de gestão e preservação.

O processo de **geração da informação descritiva** (*generate descriptive info*) extrai a informação descritiva do AIP e recolhe a informação descritiva de outras fontes para fornecê-la ao processo de coordenação de atualizações e ao processo de gestão de dados. Esta informação inclui metadados para auxiliar na pesquisa e recuperação dos AIP's; e ainda poderá incluir recursos especiais para serem utilizados na navegação e pelos instrumentos de busca (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Em se tratando de documentos digitais, as atividades de descrição ganham uma nova perspectiva. Tais atividades podem agregar, por exemplo, dados referentes aos sistemas e aos formatos de arquivo em que os documentos foram criados. Extrair metadados de um AIP é uma atividade de descrição, e tais metadados podem incorporar um sistema de recuperação da informação, e contribuir para uma melhor precisão do processo de busca.

O processo de **coordenação de atualizações** (*co-ordinate updates*) é responsável por transferir o AIP à entidade armazenamento arquivístico (*archival storage*) e informação descritiva (*descriptive info*) à entidade gestão de dados (*data management*). A transferência do AIP inclui uma solicitação de armazenamento (s*torage request AIP*) e isto pode representar uma transferência eletrônica, física, ou virtual[27]. Após a conclusão da transferência, e verificação da mesma, a entidade armazenamento arquivístico (*archival storage*) retorna a confirmação do armazenamento (s*torage confirmation*), e verifica (ou confirma) a identificação do AIP. Da mesma forma, o processo de coordenação de atualizações (*co-ordinate*

[27] Quando os dados permanecem no mesmo local.

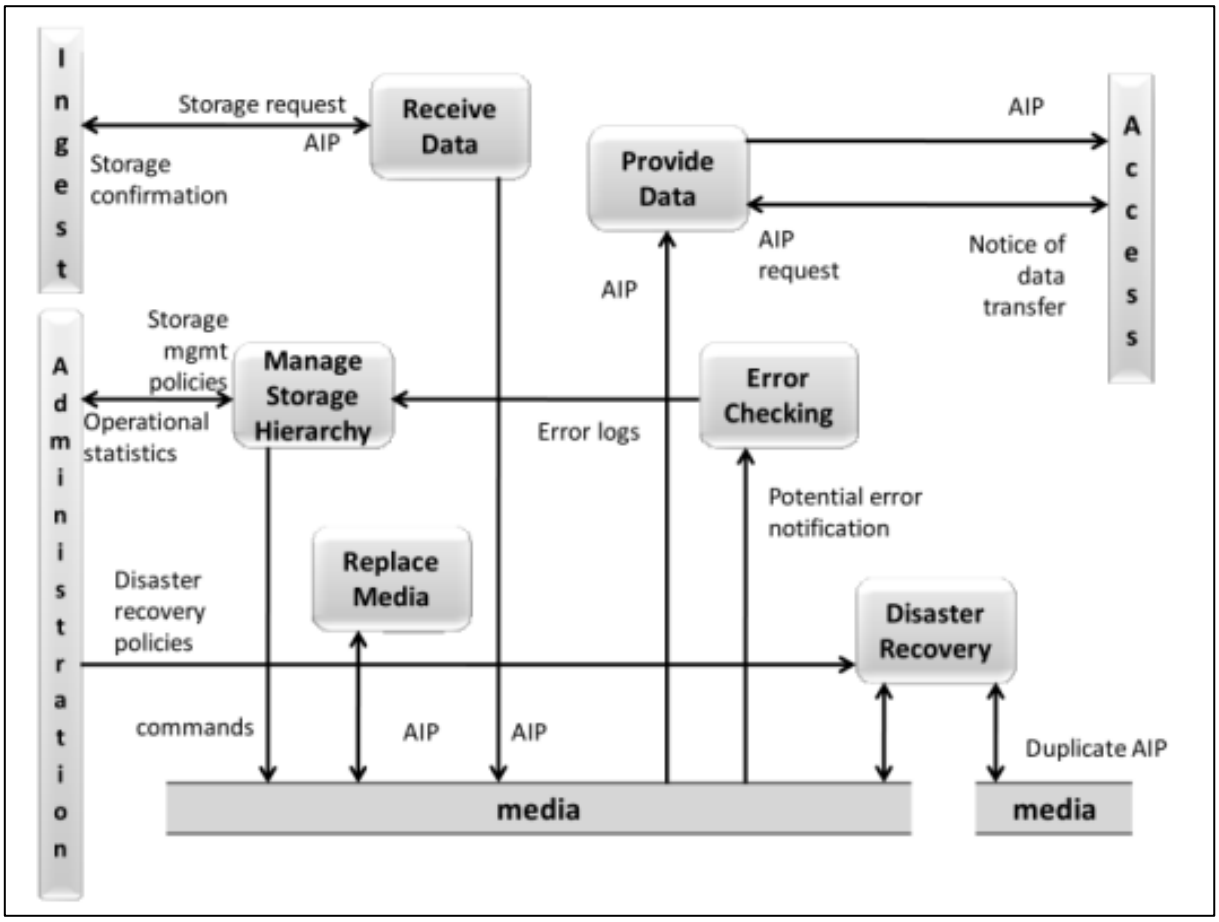
updates) incorpora a identificação do armazenamento das informações descritivas (*descriptive info*) referentes aos AIP's; transferindo as informações descritivas (*descriptive info*) para a entidade gestão de dados (*data management*) juntamente com uma solicitação de atualização do banco de dados (d*atabase update request*). Logo, a entidade de gestão de dados (*data management*) retorna uma resposta confirmando a atualização do banco de dados (*database update response*). Observa-se que a atualização da gestão de dados poderá ocorrer sem a necessidade de uma transferência para o armazenamento arquivístico (*archival storage*). Isto ocorre quando o SIP contém apenas informações descritivas (*descriptive info*) referentes a uma AIP pré-existente no armazenamento arquivístico (*archival storage*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Os fluxos de informação da entidade de admissão comportam rotinas que garantem: a correta submissão dos pacotes SIP; a extração dos metadados necessários; a transformação do SIP em AIP; e o seu consequente encaminhamento para o armazenamento arquivístico e para a gestão de dados.

4.1.3.2.3 Armazenamento arquivístico (*archival storage*)

A entidade armazenamento arquivístico é composta por seis processos, que são: recebimento de dados (*receive data*), gerenciamento da hierarquia de armazenamento (*manage storage hierarchy*), substituição de mídia (*replace media*), verificação de erros (*error checking*), recuperação de desastres (*disaster recovery*) e fornecimento de dados (*provide data*); além das próprias mídias (*media*) para armazenamento. A entidade armazenamento arquivístico possui ainda relação com outras três entidades que são: admissão (*ingest*), administração (*administration*) e acesso (*access*). A seguir a "Figura 7 – Detalhamento da entidade armazenamento arquivístico" apresenta os diversos fluxos de informação da entidade.

Figura 7 – Detalhamento da entidade armazenamento arquivístico



Fonte: (CCSDS, 2012, p. 4-8).

O processo de **recebimento de dados** (*receive data*) irá receber uma solicitação de armazenamento e um AIP da entidade de admissão (*ingest*), logo, moverá o AIP para que seja armazenamento de forma permanente no OAIS. A solicitação de transferência pode necessitar de indicação da frequência esperada para utilização dos objetos de dados (*data objects*) que compõe o AIP, a fim de possibilitar a seleção adequada dos meios de registro, sejam dispositivos de armazenamento ou mídias (*media*). Este procedimento irá selecionar o tipo de mídia (*media*), preparar os dispositivos ou volumes, e realizar a transferência física aos volumes da entidade armazenamento arquivístico (*archival storage*). Após o término da transferência, o processo de recebimento de dados (*receive data*) enviará uma mensagem à entidade de admissão (*ingest*) para confirmar o armazenamento

(*storage confirmation*)[28], incluindo a identificação de armazenamento do AIP (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Posteriormente ao processo de recebimento de dados, procede-se a uma série de fluxos de informação que visam armazenar o AIP corretamente.

O processo de **gerenciamento da hierarquia de armazenamento** (*manage storage hierarchy*) organiza o conteúdo dos AIP's nas mídias adequadas considerando as políticas de gerenciamento do conteúdo (*storage mgmt policies*), estatísticas operacionais (*operational statistics*), ou as diretrizes da solicitação de arquivamento vindas de entidade de admissão (*ingest*). Este processo também deve estar em conformidade com todos os níveis de serviços ou medidas de segurança especiais que sejam requeridas a fim de garantir o nível adequado de proteção para o AIP[29]. Este procedimento também fornece estatísticas operacionais (*operational statistics*) à administração (*administration*) resumindo o inventário de mídias disponíveis, a capacidade de armazenamento disponível nos diversos níveis de armazenamento hierárquico e as estatísticas de uso (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Observa-se que a organização dos pacotes AIP dentro da ambiente OAIS é fundamental para o seu respetivo tratamento e sua recuperação. Desta forma, o controle adequado contribuirá para a segurança dos materiais armazenados, agregando confiabilidade ao processo de preservação.

O processo **substituição de mídia** (*replace media*) possibilita a reprodução dos AIP's no longo prazo. Neste processo, informação de conteúdo (*content information*) e a PDI não devem ser alteradas. Entretanto, os dados que constituem a informação de empacotamento (*packaging information*) podem ser alterados desde que continuem a executar a mesma função, de modo que isto não cause perda de informações (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Ao substituir a mídia de armazenamento, ocorrerá uma simples replicação do conteúdo. Essencialmente, não ocorrerão alterações na informação de conteúdo e na PDI visto que as transformações podem ocorrer apenas no nível da mídia, ou seja, é possível substituir uma determinada mídia já em estágio de risco de deterioração por outra mídia nova, e de mesma natureza; da mesma forma, pode-se

[28] Logo, o processo de coordenação de atualizações (*co-ordinate updates*) irá receber essa confirmação.

[29] Estes requisitos incluem: armazenamento (*on-line*, *off-line* ou *near-line*); taxa de transferência exigida; taxa máxima de erros de bits permitida; ou ainda, um tratamento especial ou mesmo procedimentos de *backup*. Há ainda, o monitoramento de *logs* de erros para garantir que os AIP's não sejam danificados durante a transferência (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

substituir a mídia de uma tecnologia com risco de obsolescência por uma mídia atual. Neste segundo caso, ocorrerá alteração na informação de empacotamento, pois a nova mídia de armazenamento é de natureza diferente da mídia anterior.

Destaca-se ainda, que as estratégias migração devem selecionar um meio de armazenamento, considerando as taxas esperadas e reais de erros encontrados em diversos tipos de mídia, bem como o seu desempenho e os custos de propriedade relacionados. Além disso, se houver atributos dependentes de uma determinada mídia que representem parte da informação de conteúdo, será preciso preservar esta informação ao migrar para uma arquitetura diferente (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O processo de **verificação de erros** (*error checking*) fornece uma garantia, estatisticamente aceitável, de que nenhum dos componentes do AIP foi corrompido durante qualquer transferência interna do armazenamento arquivístico (*archival storage*). Este procedimento exige que todo o *hardware* e *software* dentro do OAIS forneçam notificações dos possíveis erros, de modo que estes erros sejam encaminhados, na forma de registro (*logs*) de erros padronizados, para serem verificados pela equipe da entidade armazenamento arquivístico (*archival storage*). A informação de fixidez da PDI fornece certa garantia de que as informações de conteúdo não serão alteradas quando o AIP for movido ou acessado, bem como, uma informação semelhante é necessária para proteger a própria PDI. Desta forma, o OAIS poderá usar um mecanismo padrão para rastrear e verificar a validade de todos os objetos de dados (*data object*) armazenados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A verificação de erros é um processo essencial, e quanto mais cedo for detectada, minimizam substancialmente os riscos de perda de informação do AIP. Em se tratando de documentos digitais, será indispensável a implementação de rotinas de verificação e monitoramento dos conteúdos. Tais rotinas são uma peculiaridade dos sistemas digitais e que pode ser justificada pelo fato de que as alterações proferidas sobre estres registros são praticamente imperceptíveis. Assim, qualquer alteração na sequência de *bits* de um objeto digital poderá corromper os dados impossibilitando o acesso aos documentos, além de comprometer a sua autenticidade.

O processo **recuperação de desastres** (*disaster recovery*) fornece um mecanismo para duplicar os conteúdos digitais do OAIS (*duplicate AIP*) e,

preferencialmente, armazenar as cópias em uma instalação fisicamente separada. Este processo normalmente é realizado por meio da cópia de conteúdos do arquivo para mídias de armazenamento removíveis; mas também pode ser realizado pelo transporte de *hardware* ou via transferências de dados em rede. Os detalhes da política de recuperação de desastres são especificados pela entidade administração (*administration*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A realização de cópias de segurança não se configura como um método de preservação digital propriamente dito, e sim, em um procedimento de segurança da informação. Isto porque previne desastres, no entanto, não profere tratamento em nível físico, lógico e conceitual. Desta forma, a cópia de segurança deverá ter como única finalidade, a prevenção de desastres, ressaltando-se assim, a necessidade de se localizar em um local fisicamente distante da estruturada de armazenamento do Arquivo OAIS.

O processo **fornecimento de dados** (*provide data*) disponibiliza as cópias dos AIP's armazenados para a entidade de acesso (*access*). Este processo recebe uma solicitação de AIP que identifica o AIP solicitado e o fornece conforme tipo de mídia solicitada ou ainda pode transferir o AIP para uma área de armazenamento temporário. Junto com a entrega do pedido, o processo de fornecimento de dados (*provide data*) envia uma notificação da transferência de dados para a entidade de acesso (*access*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Quanto à entrega dos materiais solicitados, cabe ressaltar que, o consumidor não tem acesso direto ao interior do repositório digital. Isto não implica em nenhum tipo de restrição aos conteúdos[30], mas sim em uma separação lógica que é expressão na relação das entidades: armazenamento arquivístico e acesso. O consumidor irá interagir com a entidade de acesso, e esta fará a solicitação para a entidade armazenamento arquivístico, a qual entregara uma cópia do material solicitado. Tal procedimento presume um nível mais elevado de confiança, principalmente no que se refere às invasões de *hackers*.

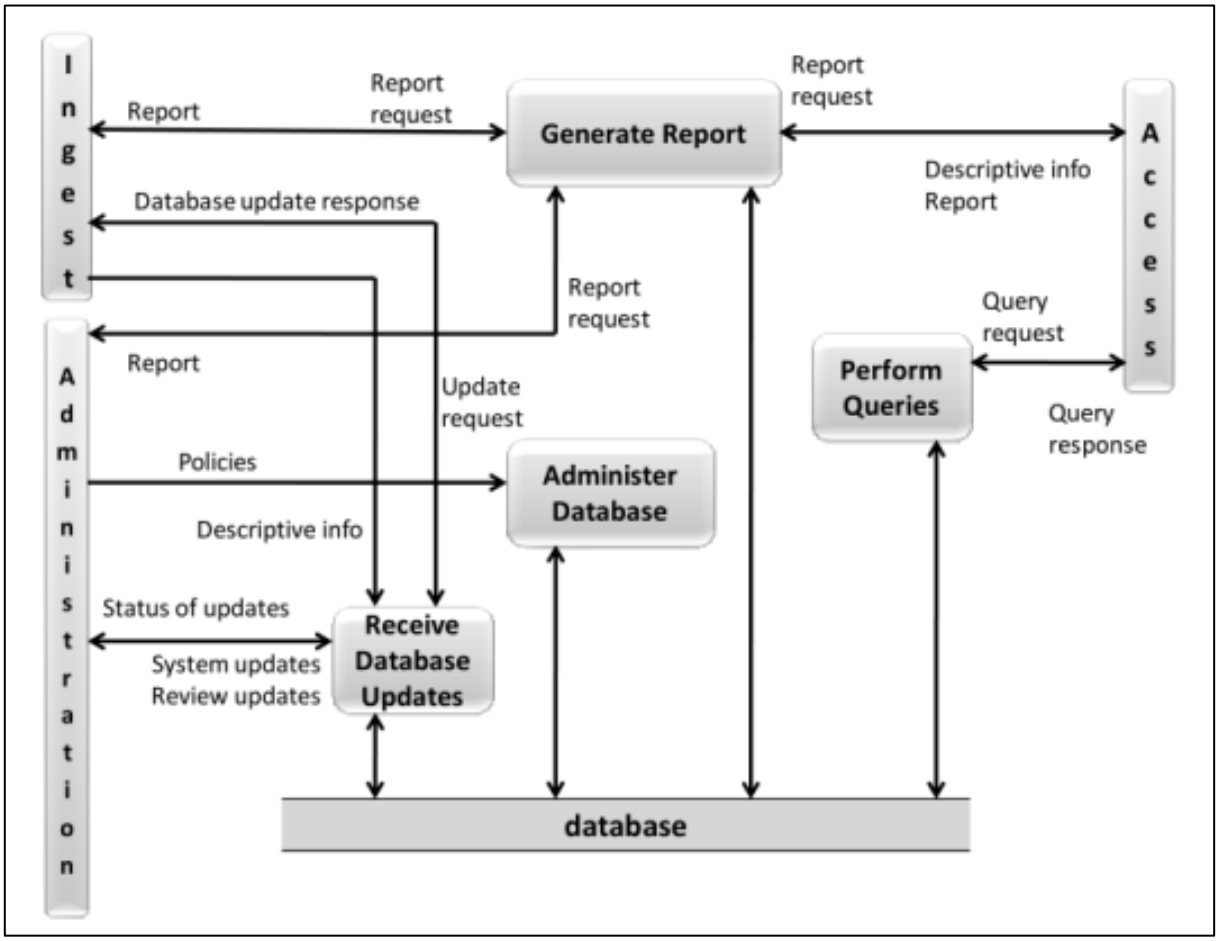
Logicamente, uma possível invasão aconteceria na plataforma de acesso, logo, os materiais armazenados na entidade armazenamento arquivístico ficariam seguros em um primeiro momento; mesmo assim será necessário definir rotinas de segurança que monitorem a rede a fim de identificar potenciais invasões ao OAIS.

[30] Salvo os casos em que seja definido algum grau de sigilo.

4.1.3.2.4 Gestão de dados (*data management*)

A entidade gestão de dados é composta por quatro processos, que são: administração do banco de dados (*administer database*), execução de consultas (*perform queries*), produção de relatório (*generate report*) e recebimento de atualizações do banco de dados (*receive database updates*). Esta entidade possui ainda relação com outras três entidades que são: admissão (*ingest*), administração (*administration*) e acesso (*access*); além disso, tem por função gerir o banco de dados (*database*). A seguir a "Figura 8 – Detalhamento da entidade gestão de dados" apresenta os diversos fluxos de informação da entidade.

Figura 8 – Detalhamento da entidade gestão de dados



Fonte: (CCSDS, 2012, p. 4-10).

O processo **administração do banco de dados** (*administer database*) é responsável por manter a integridade do banco de dados da entidade gestão de dados (*data management*), o qual armazena as informações descritivas (*descriptive info*) e as informações do sistema. As informações descritivas (*descriptive info*) identificam e descrevem os conteúdos do Arquivo OAIS, já as informações do sistema são usadas para apoiar suas operações. O processo de administração do banco de dados (*administer database*) é responsável por definir esquemas ou tabelas de descrições necessárias para apoiar os processos de gestão de dados, e então validar o conteúdo interno do banco de dados. Por fim, o processo de administração do banco de dados segue as políticas (*policies*) recebidas pela entidade de administração (*administration*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A entidade de gestão de dados administra um banco de dados que contém informações relacionadas aos objetos digitais armazenados. Em geral, são de funcionamento do OAIS enquanto sistema e informações descritivas. Tais informações descritivas normalmente são estruturadas em metadados que seguem padrões amplamente aceitos pela comunidade de preservação e de usuários. O padrão de metadados deverá ser previamente definido pelo administrador do OAIS, desta forma, será preciso orientar os produtores de conteúdo quanto aos padrões usados no repositório digital, evitando a perca de informações descritivas que sejam fundamentais para agregar confiabilidade aos documentos arquivísticos custodiados.

O processo **execução de consultas** (*perform queries*) recebe uma solicitação de consulta (*query request*) da entidade de acesso (*access*) e executa a consulta que irá gerar uma resposta (*query response*) a ser transmitida para o solicitante (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Desta forma, conteúdos da entidade gestão de dados podem ser entregues juntamente ao consumidor por meio do pacote DIP, o qual conterá os respectivos objetos armazenados na entidade armazenamento arquivístico.

O processo **produção de relatório** (*generate report*) recebe um pedido de relatório (*report request*) das entidades de admissão (*ingest*), acesso (*access*) ou administração (a*dministration*), e então, executa as consultas ou outros processos que sejam necessários para produzir o relatório[31] a ser entregue ao solicitante

[31] Os relatórios típicos podem incluir resumos dos conteúdos do OAIS, por categoria ou estatísticas de uso destes conteúdos. Além disso, poderá receber um pedido de relatório da entidade de acesso

(ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Neste caso, ocorre a solicitação de relatórios customizados dos conteúdos disponíveis e de suas informações de referência.

O processo **recebimento de atualizações do banco de dados** (*receive database updates*) adiciona, altera ou exclui informações da área permanente da entidade de gestão de dados (*data management*). Dentre as principais fontes de atualização, pode-se citar a entidade de admissão (*ingest*), que fornece Informações descritivas (*descriptive info*) para os novos AIP; e a entidade de administração (*administration*), que fornece atualizações do sistema (*system updates*) e revisão das atualizações (*review updates*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Estas atualizações são realizadas após a admissão de novos pacotes de informações, sendo assim, é necessário atualizar o banco de dados, o qual também contém informações de caráter permanente, pois são informações referentes aos objetos digitais armazenados na entidade armazenamento arquivístico. Com relação às atualizações do sistema, vindas da entidade de administração, ressalta-se que estas são um requisito mínimo para que um repositório digital possa ter alguma perspectiva de longevidade.

Em resumo, as transações da entidade de admissão (*ingest*) consistem em informações descritivas (*descriptive info*) que identificam novos AIP's armazenados no arquivo. As atualizações do sistema (*system updates*) incluem todas as informações relacionadas a estatísticas operacionais, informação de consumidor e status da solicitação. A revisão das atualizações (*review updates*) é gerada em decorrência de revisões e atualizações periódicas dos valores de informação. Desta forma, o processo de recebimento de atualizações do banco de dados (*receive database updates*) fornece relatórios periódicos à entidade de administração (*administration*) resumindo o status das atualizações (*status updates*) do banco de dados; e também envia uma resposta de atualização do banco de dados (*database update response*) para a entidade de admissão (*ingest*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

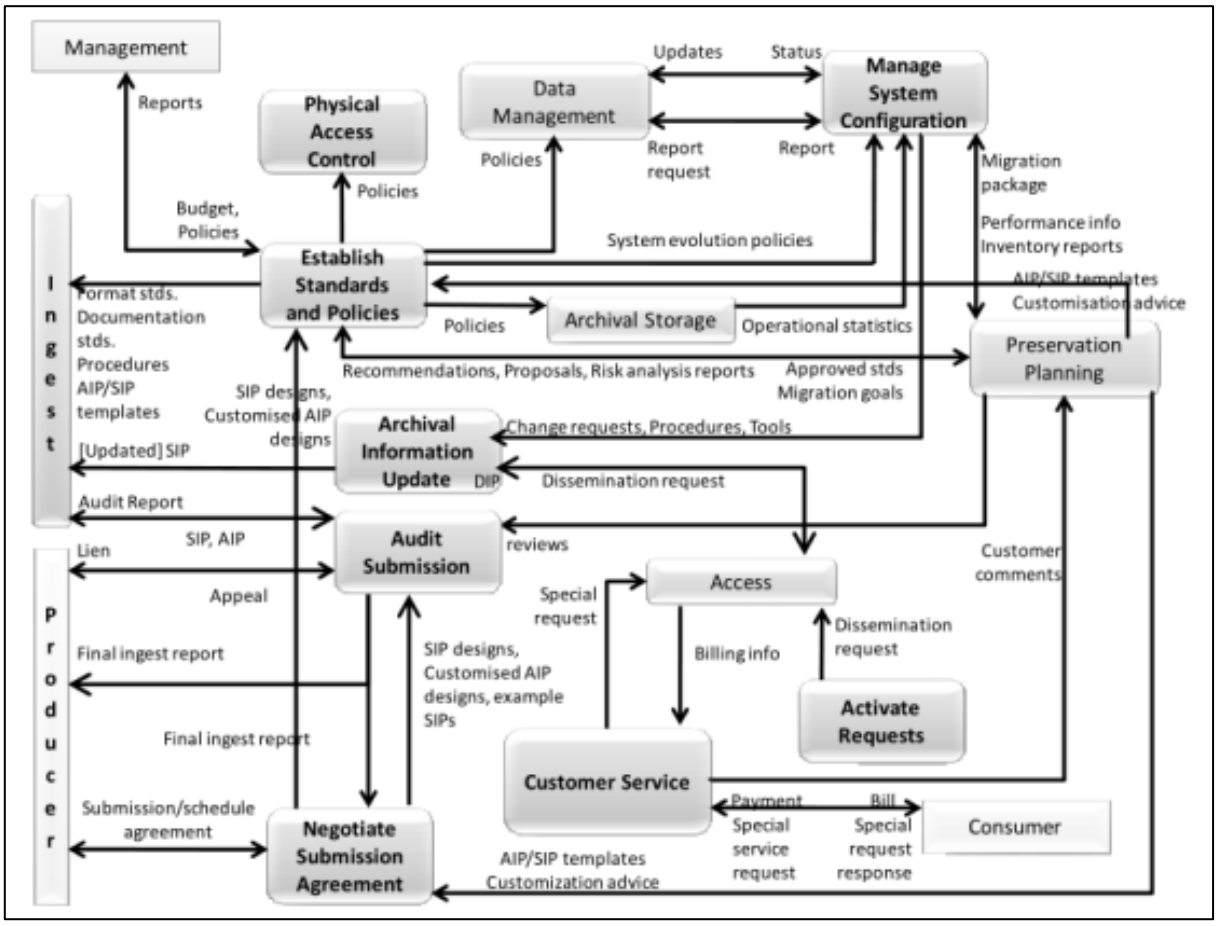
(*access*) e fornece informações descritivas (*descriptive info*) para um AIP específico (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.3.2.5 Administração (*administration*)

A entidade administração (*administration*) é composta por oito processos, que são: negociar acordo de submissão (*negotiate submission agreement*), gerenciar configurações do sistema (*manage system configuration*), atualizar informação arquivada (*archival information update*), controle de acesso físico (*physical access control*), estabelecer padrões e políticas (*establish standards e policies*), auditoria de submissão (*audit submission*), solicitações ativas (*activate requests*) e atendimento ao cliente (*customer service*). Esta entidade possui ainda relação com todas as outras entidades, tanto internas[32], quanto externas[33] ao ambiente do repositório OAIS. A seguir a "Figura 9 – Detalhamento da entidade gestão de dados" apresenta os diversos fluxos de informação da entidade.

[32] Admissão (*ingest*), gestão de dados (*data management*), armazenamento arquivístico (*archival storage*), plano de preservação (*preservation planning*) e acesso (*access*); além do próprio administrador (*management*).
[33] Produtor (*producer*) e consumidor (*consumer*).

Figura 9 – Detalhamento da entidade administração



Fonte: (CCSDS, 2012, p. 4-11).

O processo **negociar acordo de submissão** (*negotiate submission agreement*) negocia a cadeia de custódia documental, de modo que solicita as informações de conteúdo que sejam desejáveis ao OAIS e negocia acordos de submissão com os produtores (*producer*). Este procedimento também negocia um cronograma (*schedule*) de submissão de dados com o produtor (*producer*). Desta forma, mantém-se um cronograma (*schedule*) de espera das submissões de dados necessárias à transferência de SIP's ao OAIS; além de manter requisitos dos recursos para fornecer apoio às respectivas admissões (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Neste fluxo de informação pode-se situar a função arquivística de aquisição, desta forma, a entidade de administração negocia a aquisição dos objetos digitais junto ao produtor, caso haja interesse. Conforme Rousseau e Couture (1998), a

aquisição consiste na transmissão da propriedade dos documentos, pode ser realizada, por exemplo, por meio de doação ou compra (ROUSSEAU; COUTURE, 1998). Logo, ocorrerá também, a transferência das responsabilidades ao novo custodiador do acervo.

A aquisição de documentos arquivísticos digitais é em tese, mais complexa, se comparada aos documentos analógicos. Visto que o antigo custodiador deve ter mecanismos que permitam demonstrar a autenticidade dos documentos que serão adquiridos pelo OAIS. Já o novo custodiador deverá demostrar capacidade de preservar o acesso e a autenticidade dos documentos adquiridos, tornando-se assim o novo responsável pelo acervo (SANTOS; FLORES, 2016). É essencial destacar a necessidade de registrar a alteração do responsável em metadados.

Este processo irá receber modelos customizados para AIP's e SIP's (*SIP/AIP templates*), bem como avisos de adaptação (*customization advice*) vindos da entidade de planeamento da preservação (*preservation planning*); e como parte do processo de aprovação da submissão, são enviados projetos de SIP's, projetos de AIP's personalizados e exemplos de SIP's (*SIP designs, customised AIP designs, example SIP's*) ao processo de auditoria da submissão (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Na versão do ano de 2012 do OAIS (CCSDS, 2012; ISO 14721:2012), há um novo fluxo de informação entre os processos: negociar acordo de submissão (*negotiate submission agreement*) e estabelecer padrões e políticas (*establish standards and policies*). Desta forma, os projetos de SIP's, projetos de AIP's personalizados (*SIP designs, customised AIP designs*) também são enviados ao processo estabelecer padrões e políticas (*establish standards and policies*) para que posteriormente possam ser utilizados pela entidade de admissão (*ingest*). O modelo OAIS ressalta que os formatos e os procedimentos de submissão de dados devem ser claramente documentados por meio de políticas de submissão de dados, de modo que as entregas sejam identificadas pelo produtor no processo de submissão (*submission*).

O processo **gerenciar configurações do sistema** (*manage system configuration*) fornece engenharia de sistemas para monitorar continuamente as funcionalidades de todo o sistema de arquivo, além de controlar sistematicamente alterações nas configurações. Este processo irá manter a integridade e a rastreabilidade da configuração durante todas as fases do ciclo de vida do sistema.

Além disso, este processo possibilita a realização de auditorias sobre as operações, o desempenho e a utilização do sistema. Ele envia solicitações de relatórios (*report request*) para a entidade de gestão de dados (*data management*) a fim de receber relatórios (*report*) informações do sistema; além de receber estatísticas operacionais (*operational statistics*) da entidade armazenamento arquivístico (*archival storage*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Além destas questões, o processo gerenciar configuração do sistema (*manage system configuration*) resume os relatórios recebidos a fim de fornecer: informação de desempenho para o OAIS, com o envio de relatórios para o processo estabelecer padrões e políticas (*establish standards and policies*); e relatórios de inventários de conteúdo para a entidade planejamento da preservação (*preservation planning*). Desta forma, recebe pacotes de migração (*migration package*) da entidade planejamento da preservação (*preservation planning*) e orientações com relação à evolução do processo de estabelecer padrões e políticas (*establish standards and policies*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Com este processo é possível monitorar questões relativas às configurações e ao desempenho do OAIS, e possibilitar auditorias sobre o uso do sistema. Observa-se aqui, a necessidade deste processo, pois agrega segurança e confiabilidade quanto aos métodos de preservação e gerenciamento do sistema.

O processo **atualizar informação arquivada** (*archival information update*) permite atualizar os conteúdos do repositório. Também recebe solicitações de mudança (*change requests*), procedimentos (*procedures*) e ferramentas (*tools*) do processo gerenciar configurações do sistema (*manage system configuration*). Além disso, o processo atualizar informação arquivada fornece atualizações enviando uma solicitação de difusão (*dissemination request*) para a entidade de acesso (*access*), que posteriormente atualiza o conteúdo dos pacotes DIP's e os reenvia como SIP's para a entidade de admissão (*ingest*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Este processo tem como finalidade atualizar as informações quando necessário, e para garantir a qualidade da atualização, irá reenviar o pacote atualizado à entidade de admissão, perpassando pelos fluxos de informação necessários.

O processo **controle de acesso físico** (*physical access control*) tem por objetivo restringir ou permitir o acesso físico aos materiais do Arquivo conforme as suas políticas (*policies*) previamente definidas pelo processo estabelecer padrões e

políticas (*establish standards and policies*). Este é um procedimento de segurança da informação complementar, pois além de restringir o acesso lógico aos materiais é necessário que o acesso físico seja ponderado. Isto porque alterações em nível lógico podem ser rastreadas e restauradas, já os danos físicos são irreparáveis e levam a perda de finitiva dos objetos digitais.

O processo **estabelecer padrões e políticas** (*establish standards and policies*) é responsável pela definição e manutenção dos padrões e das políticas arquivo, desta forma, recebe informações referentes a orçamentos (*budget*), políticas (*policies*), e orientações quanto à utilização dos recursos por parte do administrador do repositório (*management*); da mesma forma, retorna relatórios (*reports*) periódicos para esta entidade. Este processo recebe recomendações da entidade planejamento da preservação (*preservation planning*) para aprimoramento do OAIS, contendo recomendações (*recommendations*) de novas normas e padrões, bem como relatórios de análise de riscos (*risk analysis reports*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Com base na análise dos dados recebidos, este processo estabelece os padrões e as políticas as quais são enviados a outros processos da entidade de administração (*administration*) e para outras entidades funcionais do OAIS. Dentre estas definições, podem-se citar os padrões de formato (*format standards*) e de procedimentos (*procedures AIP/SIP templates*) a serem seguidos durante o processo de admissão. Além da aprovação de padrões (*approved standards*) e das metas de migração (*migration goals*) à entidade planejamento da preservação (*preservation planning*). Este processo também irá desenvolver políticas para gerenciamento de conteúdo, definindo metas de migração para evitar a obsolescência dos formatos de arquivo. Além disso, definirá políticas para administração do banco de dados, para recuperação de desastres; e para a segurança dos conteúdos[34] (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Observa-se aqui, que há um diálogo com a entidade plano de preservação, para que sejam definidas as políticas de preservação. Desta forma, a entidade plano de preservação irá propor um determinado padrão e o qual será avaliado e implementado. Em resumo, o processo estabelecer padrões e políticas tem por

[34] Isto inclui o controle de acesso físico (*physical access control*) e o controle de erros dentro do repositório OAIS.

finalidade analisar as recomendações recebidas da entidade planejamento da preservação.

O processo **auditoria de submissão** (*audit submission*) tem por finalidade verificar se os pacotes (SIP's ou AIP's) submetidos atendem as especificações do acordo de submissão, bem como a sua inteligibilidade por parte da comunidade designada. Este processo passa por revisões (*reviews*) realizadas pela entidade plano de preservação (*preservation planning*). Além disso, deve verificar se a qualidade dos dados atende aos requisitos do OAIS e do comitê de revisão; e se há informação de representação (*representation information*) e informação descritiva de preservação (*preservation description information*) adequadas para garantir a correta interpretação das informações de conteúdo (*content information*) pela comunidade designada (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Observa-se que o processo de auditoria pode determinar que algumas partes do SIP's não são apropriados para serem admitidos no OAIS, solicitando o seu reenvio ou exclusão, e desta forma, um relatório de auditoria (*audit report*) é fornecido para entidade de admissão (*ingest*). Posteriormente, todas as inconformidades são relatadas ao produtor, que irá, em seguida, submeter novamente o SIP para a entidade de admissão (*ingest*) ou apelar (*appeal*) da decisão junto à entidade de administração (*administration*). Após a conclusão da auditoria[35], um relatório final de admissão (*final ingest report*) é preparado e fornecido ao produtor (*producer*) e ao processo negociar acordo de submissão (*negotiate submission agreement*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

É importante salientar que este processo de auditoria é relativo a conformidade dos pacotes com o que foi definido nas políticas de preservação do OAIS, não sendo relacionado ao processo de auditoria e certificação de repositórios digitais, o qual visa auditar o sistema como um todo. O processo auditoria da submissão pode ser entendido como um procedimento de rotina executado a fim de verificar a conformidade dos materiais recebidos com os padrões previamente definidos; e em caso contrário, solicitar o reenvio e proceder a substituição do pacote.

[35] Os métodos de auditoria podem incluir: a amostragem, análise periódica e revisão por pares.

O processo **solicitações ativas** (*activate requests*) mantém um registro das solicitações, e periodicamente, compara estas solicitações com os conteúdos do OAIS para verificar se todos os dados necessários estão disponíveis. Caso estes dados estejam disponíveis, este processo gera uma solicitação de difusão (*dissemination request*) que é enviada para entidade de acesso (*access*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Com esta contínua verificação é possível identificar os conteúdos que estão indisponíveis no OAIS, e assim providenciá-los. Em caso de disponibilidade dos materiais é possível gerar o DIP.

O processo de **atendimento ao cliente** (*customer service*) será responsável por gerenciar as contas dos consumidores (criar, excluir e realizar manutenção), além de recolher as informações de faturamento (*billing information*) junto a entidade de acesso (*access*), enviar faturas (*bill*) aos consumidores, e consequentemente, recolher os seus pagamentos (*payment*), referentes à utilização dos recursos do OAIS. Este processo responde pedidos gerais de informação, bem como questões sobre os serviços e produtos da entidade de acesso (*access*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Tal processo transforma o repositório OAIS em um sistema de negócios que pode ser implementado no âmbito da iniciativa privada, contemplando diversos ramos que comercializem informações. Já no setor público, o faturamento frente ao consumidor pode ser realizado como forma de reembolso[36], caso o acesso demande custos ao Arquivo.

Além do contexto das instituições sem fins lucrativos como os Arquivos, é possível implementar o OAIS no âmbito do comércio eletrônico e telecomunicações, os quais vêm constituindo a nova economia (*new economy*) de mercado.

> [...] devido ao fato de serem em boa parte de caráter imaterial, essas inovações propagam-se rapidamente, apesar das distâncias e para além das fronteiras; portanto, servem particularmente ao desenvolvimento da concorrência, e de uma concorrência doravante mundial. Em uma economia globalizada, as inovações não conhecem mais fronteiras. Elas essencialmente se traduzem em progressos da produtividade do trabalho, independente do setor de atividade envolvido. As novas técnicas permitem a um número crescente de pessoas de se pôr em contato com um número crescente de mercados, quer se trate de seus clientes ou de seus

[36] Por exemplo, um consumidor pode solicitar um serviço no qual os pacotes DIP sejam gravados em dez unidades de *Digital Versatile Disc* (DVD), desta forma, o Arquivo poderá proceder a cobrança de tais unidades na forma de reembolso dos gastos.

> fornecedores, e de adquirir informações úteis a um preço cada vez mais reduzido (JESSUA, 2016, p. 47).

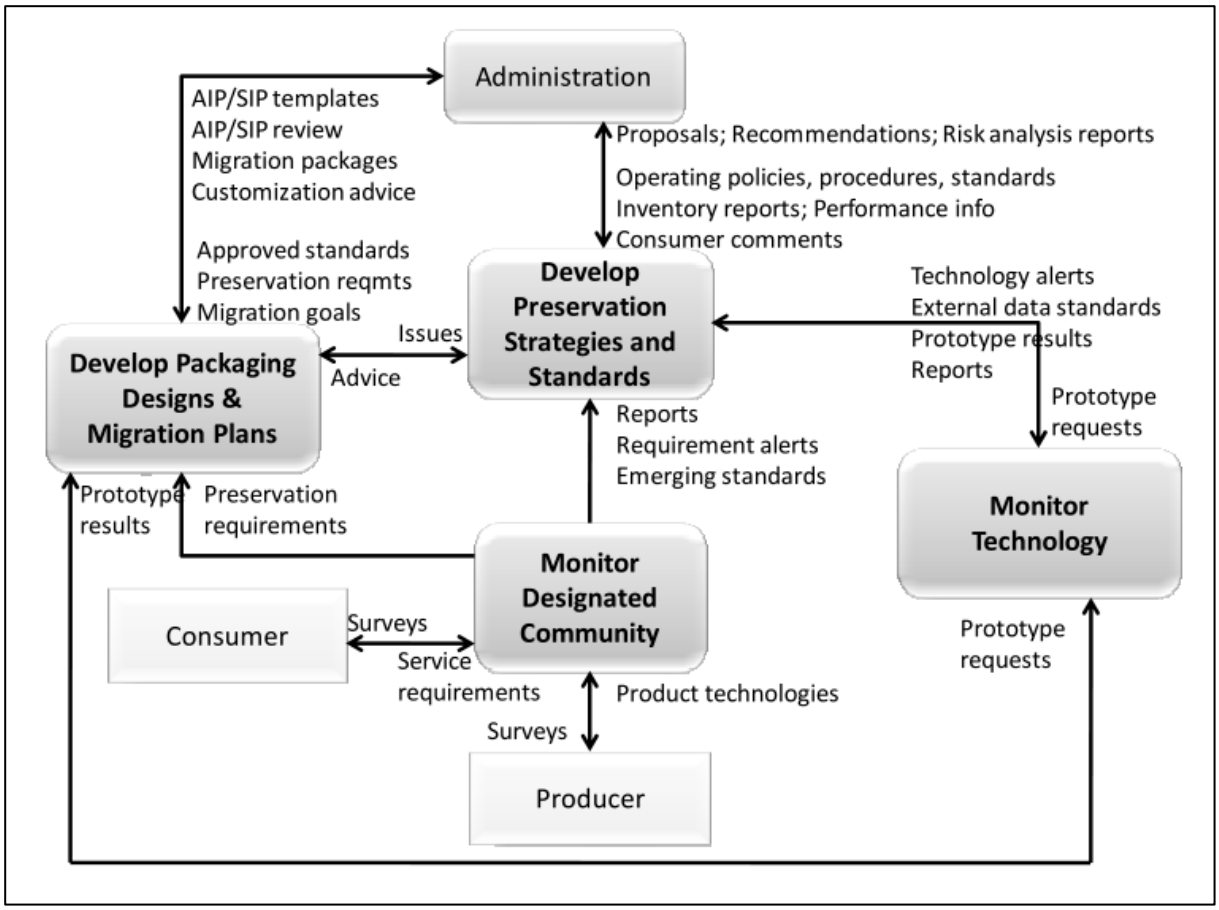
Um impacto da *new economy*, saliente no que tange a evolução do documento analógico ao digital, consiste, por exemplo, na perspectiva de redução dos custos de produção unitária do documento; e assim, aplicando-se novos procedimentos e métodos de organização e tratamento das informações digitais. Desta forma, surgem novos produtos, junto com as novas perspectivas de negócios; um repositório digital que vende informações seria um exemplo para este deste caso.

4.1.3.2.6 Plano de preservação (*preservation planning*)

A entidade plano de preservação (*preservation planning*) é composta por quatro processos, que são: monitoramento da comunidade designada (*monitor designated community*), monitoramento de tecnologia (*monitor technology*), desenvolvimento de estratégias e padrões de preservação (*develop preservation strategies and standards*) e desenvolvimento de pacotes e planos de migração (*develop packaging designs & migration plans*). Esta entidade possui ainda, relações com outras entidades, tanto internas[37], quanto externas[38] ao ambiente OAIS. A seguir a “Figura 10 – Detalhamento da entidade plano de preservação” apresenta os diversos fluxos de informação da entidade.

[37] Administração (*administration*).
[38] Produtor (*producer*) e consumidor (*consumer*).

Figura 10 – Detalhamento da entidade planejamento da preservação



Fonte: (CCSDS, 2012, p. 4-14).

O processo **monitoramento da comunidade designada** (*monitor designated community*) interage com produtores (*producer*) e consumidores (*consumer*) a fim de identificar mudanças nos requisitos[39] de seus serviços (*service requirements*), bem como nas tecnologias dos seus produtos (*product technologies*). Este processo pode ser realizado, por exemplo, por meio de pesquisas (*surveys*) e revisões periódicas. Desta forma, fornecerá relatórios (*reports*), alertas de requisitos (*requirement alerts*) e padrões emergentes (*emerging standards*) ao processo desenvolvimento de estratégias e padrões de preservação (*develop preservation strategies and standards*). E por fim, envia requisitos de preservação (*preservation requirements*) para o processo desenvolvimento de pacotes e planos de migração (*develop*

[39] Formatos de arquivo, tipos de mídia, preferências por determinados *software*, novas plataformas de *hardware*/*software* e mecanismos para comunicação com o OAIS.

packaging designs & migration plans) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Através da interação com produtores e consumidores, este processo, verifica as novas tendências em tecnologias. Desta forma, e possível definir novos padrões e desenvolver estratégias de preservação capaz de comportar as transformações no ambiente externo ao OAIS. Trata-se de monitorar o comportamento dos agentes externos, podendo assim, prever a necessidade de comportar um determinado formato de arquivo, padrão ou serviço a ser prestado.

O processo **monitoramento de tecnologia** (*monitor technology*) acompanha as tecnologias digitais emergentes, padrões e plataformas de *hardware* e *software* do ambiente OAIS, a fim de identificar tecnologias que podem se tornar obsoletas, que possam causar incompatibilidades e dificuldades de acesso.

Este processo também pode trabalhar com protótipos de padrões de formatos emergentes, podendo receber solicitações de protótipos (*prototype requests*) vindos dos processos de desenvolvimento de estratégias e padrões de preservação (*develop preservation strategies and standards*) e desenvolvimento de pacotes e planos de migração (*develop packaging designs & migration plans*). Posteriormente o processo de monitoramento da tecnologia envia relatórios (*reports*), padrões externos de dados (*external data standards*), resultados dos protótipos (*prototype results*) e alertas de tecnologias (*technology alerts*) ao processo desenvolvimento de estratégias e padrões de preservação (*develop preservation strategies and standards*); da mesma forma, envia os resultados da prototipação pra o processo desenvolvimento de pacotes e planos de migração (*develop packaging designs & migration plans*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O processo de monitoramento da tecnologia está voltado para o ambiente interno do OAIS, sendo responsável por verificar e identificar as tendências em obsolescência tecnológica de seus componentes. Por finalidade, este processo se concentra em auxiliar o desenvolvimento de estratégias e padrões para minimizar os efeitos da obsolescência. Para que este processo seja mais eficiente, ressalta-se a necessidade de manter uma base de conhecimentos sobre as tendências em termos de formatos, os padrões, as estratégias, as mídias de armazenamento, etc.

O processo **desenvolvimento de estratégias e padrões de preservação** (*develop preservation strategies and standards*) desenvolve e recomenda (*recommendations*) estratégias e padrões, além de avaliar riscos. Ele fornece

relatórios periódicos de análise de risco (*risk analysis reports*) para a entidade administração (*administration*) abordando riscos esperados, assim faz propostas (*proposals*) de atualizações, com base nas políticas operacionais, procedimentos e padrões. Por consequência, fornece informações sobre a evolução do sistema e atualização dos pacotes AIP para a entidade administração (*administration*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Este processo recebe relatórios (*reports*), alertas de requisitos (*requirement alerts*) e padrões emergentes (*emerging standards*) do processo de monitoramento da comunidade designada (*monitor designated community*); recebe relatórios (*reports*), padrões externos de dados (*external data standards*), resultados dos protótipos (*prototype results*) e alertas de tecnologias (*technology alerts*) do processo de monitoramento de tecnologia (*monitor technology*); recebe políticas operacionais (*operating policies*), procedimentos (*procedures*), padrões (*standards*), informações de desempenho (*performance info*), relatórios de inventário (*inventory reports*) e um resumo de comentários dos consumidores (*consumer comments*) da entidade de administração (*administration*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Com base nessas informações recebidas, este processo pode, por exemplo, identificar a necessidade de migração de algum formato ou adicionar informações de representação (*representation information*) e assim, atualizar AIP. Por fim, recebe ainda, questionamentos (*issues*) do processo de desenvolvimento de pacotes e planos de migração (*develop packaging designs & migration plans*), caso ocorra uma submissão com requisitos inesperados do processo, e consequentemente responder (*advice*) como se deve proceder com as novas exigências (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O desenvolvimento de estratégias e padrões está condicionado às informações recebidas de outros processos, bem como da entidade de administração. Estas informações são fundamentais para a tomada de decisão no processo de preservação digital. Desta forma, é possível decidir, fundamentado em uma base de conhecimento, quais são as estratégias e os padrões mais adequados.

O processo **desenvolvimento de pacotes e planos de migração** (*develop packaging designs & migration plans*) gera novos modelos de pacotes de informação e planos de migração detalhados e protótipos para implementar políticas e diretrizes por meio da entidade administração (*administration*). Embora os procedimentos

sejam executados na entidade plano de preservação será preciso uma aprovação prévia por parte da administração.

A migração da informação de conteúdo (*content information*) pode envolver alterações no conteúdo do objeto de dados (*data object*) e/ou na informação de representação (*representation information*). Tal atividade também fornecerá avisos (*customization advice*) sobre a aplicação destes projetos de pacotes de informação e planos de migração (*migration packages*) para as submissões e para os conteúdos específicos armazenados no OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Este processo recebe padrões aprovados (*approved standards*) e metas de migração (*migration goals*) da entidade administração (*administration*), dentre estes, incluem-se os padrões de formato, de metadados e de documentação. Posteriormente, aplica estes padrões aos requisitos de preservação e fornece projetos customizados de AIP's e SIP's (*AIP/SIP templates*) à entidade administração (*administration*), além fornecer avisos de adaptação e revisão destes projetos de AIP's e SIP's (*AIP/SIP review*). Caso este processo encontre submissões que não sejam contempladas pelos padrões e procedimentos vigentes, poderá enviar questionamentos para o processo desenvolvimento de estratégias e padrões de preservação (*develop preservation strategies and standards*) e receber orientações, incluindo novos padrões para auxiliar no cumprimento destes requisitos da submissão (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Este processo está voltada para à manutenção do acesso aos objetos de informação, para isto, recebe diversas informações vindas de outros processos, e também da entidade de administração. Desta forma, é possível identificar padrões com potencial obsoleto e assim, desenvolver novos protótipos.

As metas de migração que são recebidas pelo processo desenvolvimento de pacotes e planos de migração (*develop packaging designs & migration plans*) poderão acarretar transformações nos pacotes AIP's no que tange a sua informação de conteúdo com o objetivo de evitar a perda do acesso em razão da obsolescência tecnológica. Em resposta, às metas de migração pode ocorrer, por exemplo, o desenvolvimento de novos modelos para os AIP's (*AIP templates*) e de novos protótipos de *softwares* (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Para tal, este processo pode necessitar de conhecimentos vindos de outros processos da entidade plano de preservação (*preservation planning*). Desta forma, a

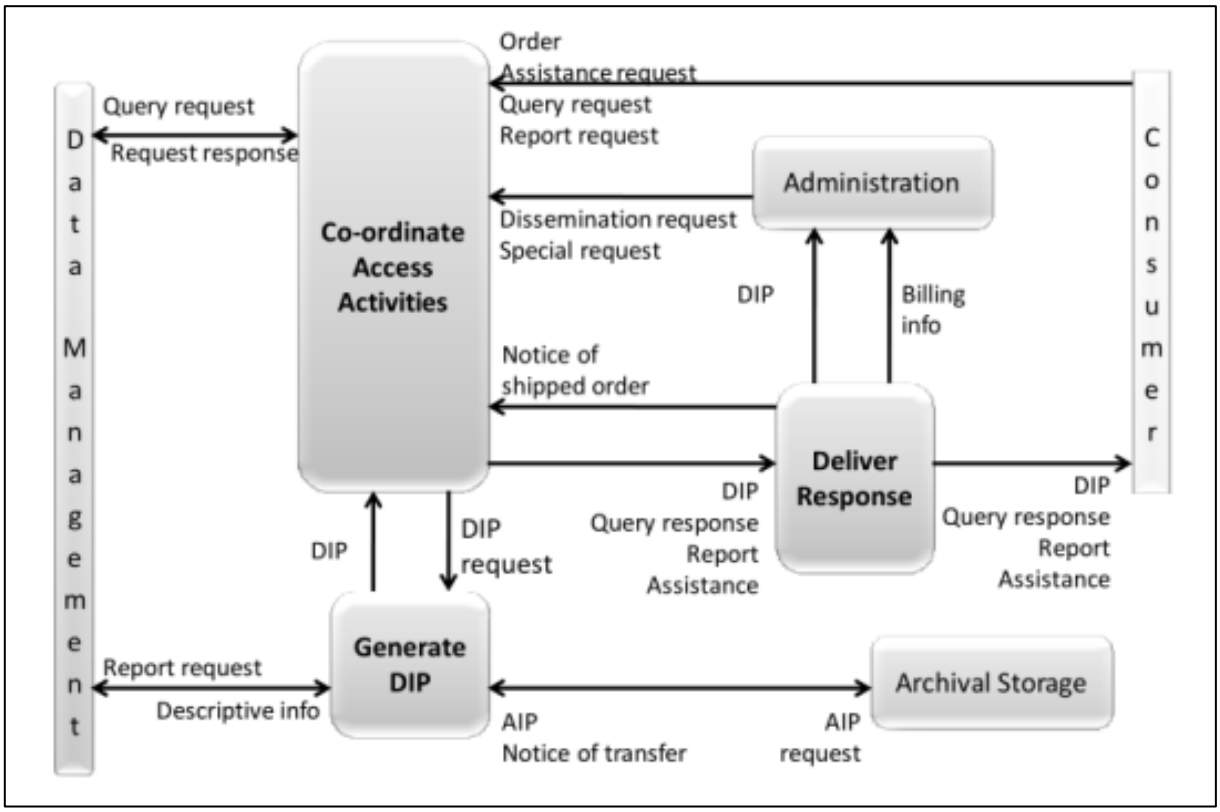
entidade denominada plano de preservação (*preservation planning*), irá desenvolver pacotes de migração, os quais serão fornecidos à entidade administração (*administration*) para que sejam validados, e após isto, executados. Após a validação destes planos, eles passam a integrar as políticas de preservação, o que reforça a necessidade de verificar sua pertinência e aplicabilidade ao acervo.

4.1.3.2.7 Acesso (*access*)

A entidade de acesso (*access*) é composta por três processos, que são: coordenar atividades de acesso (*co-ordinate access activities*), gerar DIP (*generate DIP*) e entregar resposta (*deliver response*). Esta entidade possui ainda, relações com outras entidades, tanto internas[40], quanto externas[41] ao ambiente OAIS. A seguir a “Figura 11 – Detalhamento da entidade de acesso” apresenta os diversos fluxos de informação da entidade.

[40] Administração (*administration*), gestão de dados (*data management*) e armazenamento arquivístico (*archival storage*).
[41] Consumidor (*consumer*).

Figura 11 – Detalhamento da entidade de acesso



Fonte: (CCSDS, 2012, p. 4-16).

O processo **coordenar atividades de acesso** (*co-ordinate access activities*) fornece uma ou mais interfaces para os consumidores (*consumer*) acessarem os conteúdos do OAIS. As solicitações realizadas pelo consumidor podem ser classificadas em três categorias: solicitações de consultas (*query request*), as quais são executadas pela entidade gestão de dados (*data management*), e que retornam resultados imediatos ao consumidor (*consumer*); solicitações de relatórios (*report request*), que podem exigir um número de consultas e produzir relatórios customizados ao consumidor (*consumer*); e os pedidos (*order*), os quais podem acessar as entidades gestão de dados (*data management*) e/ou armazenamento de arquivo (*archival storage*) para preparar o pacote DIP. Ressalta-se que um pedido pode ser uma ordem executada uma única vez, ou solicitações de entrega periódicas (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A entidade de acesso é meio pelo qual os consumidores solicitam pacotes de disseminação e relatórios ao OAIS. Desta mesma forma, esta entidade corrobora

para o processo de acesso/difusão da informação, já previsto nas sete funções arquivísticas preconizadas por Rousseau e Couture (1998).

No repositório OAIS, a entidade de administração (*administration*) efetua um processo de atualização da informação arquivada, e assim, envia solicitações de disseminação (*dissemination request*) para obter a informação descritiva de preservação (*preservation description information*) necessária de DIP's para os processo de atualização; além de outros tipos especiais (*special request*) que não sejam detalhados. Posteriormente, o processo coordenar atividades de acesso (*co-ordinate access activities*) verifica a disponibilidade dos recursos e as permissões de acesso para tais conteúdos, e assim, notificar o consumidor (*consumer*) de que o pedido foi aceito ou rejeitado. Em seguida, este processo transfere a solicitação para a entidade gestão de dados (*data management*) ou para o processo gerar DIP (*generate DIP*) para execução (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Além disso, o processo coordenar atividades de acesso (*co-ordinate access activities*) também fornece assistência para o consumidor (*consumer*), dentre elas, o acompanhamento do status da solicitação e outras atividades de apoio em resposta aos pedidos de assistência (*assistance*).

O processo **gerar DIP** (*generate DIP*) aceita uma solicitação de disseminação, recupera o AIP (*AIP request*) no armazenamento arquivístico (*archival storage*) e envia uma cópia para a área de armazenamento temporário para processamentos adicionais. Este processo também transmite uma solicitação de relatório à entidade gestão de dados (*data management*) a fim de obter informação descritiva (*descriptive info*) necessária ao pacote DIP. Caso algum processamento especial seja necessário, o processo gerar DIP (*generate DIP*) acessará objetos de dados armazenamentos na área temporária, e então, aplicará os processos solicitados. Os tipos de operações realizadas podem incluir: funções estatísticas, amostragem em dimensões temporais ou espaciais, conversões para diferentes tipos ou formatos de dados, filtragem de dados pessoais, entre outras. Após realizar as operações necessárias, este processo armazena o pacote DIP na área temporária e notifica o processo coordenar atividade de acesso (*co-ordinate access activities*) de que o DIP está pronto para entrega (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Além disso, observa-se que determinados pacotes AIP ou DIP podem ser mantidos em armazenamento temporário para pronta disponibilidade. Desta forma,

informações frequentemente solicitadas podem ser mantidas na área de armazenamento temporário a fim de otimizar os procedimentos de entrega ao consumidor.

O processo **entregar resposta** (*deliver response*) fornece os materiais solicitados (DIP's, relatórios e assistências) ao consumidor (*consumer*). Observa-se ainda, que é possível fazer entregas tanto *online*, quanto *off-line*.

No caso das entregas *online*, este processo irá aceitar uma resposta (*query response*/*DIP*/*report*/*assistance*) do processo coordenar atividades de acesso (*co-ordinate access activities*) e prepara para disseminação pelos meios de comunicação existentes. Desta forma, identifica-se o receptor, o meio de transmissão solicitado, e posteriormente, deposita-se a resposta (*query response*/*DIP*/*report*/*assistance*) na área temporária e acompanhar a transferência do material ao consumidor (*consumer*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Para entregas *off-line*, este processo recupera a resposta do processo coordenar atividades de acesso (*co-ordinate access activities*) prepara as listas de pacotes e outros registros, e em seguida remete a resposta (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Em ambos os casos, um aviso de solicitação enviada (*notice of shipped order*) será retornado ao processo coordenar atividades de acesso (*co-ordinate access activities*). Posteriormente, as informações de faturamento (*billing info*) serão submetidas à entidade administração (*administration*) para finalizar o processo de entrega (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A solicitação de materiais poderá ter custos relacionados, seja em um Arquivo público, seja em um sistema de negócio da iniciativa privada. Para um Arquivo público, os custos estarão relacionados às despesas que a instituição arcou, no que tange à mídias de armazenamento e processamentos adicionais específicos, para possibilitar o acesso ao consumidor. Na iniciativa privada, os custos relacionados ao repositório OAIS são definidos pelo custodiador do mesmo.

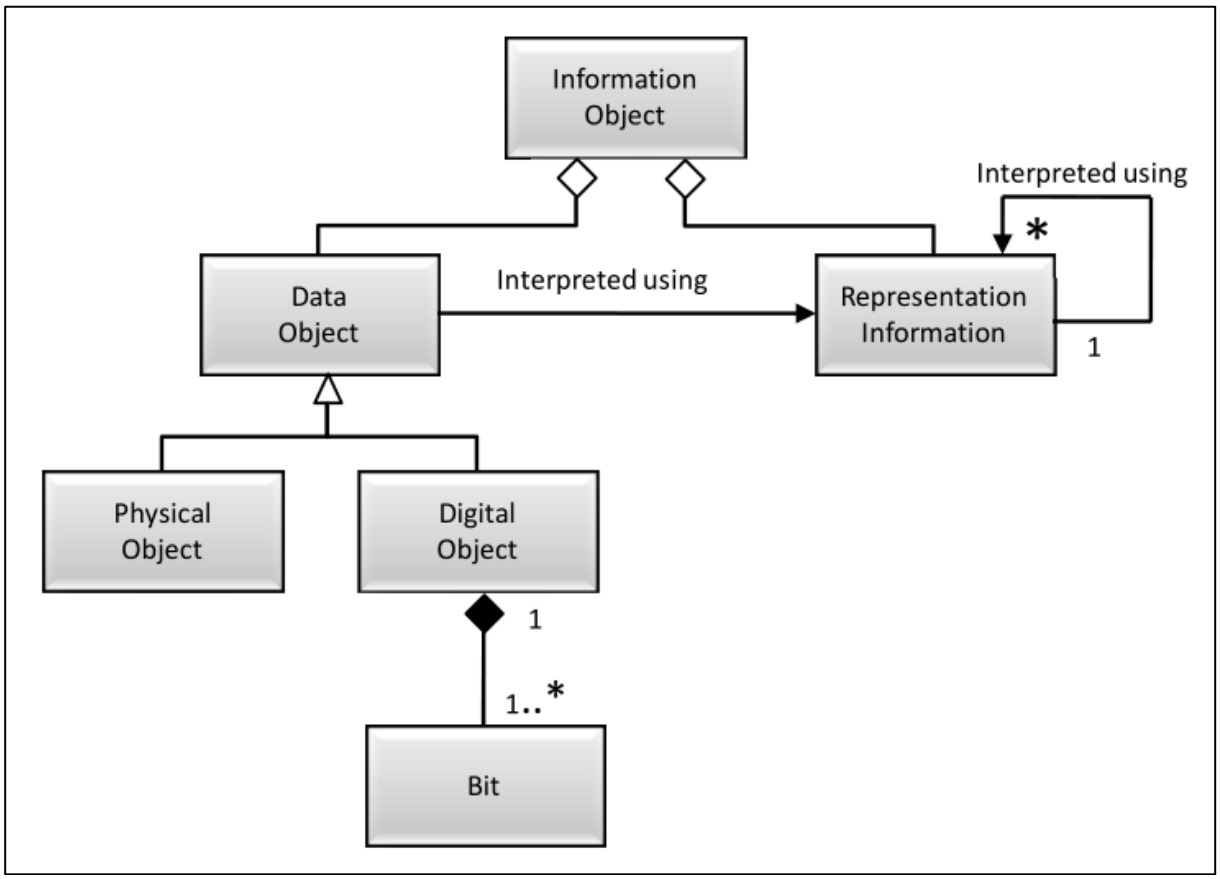
4.1.3.3 Modelo lógico das informações arquivadas

A seguir são apresentados os modelos lógicos dos tipos de informações arquivadas no ambiente OAIS.

4.1.3.3.1 Objeto de informação

Um conceito básico do OAIS é o conceito de objeto de informação (*information object*) entendido como a combinação entre objeto de dados (*data object*) e informação de representação (*representation information*). Deste modo, o objeto de informação (*information object*) é composto por um objeto de dados (*data object*) que poderá ser um objeto físico (*physical object*) ou objeto digital (*digital object*); e pela informação de representação (*representation information*) que permite a correta e completa interpretação dos dados na forma de informações significativas. A seguir, a "Figura 12 – Estrutura do objeto de informação" apresenta os componentes do objeto de informação.

Figura 12 – Estrutura do objeto de informação



Fonte: (CCSDS, 2012, p. 4-21).

4.1.3.3.2 Objeto de dados

O objeto de dados (*data object*) pode ser expresso como um objeto físico ou como um objeto digital, ambos associados a uma informação de representação (*representation information*) a qual lhe concebe sentido. Desta forma, após o objeto de dados ser interpretado com o auxílio da informação de representação, obtêm-se objeto de informação (*information object*).

Uma sequência de bits irá compor o objeto digital, já o objeto físico será composto por um objeto analógico, como uma rocha lunar. Assim, objeto físico e objeto digital irão compor o objeto de dados, e para ser preservado será necessário adicionar a informações de representação para garantir a sua correta interpretação. Esta informação de representação auxilia na interpretação da sequência de *bits*, bem como na compreensão do objeto físico, fornecendo análises e relatórios relacionados, que lhe conferem significado adicional. Desta forma, o objeto de dados juntamente com a informação de representação compõe o objeto de informação, o qual reúne as informações necessárias para preservar e compreender o significado do objeto físico e o objeto digital.

4.1.3.3.3 Informação de representação

A informação de representação (*representation information*) do objeto físico adiciona significado sobre fatores observáveis. De forma semelhante da informação de representação (*representation information*) que acompanha um objeto digital (*digital object*) ou uma sequência de *bits*.

No caso do objeto digital (*digital object*), a informação de representação (*representation information*) mapeia os *bits* em tipos de dados conhecidos, agrupando-os, e posteriormente, associa este mapeamento a significados de alto nível (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

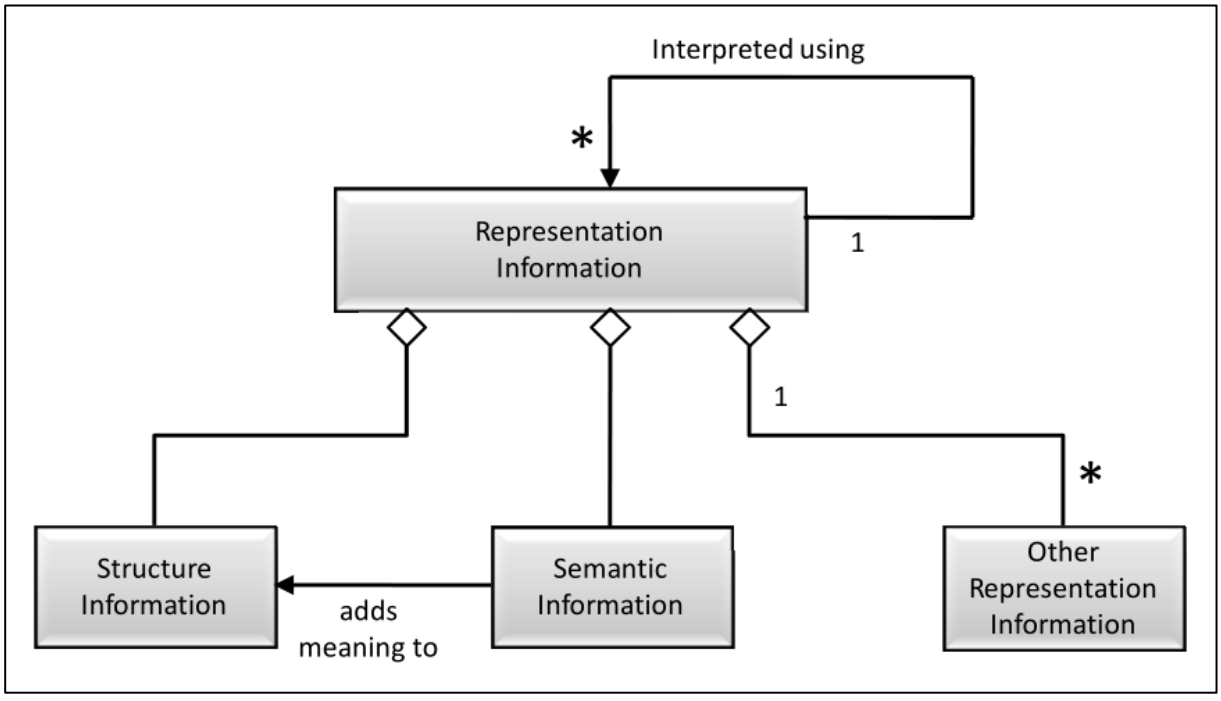
4.1.3.3.3.1 Tipos de informação de representação

O objeto digital é composto de uma ou mais sequências de *bits*, que poderá, juntamente com o objeto físico, compor o objeto de informação. O qual tem a finalidade de converter as sequências de *bits* em informações significativas.

Para isso, descrevem-se o formato ou conceitos de estrutura de dados que serão aplicados às sequências de *bits*, definidos como informação estrutural do objeto de informação de representação a qual é necessária para interpretar o objeto de dados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O conteúdo fornecido pela informação estrutural (*structure information*) raramente é suficiente à informação representação (*representation information*), sendo necessária uma informação adicional, então denominada de informação semântica (*semantic information*). Desta forma, a informação de representação (*representation information*) irá conter basicamente: informação estrutural e informação semântica; embora em algumas implementações esta distinção seja subjetiva, visto a possibilidade de haver diversos e complexos inter-relacionamentos entre informação estrutural e informação semântica; tais relacionamentos são incluídos em "outras informações de representação" (*other representation information*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir a "Figura 13 – Objeto de informação de representação" apresenta os componentes e subtipos da informação de representação.

Figura 13 – Objeto de informação de representação



Fonte: (CCSDS, 2012, p. 4-23).

Na “Figura 13 – Objeto de informação de representação” observa-se ainda, que a informação de representação (*representation information*) poderá conter referências a outras informações de representação (*other representation information*). Dentre estas, cita-se, por exemplo, *softwares*, algoritmos ou instruções, os quais sejam necessários à compreensão do conteúdo do objeto de dados.

As outras informações de representação (*other representation information*) são determinadas como parte da informação de representação (*representation information*), embora não sejam de ordem semântica ou estrutural (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Trata-se de um tipo de informação de representação “complementar”.

A informação de representação (*representation information*) é um componente do objeto de informação (*information object*) que poderá ter o seu próprio objeto de dados e suas próprias informações representação associadas (*other representation information*) visto na associação interpretado usando (*interpreted using*). Por consequência, o conjunto resultante de objetos pode ser denominado como parte de uma rede de representação (*representation network*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.3.3.3.2 Rede de representação (*representation network*)

A informação de representação (*representation information*)**,** a qual é um subtipo do objeto de informação poderá ser expressa em formatos físicos ou digitais. Caso seja digital, a informação de representação adicional (*other representation information*) será necessária para compreender a sequência de *bits* da informação de representação (*representation information*).

Observa-se que cada item da informação de representação (*representation information*) pode ter vários componentes, incluindo suas respectivas informações de representação. Desta forma, para preservar o significado de um objeto de informação é preciso preservar a sua respectiva informação de representação (*representation information*), a qual é facilitada quando for expressa em formatos que sejam facilmente compreensíveis. Ao se optar por descrição textual é preciso atentar para o uso de linguagens padronizadas de descrição suficientes para descrever a estrutura de dados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO

14721:2012). Além disso, à medida que a base de conhecimento da comunidade designada muda, será necessário manter a conformidade com a rede de representação (*representation network*).

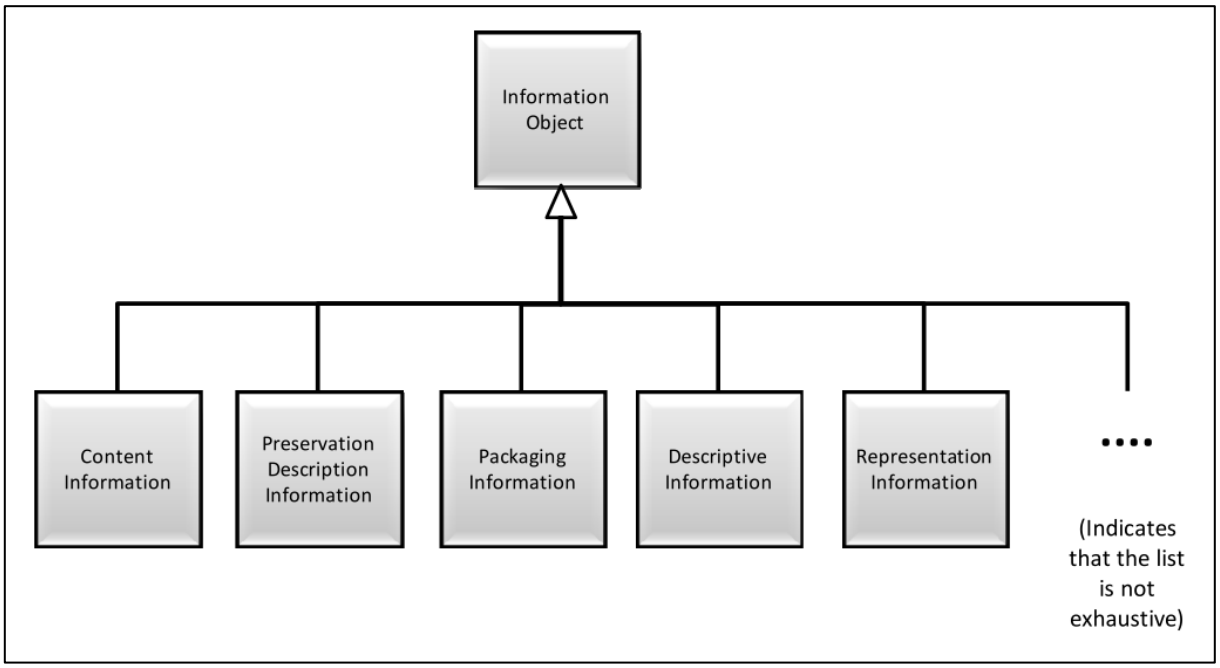
No OAIS, além da informação de representação (*representation information*), podem existem outros dois tipos especiais de informação que auxiliam na compreensão da informação de conteúdo: o *software* de apresentação e o *software* de acesso. O *software* de apresentação é capaz de exibir a informação de representação em formatos compreensíveis. Já o *software* de acesso irá apresentar parte ou todo o conteúdo de informação de um objeto de informação de modo compreensível para pessoas ou sistemas.

Observa-se ainda que, alguns arquivos poderão usar *softwares* de acesso para substituir toda a informação de representação, entretanto esta é uma prática complexa, visto a necessidade de um *software* que possua código aberto. Caso contrário, um *software* proprietário e/ou de código fechado pode ser um empecilho considerável a sua preservação, em virtude de uma série de restrições legais, além é claro, dos problemas ocasionados pela sua própria obsolescência tecnológica.

4.1.3.3.4 Taxonomia das classes de objetos de informação

A seguir são discutidos os diversos tipos de informação usados no OAIS, dentre estes: informação de conteúdo, informação de preservação, informação de empacotamento e informação descritiva. A seguir, a “Figura 14 – Taxonomia do objeto de informação” apresenta a estrutura conceitual do objeto de informação. Observa-se que a lista de subtipos de informação não é exaustiva, logo, diversos outros tipos de informação podem integrar o objeto de informação.

Figura 14 – Taxonomia do objeto de informação



Fonte: (CCSDS, 2012, p. 4-26).

4.1.3.3.4.1 Informação de conteúdo

A informação de conteúdo (*content information*) é o conjunto original de informações considerado como meta de preservação no OAIS. Entretanto, decidir o que é a informação de conteúdo (*content information*), é uma tarefa complexa, que poderá exigir negociações com o produtor (*producer*). A informação de conteúdo (*content information*) deve ser definida e separada em: objeto de dados, objeto de conteúdo e informação representação (*representation information*). Sendo esta, uma decisão de execução e de organização, relacionada à forma que os objetos de dados são admitidos e armazenados no OAIS.

Observa-se que cada um desses objetos de dados terá a sua própria informação de representação (*representation information*); além disso, poderá ter informação de representação adicional para descrever os objetos de dados relacionados. Logo, a informação de representação (*representation information*) para um objeto de dados de conteúdo digital (semântica ou sintática) é necessária para transformar os *bits* em informação de conteúdo (*content information*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Na prática, o OAIS necessita ter informação de representação (*representation information*) suficiente, associada aos *bits* do objeto de dados de conteúdo, para que assim, possa assegurar que os membros da comunidade designada podem entrar na rede de representação (*representation network*) com conhecimento suficiente para começar a interpretar as informações de representação (*representation information*) com precisão. Entretanto este é um risco significativo ao OAIS, especialmente para comunidades designadas especializadas, visto que os termos técnicos mais gerais podem ser de curta duração (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Logo, é preciso garantir a evolução natural da base de conhecimento da comunidade designada, para que assim não ocorra perda das informações de conteúdo (*content information*).

Frequentemente, as informações necessárias serão inseridas nos pacotes de *software* usados pela comunidade designada para apresentar e analisar as informações de conteúdo (*content information*). A razão para preservar o funcionamento do *software* de acesso surge a partir de um fator de conveniência. Isto porque mesmo com um conjunto completo de informação de representação (*representation information*), ressalta-se que o acesso à totalidade ou parte de um objeto de dados de conteúdo digital requer o uso do *software* de acesso (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O uso do *software* de acesso para substituir as redes de representação (*representation network*) é pertinente se for considerada a questão de minimizar os recursos necessários para processar dados e fornecer acesso aos usuários. Entretanto, a dependência por *softwares* específicos pode gerar grandes problemas para a preservação de longo prazo, em virtude de sua consequente obsolescência tecnológica. Logo, a sua preservação requer uma descrição completa e compreensível das informações de representação (*representation information*).

Conforme o modelo OAIS é importante decidir quais partes da informação de conteúdo (*content information*) formam o objeto de dados de conteúdo e quais partes formam a informação de representação (*representation information*). Este aspecto é fundamental para compreender claramente o que está sendo preservado. A identificação da informação do conteúdo (*content information*) junto aos seus objetos de informação de representação (*representation information*) pode ser abordada por meio desta sequência:

- Passo 1, identificar os *bits* da informação de conteúdo que compõem o objeto de dados;
- Passo 2, identificar um objeto de representação da informação que, de alguma forma, trate os *bits* do objeto de dados de conteúdo e converta-os em informação mais significativa;
- Passo 3, ao identificar o objeto de representação da informação (*representation information*), examinar o seu conteúdo para verificar se há objetos de representação informações adicionais. Caso existam, é preciso obter os objetos de informação representação necessários. Este processo deverá ser repetido até que não sejam mais encontrados objetos de representação de informação adicionais;
- Em seguida, para cada objeto de informação de representação (*representation information*) abordado no passo 3, deve-se identificar um objeto de informação de representação (*representation information*) necessário e repetir os passos 3 e 4 até que não sejam identificados novos objetos de informação de representação (*representation information*);
- Passo 5, as informações de conteúdo (*content information*) consistem no objeto de dados de conteúdo e em cada um dos objetos de informação de representação identificados nos passos 2 e 4.

4.1.3.3.4.2 Informação de preservação

Além da informação de conteúdo (*content information*), a informação arquivada precisa de informações adicionais para sua compreensão durante longos períodos. Logo, este conjunto específico de objetos de informação é chamado de informação descritiva de preservação (*preservation description information*).

A informação descritiva de preservação (*preservation description information*) deve incluir todas as informações necessárias para preservar adequadamente a informação de conteúdo (*content information*) a qual está associado. Sua função é, especificamente, descrever os estados passados e presentes da informação de conteúdo, garantir sua identificação única, e que tenha sido alterada de forma desconhecida (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Conforme o modelo OAIS, a informação descritiva de preservação (*preservation description information*) possui quatro categorias assim definidas:

a) **Informação de referência**: identifica, e caso necessário, descreve os mecanismos utilizados para identificar as informações de conteúdo. Também fornece identificadores para sistemas externos referenciarem as informações de conteúdo;
b) **Informações de contexto**: documenta as relações das informações de conteúdo com o seu ambiente. Isto inclui o motivo de sua produção e a forma como se relaciona com outros objetos informações de conteúdo existentes em outro local;
c) **Informações de proveniência**: documenta o histórico da informação de conteúdo, relata sua fonte/origem e a sua cadeia de custódia. Desta forma, fornece trilhas de auditoria contendo quaisquer alterações proferidas desde a origem, demonstrando assim, confiabilidade aos usuários;
d) **Informação de fixidez**: fornece verificações de integridade dos dados ou chaves de validação/verificação usadas para garantir que o objeto de informação de conteúdo não tenha sido alterado de forma não documentada. Além disso, pode incluir esquemas de detecção de erro para os objetos de conteúdo. Entretanto, a informação de fixidez não inclui mecanismos para preservação da integridade, mas poderá especificar os requisitos mínimos a serem fornecidos pelos serviços de apoio.

Em resumo, o OAIS precisa definir com precisão, a informação de conteúdo, para então assegurar que possui a informação descritiva de preservação (*preservation description information*) necessária para preservar a informação de conteúdo. Após definir a as informações de conteúdo será possível avaliar as informações descritivas de preservação (*preservation description information*).

4.1.3.3.4.3 Informação de empacotamento

A informação de empacotamento (*information packaging*) relaciona logicamente os componentes de um pacote em uma entidade identificável ou em uma mídia específicos. Sua preservação no OAIS é facultativa.

Observa-se que as informações de empacotamento não contribuem para a informação de conteúdo ou para a informação descritiva de preservação (*preservation description information*), logo não há necessidade de preservá-la. Entretanto, há casos em que será necessário, reproduzir a submissão original com exatidão, logo, a informação de conteúdo precisa incluir todos os *bits* previamente submetidos (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O OAIS também deve manter a informação descritiva de preservação (*preservation description information*) ou a informação de conteúdo nas conversões de estruturas de nomes dos diretório/arquivo de dados. Estas estruturas possuem maior tendência para serem utilizadas como informação de empacotamento (*information packaging*). Ressalta-se que a informação de empacotamento (*information packaging*) não é preservada por todas as migrações digitais. Qualquer informação salva em estruturas de nomes de arquivos/diretórios poderá ser perdida quando a informação de empacotamento (*information packaging*) é alterada (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Logo, a informação de empacotamento (*information packaging*) deve ser considerada na migração de informações para novas mídias de armazenamento.

4.1.3.3.4.4 Informação descritiva

A informação descritiva (*descriptive information*) é uma especialização do objeto de informação que fornece recursos adequados para permitir que os consumidores localizem informações de interesse potencial, posteriormente analisem essas informações, e por fim solicitem a informação desejada; além de conter dados que são utilizados como entradas (instrumentos chaves) para documentos ou aplicações.

A informação descritiva (*descriptive information*) é geralmente derivada da informação do conteúdo (*content information*) e da informação descritiva de preservação (*preservation description information*). Ela pode ser vista como um índice que permite acessar o pacote de informação associado de forma mais eficiente, com os instrumentos de acesso. Estes instrumentos são documentos ou aplicações que podem ser usados para localizar, analisar, recuperar ou solicitar informações armazenadas no OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.3.4 Modelo lógico de informação no OAIS

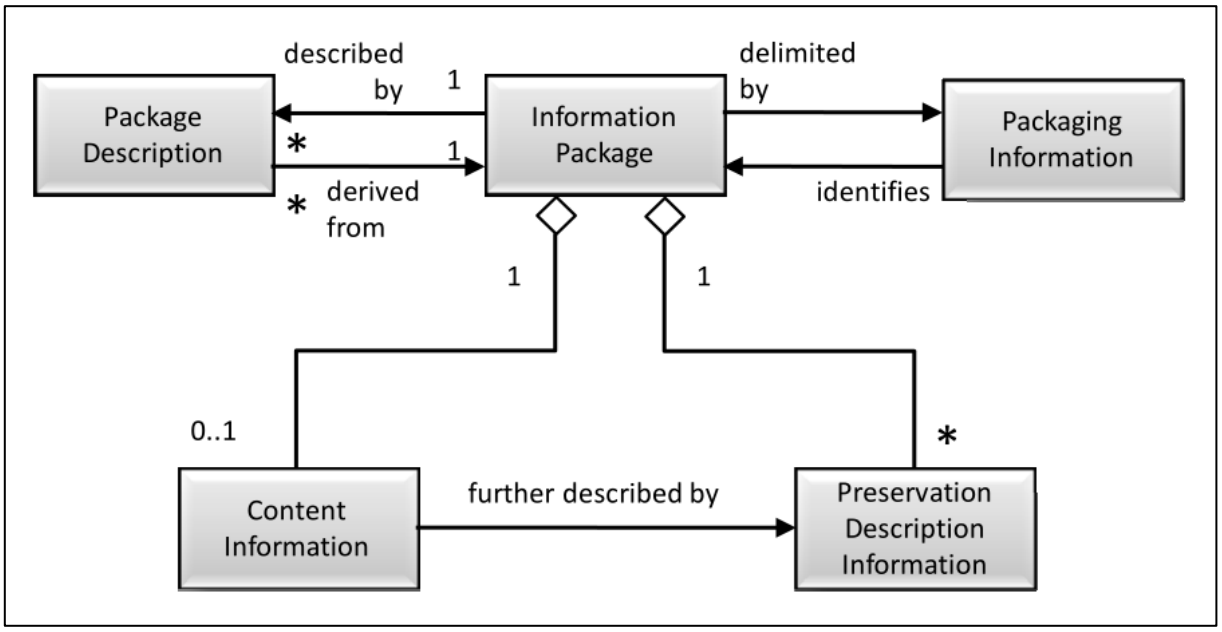
A seguir são apresentados os modelos de estruturas conceituais de informação para realizar a preservação de longo prazo, e garantir o acesso à informação pela comunidade designada.

4.1.3.4.1 Pacote de informação

O pacote de informação é a estrutura conceitual utilizada para apoiar o processo de preservação em longo prazo. Ele é um recipiente que contém dois tipos de objetos de informação: informações de conteúdo e informação descritiva de preservação (PDI). Tal pacote pode ser associado com outros dois tipos de objetos de informação: informação de empacotamento e descrição do pacote.

Observa-se que existem vários tipos de pacotes de informação que são usados na preservação dos documentos, tais pacotes pode ser usados para: estruturar e armazenar os conteúdos do OAIS; transportar a informação necessária vinda do produtor até o OAIS; ou para transportar a solicitação de informações entre o OAIS e consumidores (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir a “Figura 15 – Conteúdos do pacote de informação” apresenta a relação entre estes elementos.

Figura 15 – Conteúdos do pacote de informação



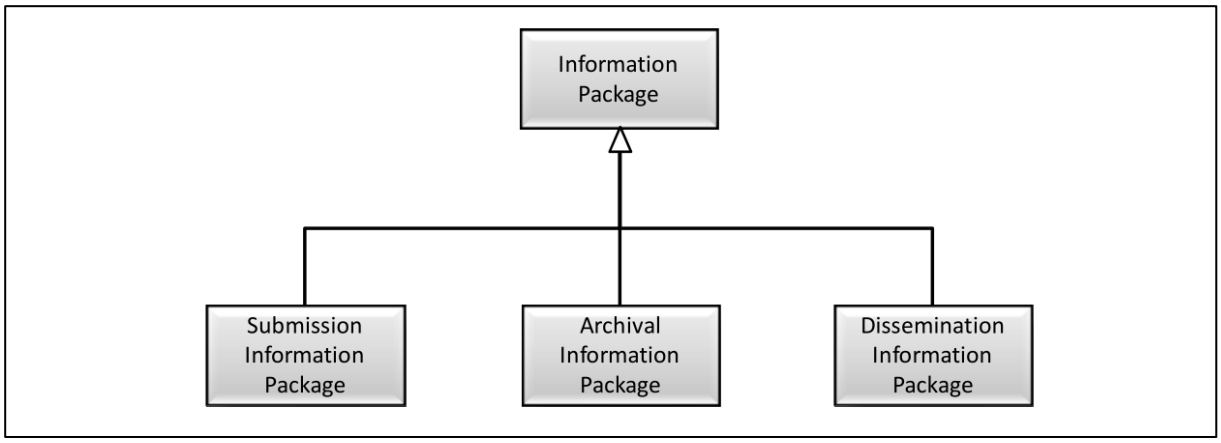
Fonte: (CCSDS, 2012, p. 4-34).

Observa-se que um pacote de informação poderá conter “zero” ou “um” objeto de informação de conteúdo; “zero” ou “vários” objetos de informação descritiva de preservação; e está associado exatamente a “uma” unidade de empacotamento que o identifica e delimita. Além disso, o pacote de informação também está associado a “zero” ou “várias” descrições de pacote que descrevem o objeto de conteúdo a fim de otimizar o acesso.

4.1.3.4.2 Tipos de pacote de informação

No modelo OAIS existem três tipos de pacote de informação: SIP, AIP e DIP. Estes tipos são variações de um mesmo pacote de informação, conforme apresentado na “Figura 16 – Variações do pacote de informação”.

Figura 16 – Variações do pacote de informação



Fonte: (CCSDS, 2012, p. 4-35).

O produtor envia um pacote de informação à entidade de admissão, este pacote é denominado SIP; posteriormente, o mesmo pacote é arquivado no repositório e assim transformado em pacote AIP; e por fim, após solicitação do consumidor, uma versão é entregue pela entidade de acesso, denominada pacote DIP.

A maioria dos SIP's terá alguma informação de conteúdo e algumas informações descritivas de preservação, mesmo assim, vários SIP's poderão ser necessários para fornecer um conjunto completo de informações de conteúdo e informação descritiva de preservação associada. As informações de conteúdo e as informações descritivas de preservação possuem informação de representação associada; e observa-se ainda, que no caso de existem vários SIP's que usem a mesma informação de representação, é provável que tais informações de representação sejam fornecidas uma única vez ao OAIS, caso seja aplicada a diversos SIP's. Em outro caso, a informação descritiva de preservação será fornecida em um SIP separado sem informação de conteúdo. Já a informação de empacotamento sempre estará presente de alguma forma (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Salienta-se que no ambiente OAIS, um ou mais pacotes SIP's são transformados em um ou mais pacotes AIP's para preservação. O pacote AIP possui um conjunto completo de informação descritiva de preservação para as informações

do conteúdo associadas; e esse pacote ainda pode conter um conjunto de outros AIP's (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

As informações de empacotamento de um AIP seguirão a conformidade com as normas internas OAIS, e podem variar, conforme essa gestão. Logo, observa-se que caso a informação descritiva associada a uma AIP seja abrangente, os consumidores podem encontrar e encomendar as informações de conteúdo de interesse; o que otimiza o processo de busca e recuperação da informação.

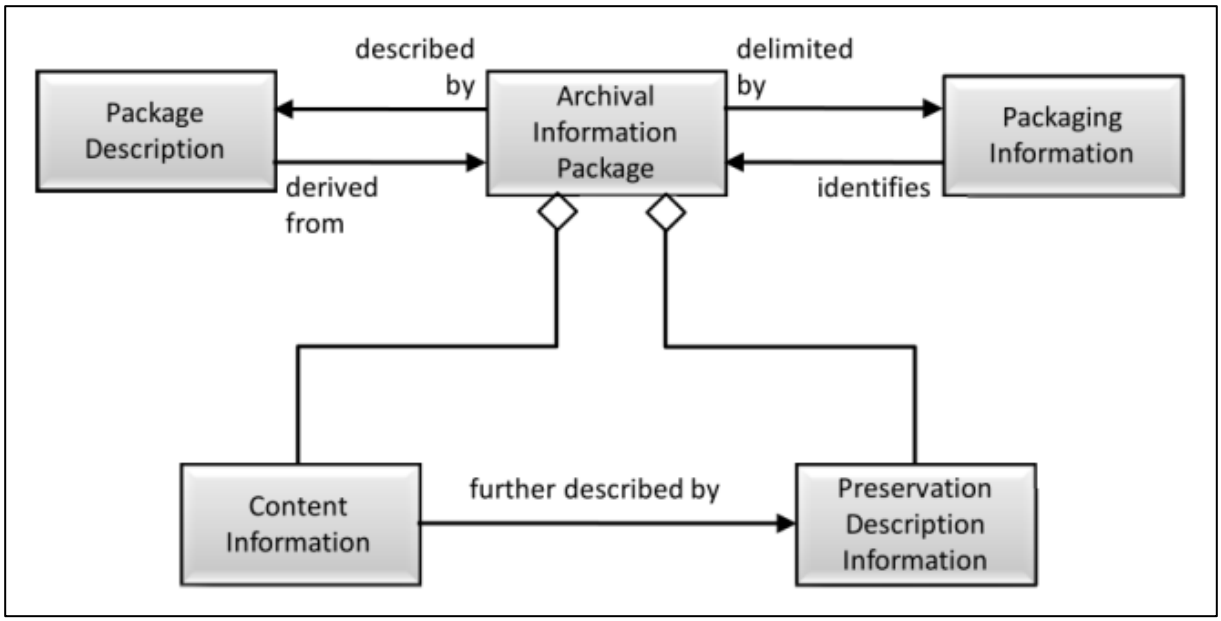
Em resposta a uma solicitação, o OAIS irá fornecer uma parte ou até mesmo o pacote AIP completo ao consumidor, que será entregue na forma de um pacote DIP. O pacote DIP pode incluir coleções de AIP, e conter informação descritiva de preservação, seja ela completa ou não. Ressalta-se que as informações de empacotamento estarão presentes, de alguma forma, para que o consumidor possa distinguir claramente a informação solicitada. As informações de empacotamento podem assumir várias formas, dependendo da mídia de divulgação e das exigências dos consumidores.

Já a informação descritiva associada ao DIP, poderá ser fornecida em qualquer momento da transferência do DIP; sua finalidade é fornecer ao consumidor informações suficientes para reconhecer o DIP entre possíveis pacotes semelhantes, por exemplo, uma descrição textual integrando a informação de empacotamento (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.3.4.3 Pacote de Informação de Arquivamento

A definição do pacote AIP fornece um conjunto de informações contendo as qualidades necessárias à preservação em longo prazo de um determinado objeto de informações. O pacote AIP, é por si só, um objeto de informação, o qual é tido como um recipiente de outros objetos de informação. No interior do AIP encontra-se o objeto de informação-alvo, denominado, informação de conteúdo (*content information*). Tal esquematização pode ser observada na "Figura 17 – Pacote de Informação de Arquivamento (AIP)".

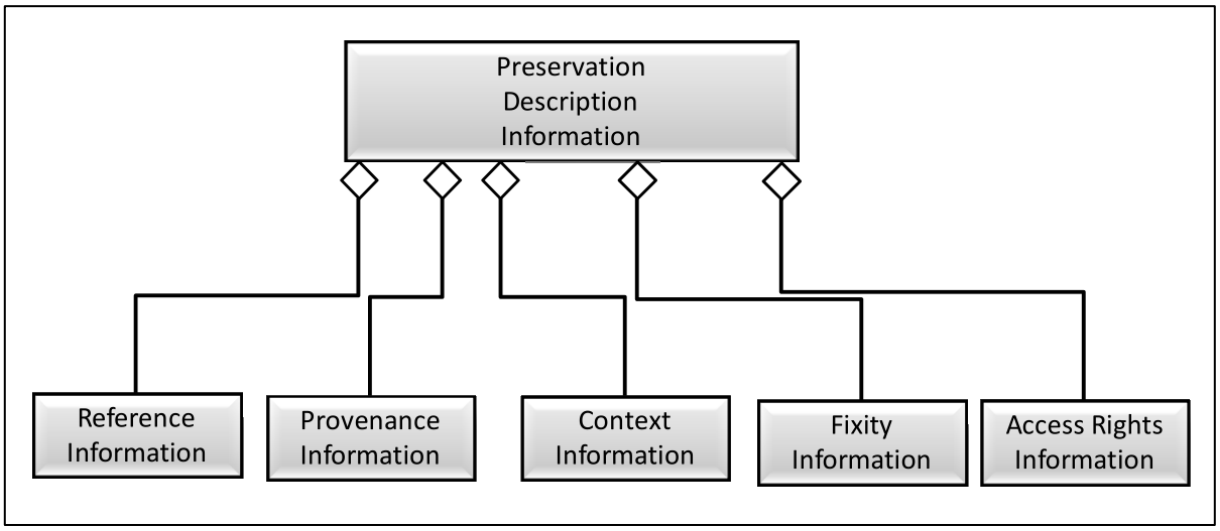
Figura 17 – Pacote de Informação de Arquivamento (AIP)



Fonte: (CCSDS, 2012, p. 4-37).

Dentro deste pacote AIP encontra-se a informação descritiva de preservação (*preservation description information*) que contém informações adicionais, as quais são necessárias para tornar as informações de conteúdo significativas no longo prazo. Observa-se que os requisitos da informação descritiva de preservação de um AIP são obrigatórios, de modo que todas as suas classes de informações devem estar presentes, diferentemente dos demais pacotes de informação, onde a informação descritiva de preservação não é obrigatória (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir, a “Figura 18 – Informação descritiva de preservação” apresenta os seus subtipos de informação.

Figura 18 – Informação descritiva de preservação



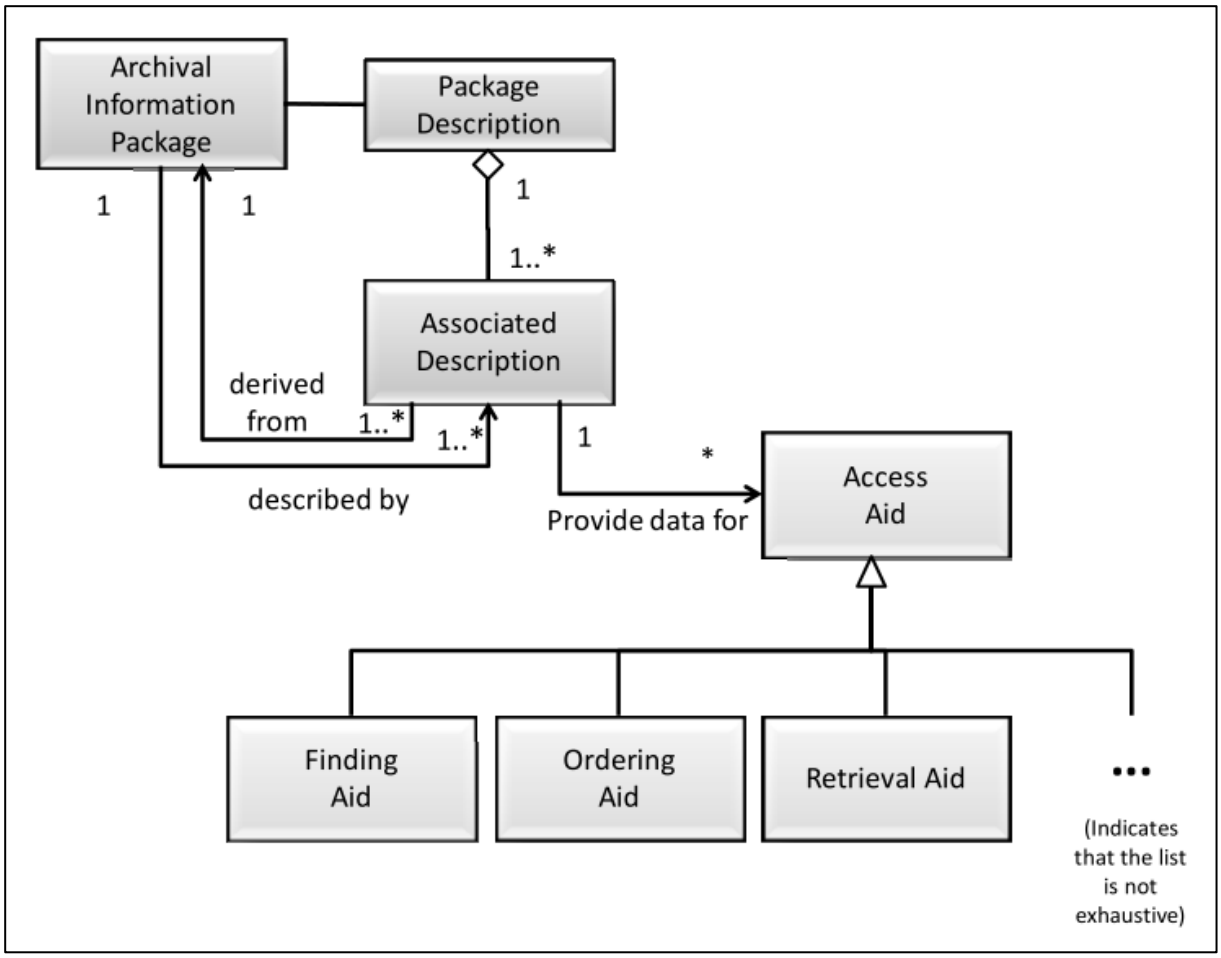
Fonte: (CCSDS, 2012, p. 4-38).

O pacote AIP é delimitado e identificado pelas informações de empacotamento, as quais poderão estar presentes como uma estrutura na mídia que contém o AIP ou contida na entidade armazenamento arquivístico. Ressalta-se que as funções internas de delimitação e identificação devem ser bem definidas pelo OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Cada pacote AIP está associado a uma estruturada de informações descritivas chamada de descrição do pacote, que permite ao consumidor localizar e analisar as informações de interesse e solicitar as informações desejadas. A informação necessária para um instrumento de acesso é chamado de descrição associada.

Observa-se que uma descrição de pacote pode conter várias descrições associadas, isto depende da quantidade dos diferentes instrumentos de acesso utilizados para localizar, visualizar, recuperar ou solicitar a informação de conteúdo associado e a informação descritiva de preservação (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Esta esquematização é apresentada a seguir na “Figura 19 – Descrição do pacote”.

Figura 19 – Descrição do pacote



Fonte: (CCSDS, 2012, p. 4-39).

Conforme expresso na “Figura 19 – Descrição do pacote” a descrição do pacote (*package description*) deve conter uma descrição associada (*associated description*) a qual fornece dados para um instrumento de recuperação (*retrieval aid*). Desta forma, os usuários autorizados recuperem as informações de conteúdo e a informação descritiva de preservação que são especificadas pela descrição do pacote (*package description*).

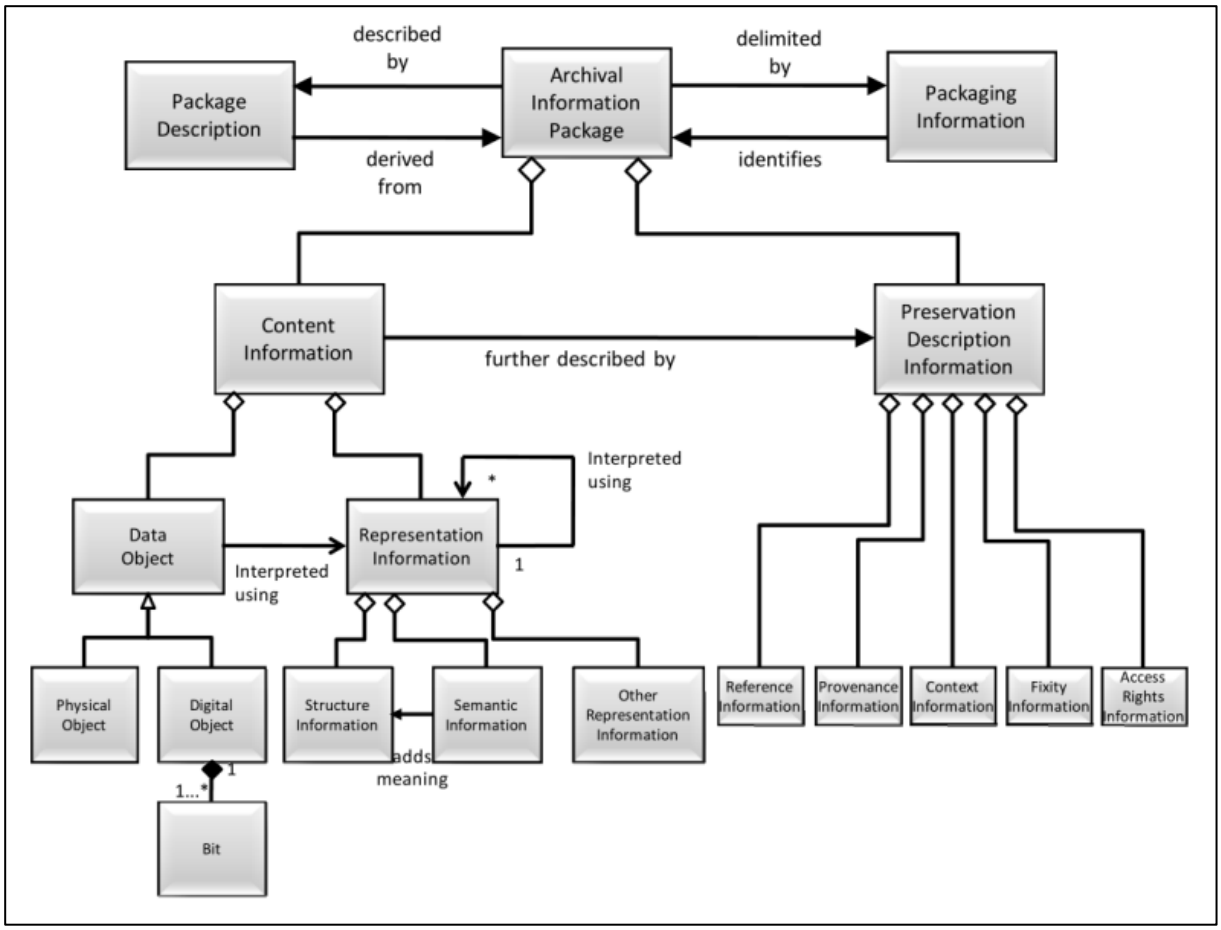
Este instrumento de recuperação geralmente faz parte da entidade armazenamento arquivístico. Ele traduz o identificador único do AIP, então atribuído pelo OAIS, a fim de identificar a AIP em um subconjunto de operações e nomes de arquivos de dados, então necessários para recuperar o AIP na entidade armazenamento arquivístico. Após isto, retorna as informações de conteúdo e as

informações descritivas de preservação do AIP solicitado (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A descrição do pacote (*package description*) também pode conter séries de descrições associadas (*associated description*), sendo que cada uma irá conter dados para um ou mais instrumentos de acesso (*access aid*). Há ainda outros dois subtipos adicionais de acesso que são os instrumentos de busca (*finding aid*) e os instrumentos de solicitações (*ordering aid*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Os instrumentos de busca auxiliam o consumidor a localizar a informação de interesse. Já os instrumentos de solicitação auxiliam o consumidor a descobrir o custo de solicitar um pacote AIP de interesse, além disso, o consumidor ainda pode especificar as transformações proferidas sobre o AIP antes da disseminação via pacote DIP.

A descrição do pacote não é requisito à preservação de longo da informação de conteúdo, no entanto é necessária para fornecer visibilidade e acesso aos conteúdos do OAIS. O conteúdo da descrição do pacote é altamente dependente da estrutura da informação de conteúdo e da informação descritiva de preservação que ele descreve (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir, a “Figura 20 – Pacote AIP (visão detalhada)” apresenta o pacote AIP, expandindo elementos abordados anteriormente, como a sua informação de conteúdo e a sua informação descritiva de preservação.

Figura 20 – Pacote AIP (visão detalhada)

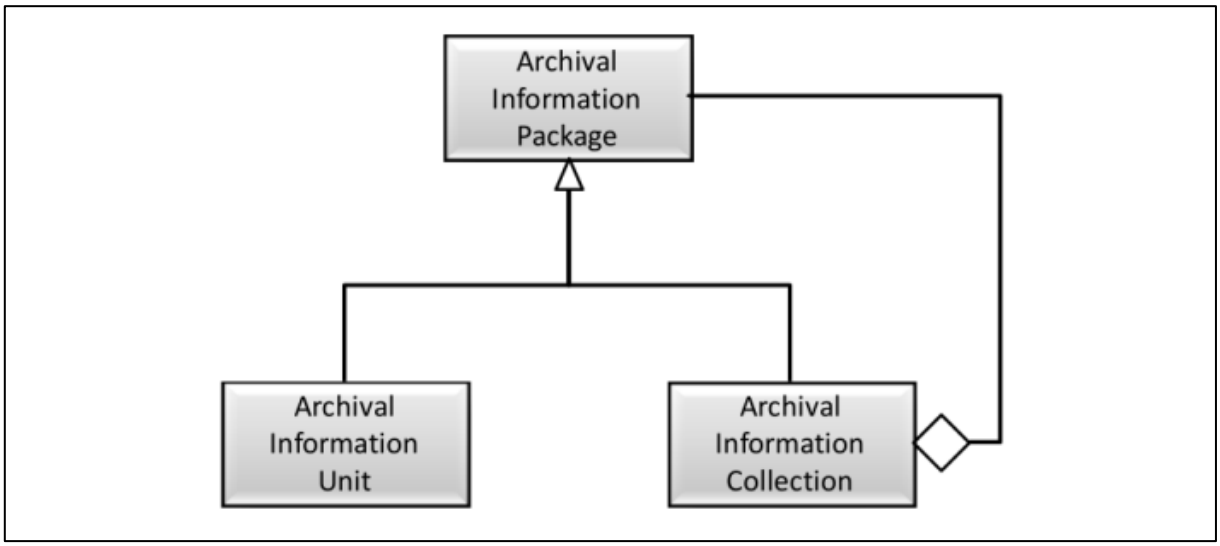


Fonte: (CCSDS, 2012, p. 4-40).

4.1.3.4.4 Especialização do AIP e descrição de pacote

O pacote AIP possui duas especializações: a unidade de arquivamento de informação (AIU) e a coleção de arquivamento de informações (AIC), estes subtipos do AIP contém estruturas que permitam a preservação e o acesso em longo prazo aos consumidores. Tal esquematização é representada a seguir na “Figura 21 – Especialização do AIP”.

Figura 21 – Especialização do AIP



Fonte: (CCSDS, 2012, p. 4-41).

A unidade de arquivamento de informação (AIU) é utilizada para preservar um único objeto de informação de informação de conteúdo, o qual não está decomposto em outros AIP's. Já a coleção de arquivamento de informação (AIC) organiza um conjunto de AIP's (AIU's e outros AIC's) em uma hierarquia temática, que proporcione acesso flexível e eficiente aos consumidores.

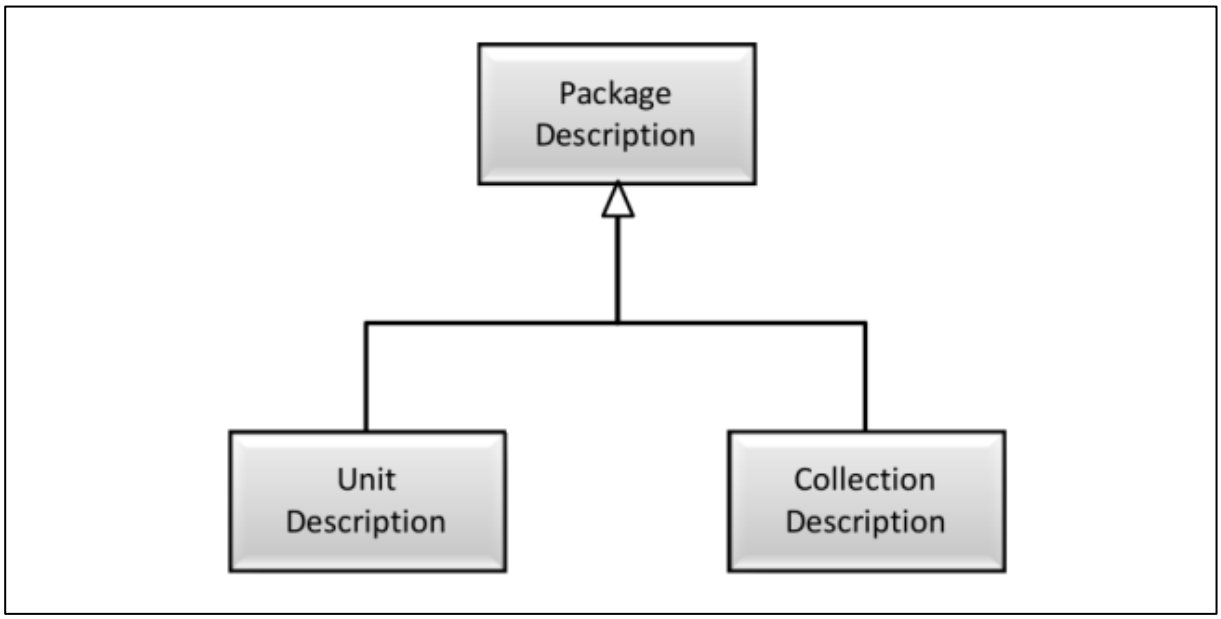
Todos os AIP's organizados por um AIC estão contidos nas informações de conteúdo do AIC. A diferença básica entre AIU's e AIC's está na complexidade da sua informação de conteúdo e de suas respectivas descrições de pacotes e informações de empacotamento associadas. O modelo OAIS considera as diferenças, entre AIU e AIC, referentes à informação de conteúdo e as funcionalidades de empacotamento e descrição associadas, as quais devem ser adequadamente complexas e interligadas para justificar a definição de classes separadas (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Com relação à preservação da informação, há uma clara distinção entre AIU e AIC. Observa-se que a AIU é composta por um único objeto informações e o conteúdo, o qual é descrito por exatamente um conjunto de informação descritiva de preservação. Já a informação de conteúdo de uma AIC é composta por uma coleção de outros AIC's e AIU's, e cada um possui a sua própria informação descritiva de preservação. Além disso, a AIC tem a sua própria informação descritiva de

preservação que descreve os critérios e os processos da coleção (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Como consequência da especialização do AIP têm-se duas descrições do pacote: a descrição da unidade e a descrição da coleção. Assim, as descrições do pacote podem ser observadas a seguir na “Figura 22 – Especialização da descrição de pacote”.

Figura 22 – Especialização da descrição de pacote



Fonte: (CCSDS, 2012, p. 4-42).

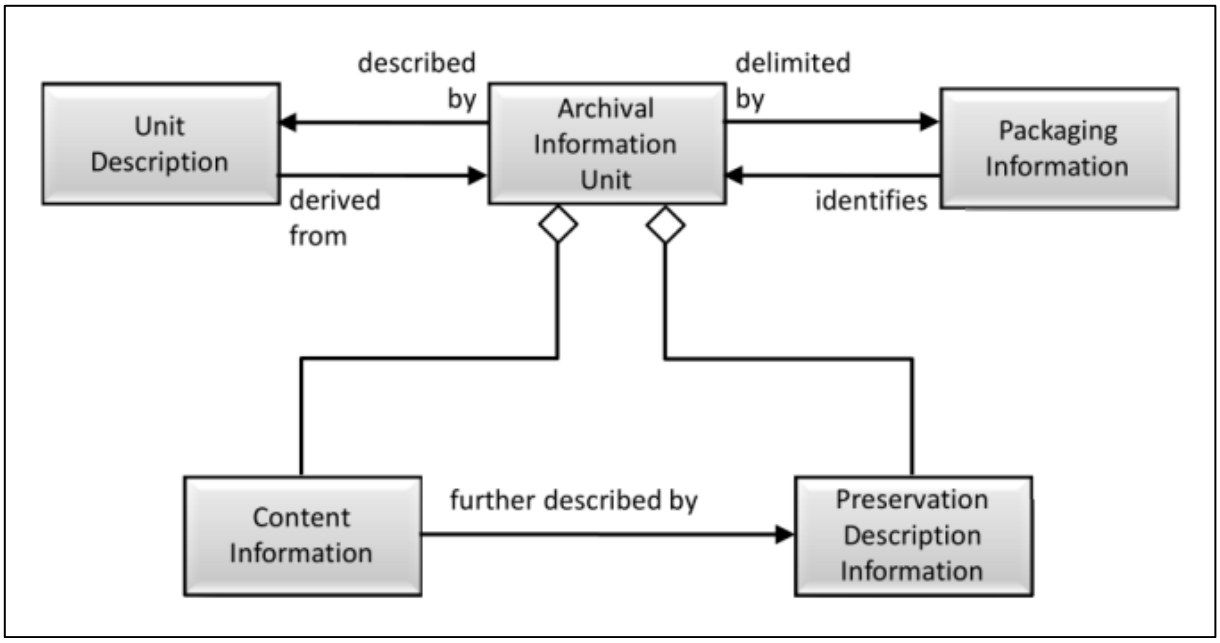
4.1.3.4.5 Unidade de informação de arquivamento

Uma única AIU contém exatamente um objeto informações de conteúdo (que pode consistir em múltiplos arquivos de dados) e exatamente um conjunto de PDI. Salienta-se que o OAIS é livre de decidir como construir a AIU, além disso, um AIU não precisa, necessariamente, ser um único arquivo de dados.

Quando um objeto de informação é admitido no OAIS, uma descrição de unidade (*unit description*, subtipo de descrição de pacote) é criada para extrair informações a partir da informação de conteúdo (*content information*), da PDI (*preservation description information*) e com adição de informações específicas

(ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir a “Figura 23 – Unidade de informação de arquivamento” esquematiza as relações da AIU.

Figura 23 – Unidade de informação de arquivamento

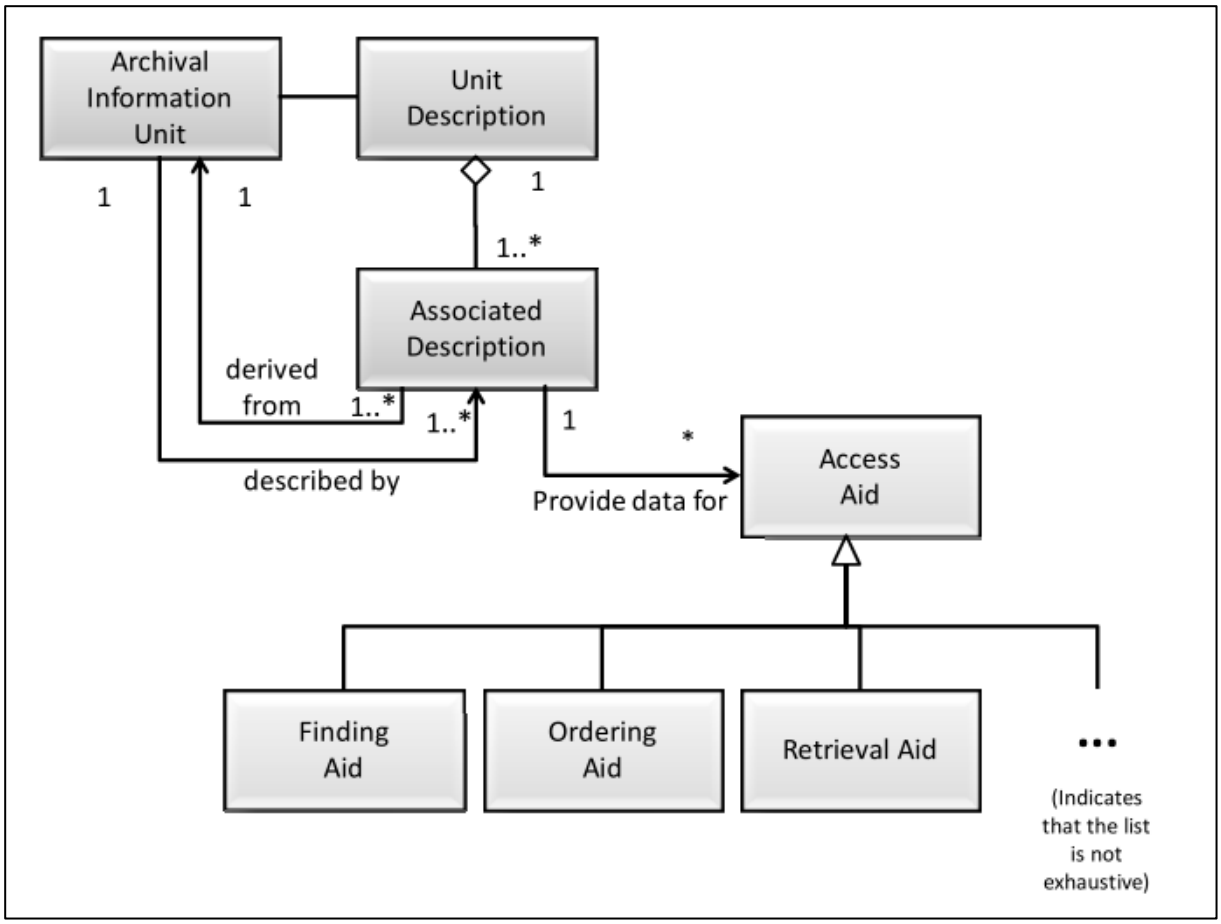


Fonte: (CCSDS, 2012, p. 4-43).

4.1.3.4.6 Descrição de unidade

A descrição de unidade é uma especialização da descrição do pacote que conterá um conjunto de descrições associadas, assim, cada uma irá descrever as informações de conteúdo da AIU do ponto de vista de um único instrumento de acesso (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir, o conteúdo de descrição da unidade é apresentado na “Figura 24 – Descrição da unidade”.

Figura 24 – Descrição da unidade



Fonte: (CCSDS, 2012, p. 4-44).

Todas as descrições de unidade deve fornecer uma descrição associada para um instrumento de recuperação o qual permitirá que os usuários autorizados recuperem AIU descrita pela descrição de unidade da entidade armazenamento arquivístico. Esta descrição inclui o identificador único que a entidade armazenamento arquivístico (*archival storage*) atribui ao AIP durante o processo de admissão (*ingest*) (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Uma única AIU pode ter diversas descrições associadas que descrevem as informações de conteúdo utilizando diferentes tecnologias. À medida que surgem novas tecnologias de extração de descrição e de apresentação, o OAIS pode querer atualizar a descrição de unidade associada a cada uma de suas AIU's, criando assim, novas descrições associadas que utilizam essas tecnologias (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Destaca-se que um tipo importante

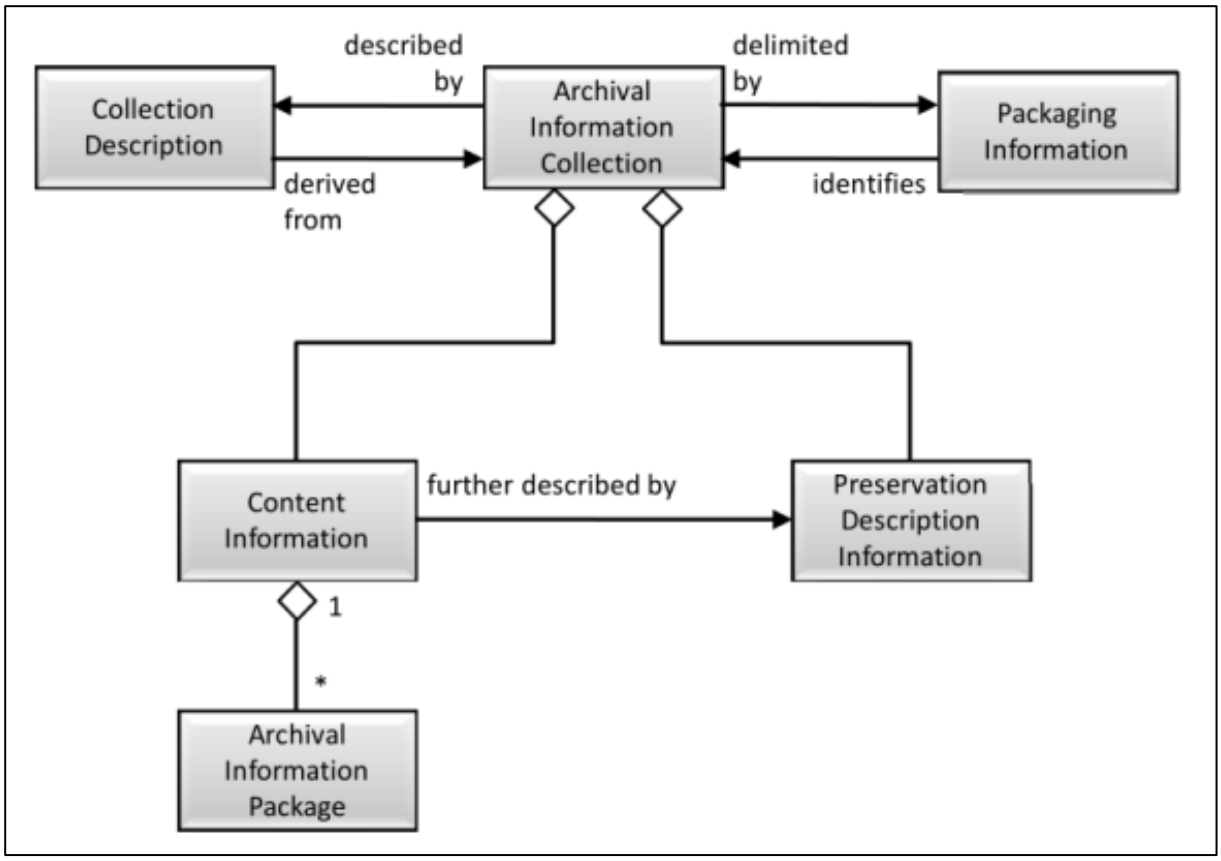
de instrumento de acesso (*access aid*) para estes conteúdos é instrumento de busca (*finding aid*), um aplicativo que auxilia o consumidor na localização de informações de interesse; aumentando o processo de precisão da informação.

Outra categoria importante de descrições associadas fornece dados aos instrumentos de solicitação, de modo que o consumidor conheça os custos e solicite as AIU's de interesse (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Os instrumentos de solicitação também permitem que os usuários especifiquem as transformações a serem aplicadas às AIU's antes da disseminação. Ressalta-se que essas transformações podem se aplicar ao objeto de dados, e até mesmo a envolver a PDI da AIU, antes da disseminação.

4.1.3.4.7 Coleções de informação de arquivamento

A informação de conteúdo de uma AIC é composta por AIP completos, cada um contendo a sua própria informação de conteúdo, PDI, informação de empacotamento associada e descrição do pacote. Estes AIP's são agregados em AIC's considerando os critérios definidos pelo arquivista. Geralmente as AIC's são baseadas no AIU's com temas ou origens comuns e um conjunto comum de descrições associados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir a "Figura 25 – Coleção de informação de arquivamento" apresenta a estrutura de uma AIC.

Figura 25 – Coleção de arquivamento da informação

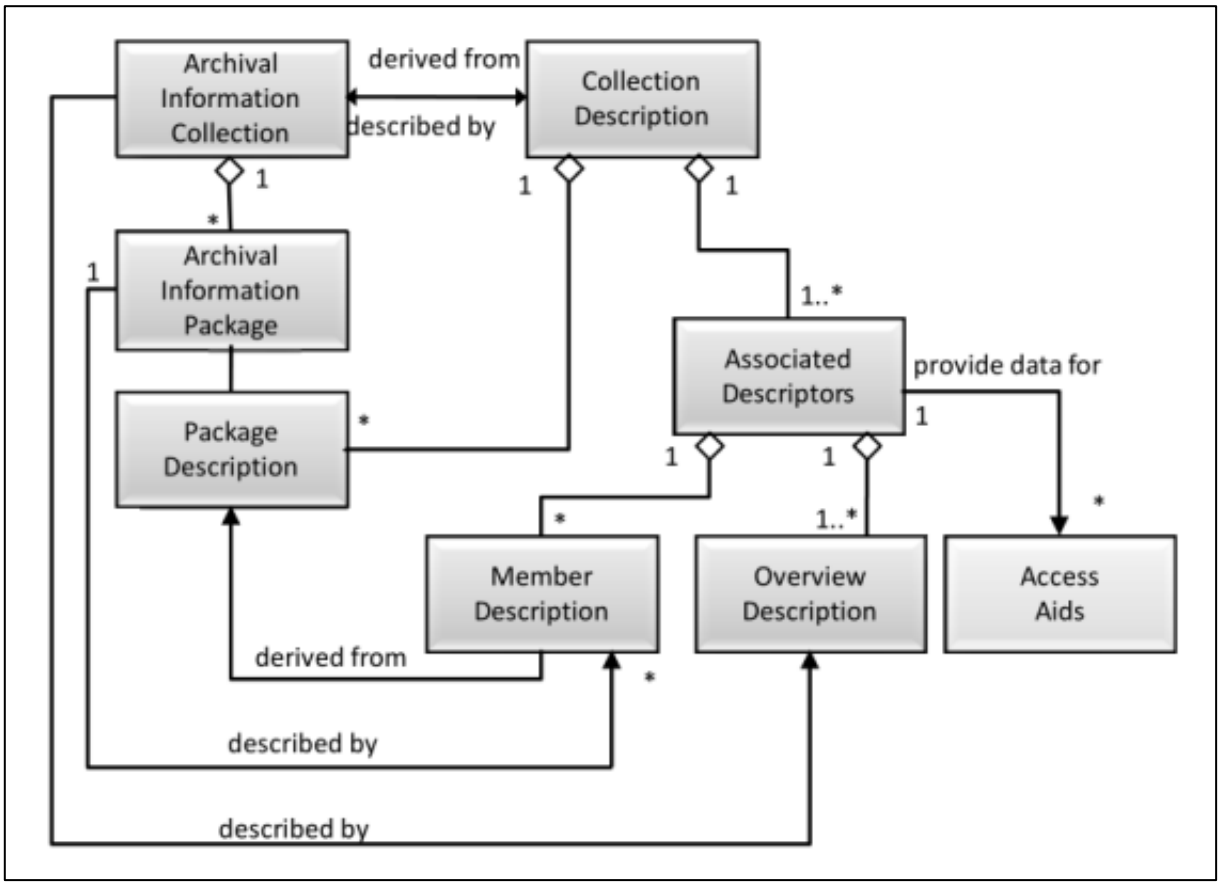


Fonte: (CCSDS, 2012, p. 4-46).

4.1.3.4.8 Descrições da coleção

A descrição da coleção é um subtipo da descrição do pacote, que contém estruturas para trabalhar melhor com a informação de conteúdo complexa de uma AIC. Existem dois tipos de descrição associada em uma descrição de coleção: uma descrição associada que descreve a coleção como um todo; e zero ou mais descrições de membro que descreva separadamente cada membro da coleção (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A seguir, as classes da descrição da coleção são apresentadas na “Figura 26 – Descrições da coleção”.

Figura 26 – Descrições da coleção



Fonte: (CCSDS, 2012, p. 4-47).

A descrição associada (*associated descriptors*), necessária em uma descrição de coleção (*collection description*), fornece informações para instrumentos de solicitação, permitindo que o usuário acesse todo o conjunto de informações de conteúdo e PDI da AIC associada[42]. A descrição da coleção (*collection description*) pode conter as descrições de pacotes AIP contidos na AIC. Logo, a AIC pode incluir as descrições de pacotes (*package description*) dos pacotes de informação membro. Esta lista das descrições dos pacotes (*package description*) para AIP contidos em uma AIC pode fornecer instrumentos de acesso (*access aids*) com um método para recuperar ou solicitar membros individuais da AIC (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Além disso, ressalta-se que é possível implementar instrumentos de acesso alternativos, onde o consumidor poderá solicitar AIP's de interesse que estejam contidos em um AIC.

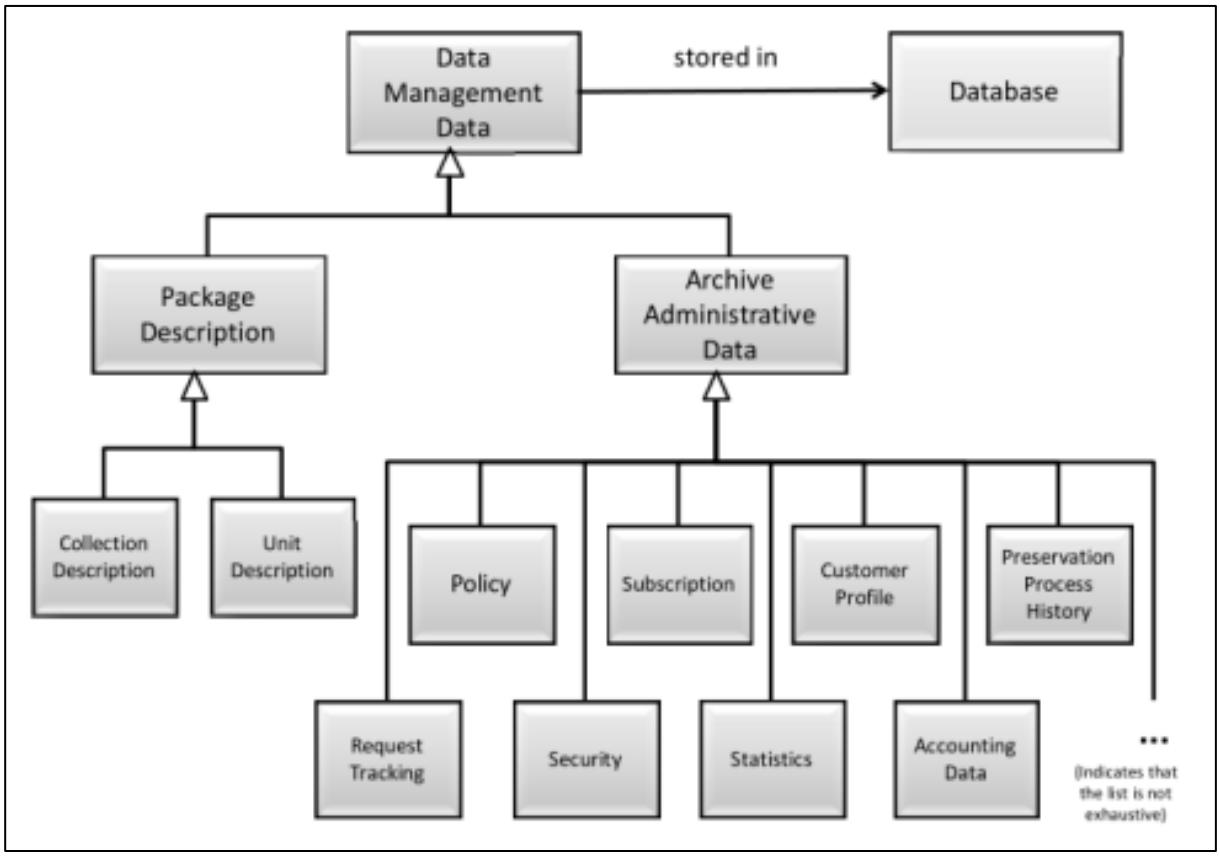
[42] Mas não necessariamente para os AIP individuais contidos na AIC.

4.1.3.5 Informações da gestão de dados

As descrições de pacotes são armazenadas em uma área permanente, que pode ser comparada a sistemas gerenciadores de banco de dados sistemas, para assim, facilitar o acesso e atualização das descrições associadas de modo flexível. Observa-se que além das descrições de pacotes, todas as informações necessárias para operação do OAIS pode ser armazenadas em bancos de dados com classes de dados permanentes (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A informação de administração do arquivo representa o conjunto de informações necessárias para operação rotineira do OAIS. A seguir a "Figura 27 – Informação de gestão de dados" ilustra os vários tipos desta informação de gerenciamento dentro do OAIS.

Figura 27 – Informação de gestão de dados



Fonte: (CCSDS, 2012, p. 4-50).

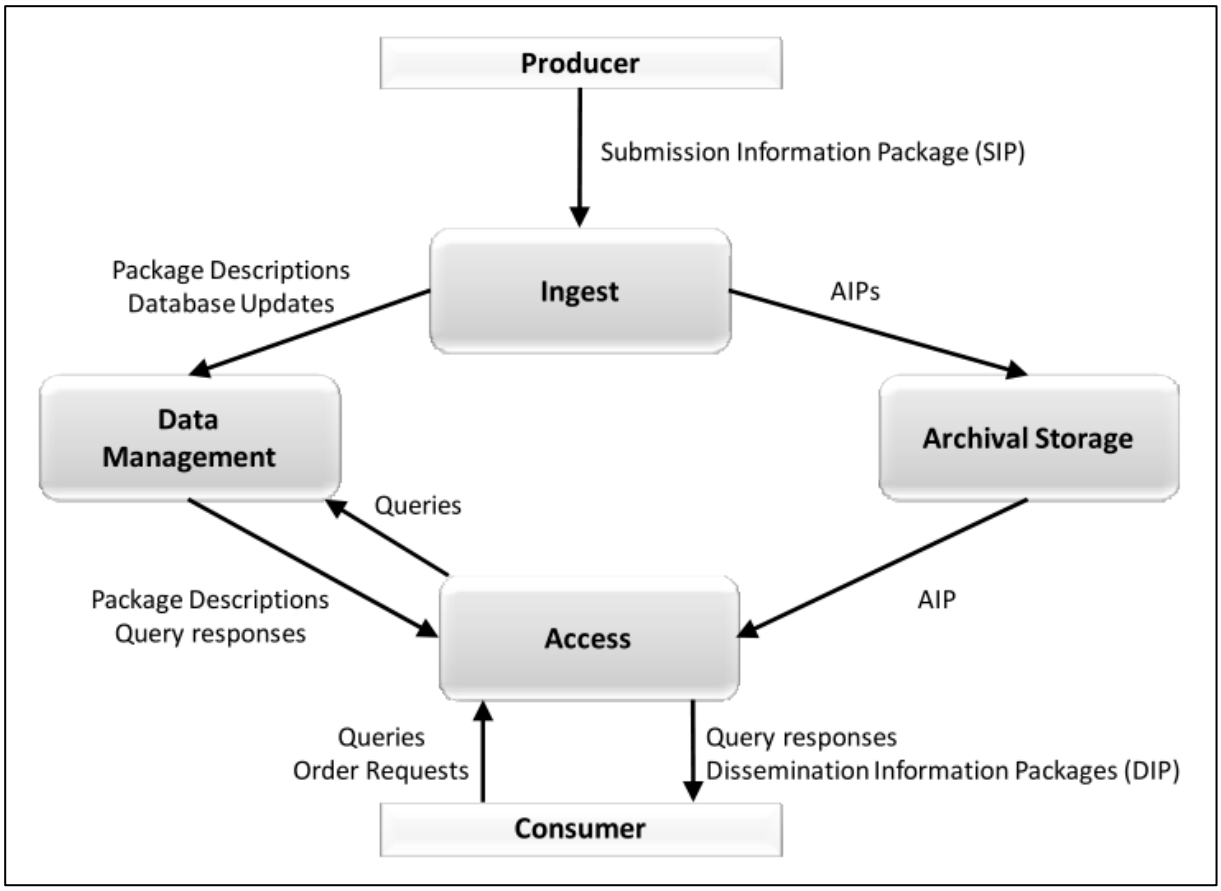
Conforme a figura 27, a “informação de gestão de dados” inclui:

- Informações sobre as políticas, compreendendo os custos, a disponibilidade e as restrições para solicitar informações arquivadas;
- Acompanhamento das requisições dos usuários e registro do progresso de cada transação;
- Informações de segurança, incluindo nomes de usuário, senhas e demais mecanismos de autenticação;
- Informações sobre solicitações programadas, que fornecem suporte para repetir as pedidos futuros;
- A informação estatística para entidade de administração com a finalidade de determinar futuras políticas e ajustar o desempenho do OAIS para operar de forma mais eficaz;
- A informação histórica do processo de preservação que rastreia as migrações, alteração de suporte e demais transformações no AIP;
- Informações sobre o perfil do consumidor, desta forma, o OAIS armazena informações básicas do consumidor que não necessitam ser informadas em solicitações futuras;
- Informação contábil, incluindo os dados necessários ao funcionamento do OAIS enquanto negócio.

4.1.4 Transformações do pacote de informação

Durante o ciclo de vida entre: produtor e OAIS; e OAIS e consumidor; ocorrerão transformações lógicas e/ou físicas nos pacotes de informação e em seus respectivos objetos associados. Estas transformações podem ser observadas a seguir na “Figura 28 – Fluxo de dados em alto nível do OAIS” que apresenta os fluxos de dados essenciais, presentes nas operações do OAIS. Posteriormente, discutem-se as transformações nas entidades: produtor (*producer*), admissão (*ingest*), armazenamento arquivístico (*archival storage*), gestão de dados (*data management*), acesso (*access*); e no próprio fluxo de dados.

Figura 28 – Fluxo de dados em alto nível do OAIS



Fonte: (CCSDS, 2012, p. 4-51).

4.1.4.1 Transformações de dados na entidade produtor

Os dados sob custódia da entidade produtor, são por natureza, dados privados, logo, podem estar em qualquer formato que o produtor desejar (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Desta forma, há possibilidade de uma variada gama de formatos de arquivos, originados de diversos *softwares*, e por vezes, sem a conformidade com os padrões recomendados para preservação de longo prazo.

No entanto, quando se decide armazenar estes dados em um OAIS, este produtor deve reunir-se com os arquivistas a fim de negociar um acordo de submissão que define informações como o conteúdo, o formato e os horários programados para recebimento dos SIP's. Posteriormente o repositório procede a execução das atividades de preservação definidas em sua política.

4.1.4.2 Transformações de dados na entidade admissão

O processo de admissão (*ingest*) transforma os SIP's recebidos em um conjunto de AIP's e descrições de pacote os quais que podem ser aceitos, e consequentemente, armazenados pelas entidades armazenamento arquivístico e gestão de dados. Observa-se que a complexidade do processo de ingestão pode variar consideravelmente, conforme as peculiaridades do OAIS e o produtor em questão.

Além disso, a entidade de admissão classificará os objetos de informação recebidos; posteriormente, determinará em quais coleções existentes cada objeto se enquadra; e por fim, após armazenar o AIP na entidade armazenamento arquivístico, a entidade de admissão emitirá mensagens solicitando a atualização das respectivas descrições das coleções (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Espera-se que a entidade de admissão coordene as atualizações entre as entidades armazenamento arquivístico e gestão de dados. Logo, será possível fornecer o gerenciamento e a recuperação de erros de forma adequada.

Desta forma, o AIP deverá, inicialmente, ser armazenado na entidade armazenamento arquivístico; em seguida, como confirmação dessa operação será incluída uma identificação única para recuperar esse AIP; e por fim, este identificador deve ser incorporado pela descrição do pacote antes de ser inserido na descrição de coleções na entidade de gestão de dados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.4.3 Transformações de dados nas entidades armazenamento arquivístico e gestão de dados

A entidade armazenamento arquivístico recebe os AIP's gerados no processo de admissão, que são acrescentados aos conteúdos permanentes do arquivo. Já a entidade gestão de dados recebe as descrições de pacotes gerados no processo de admissão e amplia as descrições de coleções existentes, para então, incluir seu conteúdo.

A visão interna do OAIS consiste na representação permanente dos dados armazenados, de modo que todas as codificações e mapeamentos devem ser devidamente documentados e compreendidos. A transferência dos objetos admitidos normalmente é realizada por um *software*, logo, o OAIS tem a responsabilidade de manter uma cópia deste *software* ou a documentação criteriosa dos formatos de arquivos que possuir. Desta forma, será possível realizar transferências para outros sistemas no futuro, sem perda de informação, mesmo que ocorra algum erro com o *software* que realiza as transferências (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.4.4 Fluxos de dados e transformações na entidade de acesso

Um instrumento de busca poderá ser usado quando um consumidor deseja localizar informações de interesse contidas no OAIS, estabelecendo uma relação de pesquisa com a entidade de acesso. Estes instrumentos de busca permitem que os consumidores possam selecionar o AIP de interesse e proceder à solicitação.

Desta forma, o consumidor produz uma visão lógica dos AIP's desejados e de suas respectivas descrições de pacote associadas a serem incluídos no pacote DIP. Além disso, o consumidor pode especificar os detalhes como tipo de mídia e o formato do objeto (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A entidade de acesso irá registrar a solicitação na entidade gestão de dados, e posteriormente, coordenará a resposta assim que a solicitação puder ser plenamente atingida. Observa-se que a maioria destas solicitações será atendida plenamente, caso contrário, a entidade de administração irá notificar a entidade de acesso quando os conteúdos estiverem disponíveis para entrega. Desta forma, a entidade de acesso contata as entidades armazenamento arquivístico e gestão de dados e solicitam os AIP's e as descrições de pacotes associados que sejam necessários para preencher o pacote DIP solicitado pelo consumidor. Assim, as entidades armazenamento arquivístico e gestão de dados criam cópias dos objetos solicitados na área de armazenamento temporário (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Por fim, a entidade de acesso transforma os pacotes AIP e as respectivas descrições de pacote associadas em um conjunto de pacotes DIP. Salienta-se que a complexidade deste processo de transformação pode variar consideravelmente em

virtude do nível dos serviços de processamento oferecidos pelo OAIS e solicitados pelo consumidor.

4.1.5 Perspectivas de preservação

A seguir discute-se a preservação da informação digital, no que tange à migração de formatos e suportes. Posteriormente discute-se a preservação dos serviços de acesso à informação, por meio do uso de estratégias, considerando as prováveis mudanças tecnológicas do *software* responsável por garantir o acesso.

4.1.5.1 Preservação da informação

A natureza efêmera das mídias de armazenamento aliada às rápidas mudanças da indústria de computadores compõe um antagonismo frente ao propósito fundamental do modelo OAIS: a preservação de informações no longo prazo. Neste ritmo de evolução acelerada da tecnologia, os sistemas informatizados tornam-se menos rentáveis em virtude da redução de sua perspectiva de longevidade.

Da mesma forma, a manutenção do aparato tecnológico necessário por garantir o acesso aos documentos se tornará mais complexa. Logo, isto poderá impactar na informação de representação, então necessária para preservar a informação de conteúdo (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Além disso, há de se considerar ainda que a base de conhecimento da comunidade designada irá mudar conforme os avanços da tecnologia, novamente afetando a informação de representação necessária. Como consequência, a migração de suportes e de plataformas de *hardware* e *software* torna-se necessária para continuar fornecendo o acesso aos consumidores.

A migração digital é definida como a transferência da informação digital que se pretende preservar no ambiente OAIS. Ela se distingue das transferências em geral por três aspectos, que são: o foco na preservação do conteúdo; a nova versão da informação implementada substituirá a anterior; e que possuirá controle e responsabilidade total sobre os aspectos da transferência do OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A migração digital possui uma série de especificidades, que devem ser consideradas no ambiente OAIS. Dentre estas, pode-se enfatizar: as razões para realizar a migração; o contexto da migração e os tipos de migração.

a) **Razões para a migração digital**: conforme o modelo OAIS há três principais razões para se realizar a migração digital, dentre elas, as melhorias do custo-benefício, a necessidade de contemplar novos requisitos para atender ao consumidor, e a substituição da mídia em virtude da sua deterioração;
b) **Contexto da migração**: corresponde a uma sequência de etapas, iniciando com a identificação da informação de conteúdo, em seguida, o mapeamento da informação descritiva, a identificação do respectivo AIP, e por fim, a informação de empacotamento irá identificar e delimitar a informação de conteúdo, a PDI, reunindo-as logicamente, em uma única entidade de preservação;
c) **Tipos de migração**: há quatro tipos de migração compatíveis com o modelo OAIS, que são a renovação, a reprodução, o reempacotamento e a transformação.

4.1.5.1.1 Tipos de migração

A **renovação** é um tipo de migração que envolve estratégias de refrescamento, tendo por finalidade, substituir uma mídia de armazenamento através da cópia exata para uma nova mídia, de modo que, o conjunto de *hardware* e *software* do armazenamento arquivístico continuará a funcionar como antes (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). A título de exemplo, a renovação ocorre ao se copiar os componentes AIP armazenados em um *Compact Disc* (CD) antigo (o qual corre risco de deterioração) para um CD novo.

A **reprodução (replicação)** é um tipo de migração que consiste na replicação dos componentes do objeto de informação (informação de empacotamento, informação de conteúdo e PDI), de modo que não ocorrerão alterações nos seus respectivos *bits*. Desta forma, os componentes do objeto de informação podem ser encapsulados e assim, serão facilmente replicados, mantendo a sequência de *bits* intacta. Este procedimento facilita a migração para novos tipos de mídia de

armazenamento e possui baixo risco de perda de informações (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

O **reempacotamento** é um tipo de migração necessário quando houver alterações nas informações de empacotamento durante a transferência. Desta forma, ocorrerá um reempacotamento ao se mover a informação de conteúdo, a informação de empacotamento e a PDI para uma nova mídia de armazenamento. Isto porque os *bits* usados para representar a informação de empacotamento são alterados (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A **transformação** é um tipo de migração digital que requer alterações na informação de conteúdo ou na PDI. Logo, as alterações nos *bits* do objeto de dados se refletem na informação de representação associada que lhe é correspondente. O AIP resultante do processo de transformação irá substituir o AIP que é submetido inicialmente. Assim, o novo AIP é entendido como uma nova versão do AIP anterior. No entanto, observa-se que a primeira versão da AIP, então dita original, pode ser preservada para fins de verificação da autenticidade das informações preservadas (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

As transformações podem ser de natureza reversível e não reversível. Desta forma, observa-se que a informação de representação desempenha um papel fundamental nas transformações, e os impactos das alterações sobre a mesma podem ser usados para categorizar as transformações.

a) **Transformação reversível**: ocorre a mudança de um determinado padrão por outro equivalente, ressalta-se que haverá equivalência semântica além de não haver perda de informação, logo, a transformação é reversível. A compressão sem perdas de uma imagem digital é uma transformação reversível;
b) **Transformação não reversível**: não há equivalência semântica, ocorrendo assim, perda de informação, o que impossibilita realizar o caminho reverso. Neste caso, a compressão com perdas de uma imagem digital é uma transformação não reversível, por isto, é preciso assegurar que não ocorram perdas significativas de informação para a comunidade designada.

É útil preservar as propriedades da informação de transferência como uma propriedade de informação do objeto; logicamente elas não podem verificar se a

transformação de natureza não reversível preservou adequadamente a informação de conteúdo, entretanto, podem evidenciar a autenticidade durante este processo de transformação não reversível (CCSDS, 2012; ISO 14721:2012). Observa-se que esta propriedade da informação do objeto atua como um mecanismo que registra as transformações não reversíveis, desta forma, tem-se uma visão das transformações ocorridas que corroboram com a presunção de autenticidade.

Salienta-se que com exceção da transformação, não será necessário criar uma nova versão do AIP ou mesmo atualizar a sua PDI para os demais casos de migração digital. A versão do AIP possui independência em relação à renovação, reprodução e reempacotamento; visto que tanto a informação de conteúdo, quanto a PDI não são afetadas por estes tipos de migração digital. Mesmo assim, o OAIS verificará se a migração não alterou a informação de conteúdo ou a PDI.

Quando a migração digital envolver transformação será necessário criar uma nova versão do AIP, na qual a PDI necessita ser atualizada para identificar a fonte e a versão do AIP, assim como descrever e justificar as alterações realizadas. Além disso, a descrição associada também necessita ser atualizada, no entanto, isto não implica, necessariamente, em alterar os instrumentos de acesso, salvo casos específicos (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

4.1.5.2 Preservação dos serviços de acesso

Tendo em vista as constantes mudanças tecnológicas, observa-se que o OAIS necessita preservar os serviços de acesso aos consumidores. Desta forma, são abordadas a seguir as seguintes questões relativas à interface de disseminação, perpassando ainda, questões como o código-fonte do *software* de acesso e o uso das estratégias de emulação.

4.1.5.2.1 Interface de disseminação

Haverá casos em que o acesso será mediado por *softwares* específicos, os quais não são essenciais para preservar as Informações do conteúdo, embora sejam convenientes ao acesso. Mesmo assim, estes *softwares* que apoiam o acesso se tornarão obsoletos com o tempo, e por consequência, deixarão de funcionar em virtude de alterações no ambiente operacional.

Em caráter paliativo, pode-se recriar a funcionalidade destes *softwares* para um novo ambiente. Tal ação não tem nenhum impacto sobre a preservação da informação de conteúdo, visto que se limita aos *softwares* de acesso. A recriação dos *softwares* poderá tem como base, o uso de emuladores, sendo que estes não alteram a informação de conteúdo (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A opção do OAIS em preservar um serviço para executar o *software* de acesso dependerá, essencialmente, da disponibilidade do código-fonte deste aplicativo. Desta forma, com a posse do código-fonte e da documentação adequada sobre o aplicativo, o procedimento recomendado seria a migração para um novo ambiente, e posteriormente testá-lo para garantir o seu funcionando adequado (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Se o *software* de acesso foi um pacote proprietário, amplamente utilizado e disponível comercialmente, é provável que exista um *software* de conversão usado comercialmente para transformar os atuais objetos de dados de conteúdo para outros formatos com aparência semelhante. Observa-se que este tipo de migração, provavelmente será uma transformação de caráter não reversível.

Caso não haja alternativa comercial, o OAIS poderá solicitar ao proprietário do *software* de acesso original uma ferramenta simplificada, com disponibilidade de parte do código fonte, a fim de acessar os objetos de dados de conteúdo. Este procedimento trata-se de uma negociação que envolverá custos adicionais ao processo de preservação, além de manter certo nível de dependência do OAIS em relação ao fabricante de *software*. Observa-se que esta abordagem pode ser inviável em virtude do custo ou mesmo por questões legais. Em todos os casos, o OAIS deve implementar mecanismos para verificar que nenhuma informação preservada foi perdida; além de garantir a disponibilidade do novo *software* de acesso à comunidade designada (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Tradicionalmente, as estratégias de emulação estão sendo utilizadas quando um determinado sistema operacional deve ser executado em uma plataforma de *hardware* para a qual não foi projetado. Entretanto, alguns recursos específicos podem ser perdidos em virtude da falta de compatibilidade.

Por esta razão, há investigações que abordam formas alternativas de emulação, como o desenvolvimento de máquinas virtuais ou emulação em nível de sistema operacional. Tais abordagens resolvem alguns dos problemas de emulação

de *hardware*, mas introduzem complexidade e consequentemente, novas preocupações (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

A emulação de um ambiente operacional com poucas aplicações a serem suportadas irá reduzir o risco de perda de informação, tornando sua implementação viável para o OAIS. Desta forma, a emulação poderá apoiar a preservação de longo prazo, sendo importante destacar que ela provoca alterações na PDI associada ao AIP, necessitando ser documentada; logo, é considerada como um tipo de migração digital, mais precisamente, uma transformação (CCSDS, 2012; ISO 14721:2012).

4.1.6 Interoperabilidade entre arquivos

Um OAIS pode ser distribuído geograficamente e mesmo assim, manter todas as partes sob a mesma administração, por exemplo, a entidade armazenamento arquivístico (*arquival storage*) pode ser dividida em diversos locais para aumentar a resistência contra desastres. Há casos em que consumidores de vários arquivos OAIS podem desejar uniformidade ou cooperação entre eles, como por exemplo, usar instrumentos de pesquisa comuns para ajudar na localização de informações em vários arquivos e possuir um local de acesso global. Já os produtores podem desejar um esquema de SIP comum para diferentes arquivos OAIS. E os administradores podem desejar meios para redução de custos com a partilha de *hardware*, *software* e esforços de preservação (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Desta forma, é observado no OAIS que a cooperação poderá ser vantajosa aos arquivos, tendo por finalidade:

- Reduzir custos;
- Satisfazer os consumidores com seus produtos e manter qualidade de serviço;
- E tornar o repositório mais competitivo frente a outros arquivos, objetivando questões como a sobrevivência e o crescimento.

4.1.6.1 Níveis de interação entre arquivos OAIS

Por padrão, um arquivo em conformidade com o modelo OAIS não é interoperável com outros arquivos. Entretanto, há razões para manter algum nível de

interoperabilidade desejável. Desta forma, há quatro categorias de associação para arquivos OAIS: independentes, cooperados, federados e de recursos compartilhados.

a) **Arquivos independentes**: atendem exclusivamente a uma comunidade designada. Questões como o projeto de pacotes DIP's e instrumentos de acesso são negociados com os consumidores. Um arquivo independente pode projetar essas estruturas com base em padrões de fato ou em normas, o que permitirá a cooperação com outros arquivos que implementam os mesmos padrões. Observa-se que a classificação de um arquivo OAIS como "independente" não é baseada em seu tamanho ou distribuição de funcionalidades. Logo, um arquivo independente pode ser fisicamente distribuído em diversos locais, além de poder usar diversos padrões para um determinado elemento interno. Entretanto, somente será considerado independente, caso não existam interações com outros arquivos;
b) **Arquivos cooperados**: são fundamentados em acordos de normalização entre dois ou mais arquivos. Um exemplo simples de cooperação entre arquivos é quando um OAIS atua como consumidor dos materiais de outro OAIS. Não há definição de padrões para pacotes SIP e DIP, o único requisito para esta arquitetura é que os grupos cooperados suportem pelo menos um formato SIP e DIP comum para pedidos entre os arquivos;
c) **Arquivos federados**: são conceitualmente orientados aos consumidores; ressalta-se que existe uma comunidade designada, a qual terá prioridade quanto ao acesso. Paralelamente, há uma comunidade global, a qual tem interesses em diversos arquivos OAIS e que de certa forma, influenciou esses arquivos para fornecer acesso por meio de instrumentos de pesquisa;
d) **Arquivos com entidades funcionais compartilhadas**: ocorre o compartilhamento ou integração de entidades funcionais em virtude de redução de custos necessários para a plena implementação do OAIS. Assim, o armazenamento comum consiste em manter uma entidade de armazenamento e uma entidade de gerenciamento de dados para dois arquivos distintos (OAIS-1 e OAIS-2). Observa-se que cada arquivo poderá servir comunidades totalmente independentes, no entanto, para o sucesso do armazenamento em comum, será preciso definir padrões para as interfaces

internas: admissão-arquivamento e acesso-arquivamento (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

No âmbito da Arquivística, pode-se destacar a aplicabilidade dos arquivos independentes e dos arquivos com entidades funcionais compartilhadas. No primeiro caso, se proporciona a cooperação quanto aos padrões de formatos e normas facilita o desenvolvimento da política de preservação. Deste modo, os Arquivos envolvidos podem se beneficiar mutuamente dos estudos e das práticas desenvolvidas em conjunto.

Já no segundo caso, o compartilhamento de entidades funcionais pode ser pertinente para a minimização de custos à administração. Entretanto, há necessidade de discussões de caráter predominantemente teórico, visto que compartilhar estas unidades funcionais implica em uma nova dimensão do princípio da proveniência dos Arquivos. Não se trata de uma nova visão deste princípio, e sim, de uma extensão adaptável ao contexto das tecnologias da informação e do próprio modelo OAIS. Desta forma, o ponto central desta questão consiste em: garantir que documentos digitais provenientes de diferentes arquivos poderão ser armazenados nas mesmas unidades funcionais sem que o princípio da proveniência seja desrespeitado.

Por fim, é preciso destacar que a interoperabilidade entre os repositórios pode acarretar significativos benefícios às comunidades de preservação digital. Estes benefícios se estendem desde a economia de recursos até a colaboração no desenvolvimento de padrões e conhecimentos.

4.2 ACTDR – ISO 16363:2012

Para que um repositório arquivístico digital seja considerado confiável, este deverá estar em conformidade com uma série de requisitos de ordem tecnológica e política. A literatura sobre preservação digital assinala o modelo funcional OAIS como principal referência base para se desenvolver um repositório digital. Da mesma forma, o OAIS permite o diálogo com a Arquivística, e poderá preservar documentos arquivísticos digitais autênticos em longo prazo.

No entanto, torna-se necessário desenvolver um ambiente de custódia confiável, e demonstrar que os conteúdos preservados, permanecem autênticos e

acessíveis no longo prazo. Logo, a ISO 16363:2012 atua como uma ferramenta capaz de avaliar a confiabilidade do repositório digital, e verificar se este atende os requisitos para ser considerado um “repositório digital confiável”. Desta forma, procede-se a análise dos requisitos para auditoria, observando sua relação com os requisitos do OAIS.

Os requisitos de auditoria da ISO 16363:2012 estão divididos três seções primárias: infraestrutura organizacional (*organizational infrastructure*), gestão de objetos digitais (*digital object management*), e infraestrutura e segurança da gestão de riscos (*infrastructure and security risk management*).

4.2.1 Infraestrutura organizacional

Inicialmente, a seção infraestrutura organizacional compreende aspectos relacionados à governança e viabilidade organizacional, estrutura organizacional e pessoal, políticas de responsabilidade e preservação, sustentabilidade financeira, e contratos, licenças e passivos. Estas questões estão diretamente relacionadas às políticas institucionais para preservação de documentos, e delineiam o planejamento organizacional e o funcionamento legal do arquivo responsável pela custódia documental.

4.2.1.1 Governança e viabilidade organizacional

Consiste em definir a missão do repositório e assumir o compromisso com a preservação e o acesso em longo prazo. Para isto, são definidos de forma explícita, os planos de sucessão e a política de recolhimento para custódia. Um RDC-Arq deve declarar o seu compromisso com a preservação dos documentos de tal caráter, e definir previamente quaisquer alterações na custódia, de modo a designar os requisitos a serem cumpridos por um eventual novo custodiador.

a) **Ter uma declaração de missão que reflete um compromisso de preservação, de retenção no longo prazo, de gestão, e de acesso à informação digital**: consiste em assegurar o compromisso com a preservação e garantia de acesso em longo prazo aos documentos em custódia. Esta é uma questão que deve ser definida em nível estratégico, e

pode ser expressa por uma declaração de missão ou mandato definido em âmbito jurídico[43]. Esta declaração deve ser mantida atualizada, de modo que os objetivos de preservação sejam explícitos, e reflitam os objetivos organizacionais (CCSDS, 2011; ISO 16363:2012). Tal declaração pode ser facilmente realizada por uma instituição arquivística, visto que esta tem o compromisso em preservar documentos arquivísticos. Mesmo assim, destaca-se a importância de reafirmar este compromisso, com a menção de termos como “documentos arquivísticos digitais”, “repositório arquivístico digital”, o que define claramente um compromisso em preservar os registros em ambiente informatizado;

b) **Ter um plano estratégico de preservação definido que o aproxime de sua missão apoiando o seu cumprimento no longo prazo**: ajuda o repositório a tomar decisões administrativas, definir políticas e alocar recursos para cumprir os seus objetivos de preservação. Tais questões podem ser evidenciadas por meio de atas de reuniões, documentos referentes a tomadas de decisões administrativas e da elaboração do próprio plano estratégico de preservação. Este plano deverá refletir os objetivos e os valores organizacionais definidos previamente em sua missão. Além disso, precisa ser revisado periodicamente (CCSDS, 2011; ISO 16363:2012). A preservação de documentos arquivísticos digitais exige uma série de recursos para garantir a sustentabilidade do arquivo no longo prazo. Logo, é preciso que estes recursos estejam previamente definidos no plano estratégico de preservação;

- **Ter um plano de sucessão, contingência e/ou acordos judiciais apropriados caso em algum momento, o repositório cesse a sua atividade ou o governo ou instituição de financiamento altere substancialmente o seu âmbito**: caso o repositório deixe de operar, estes planos permitem preservar as informações de conteúdo, de modo que estas sejam entregues para um novo custodiador. Para efetuar este procedimento o repositório deve declarar explicitamente, junto ao sucessor, a intenção de garantir a sua continuidade, bem como conceder

[43] Delegação procuração, representação, encargo incumbência, etc.

os direitos necessários para garantir o acesso aos conteúdos e prestação de serviços. Além disso, é preciso assinalar os *softwares* e metadados necessários para que o sucessor seja capaz de reconstruir o novo repositório em caso de falha (CCSDS, 2011; ISO 16363:2012). É essencial definir previamente os possíveis rumos dos documentos preservados em caso de alterações que gerem impacto direto no custodiador. Alterar recursos financeiros ou mesmo o responsável pela custódia documental implica em reformular o processo de preservação. Para isto, deve garantir todas as informações e permissões necessárias para que o novo custodiador consiga executar as atividades de preservação necessárias;

- **Controlar seu ambiente organizacional para determinar quando deve executar o seu plano de sucessão, contingência e/ou acordos judiciais**: garante que o repositório será capaz de reconhecer quando é necessário executar esses planos. Para isto, o repositório utiliza-se de planos de negócio, análises financeiras e políticas administrativas para verificar periodicamente a sua viabilidade (CCSDS, 2011; ISO 16363:2012). O arquivo enquanto instituição deve estar ciente das influências que circundam o ambiente de preservação, analisando questões políticas e econômicas para definir a viabilidade de continuar preservando tais conteúdos. Assim, caso não seja sustentável, o RDC-Arq deve proceder a sucessão dos conteúdos, e repassar a responsabilidade pela custódia;

c) **Ter uma política de recolhimento ou documentação que especifique o tipo de informação que irá preservar e garantir acesso**: orienta sobre a aquisição de conteúdos digitais que serão mantidos em custódia, a fim de preservar e garantir acesso. Para isto é preciso definir políticas de preservação digital fundamentadas na missão, na visão e nos objetivos do repositório (CCSDS, 2011; ISO 16363:2012). No caso de um RDC-Arq digital confiável, os conteúdos a serem admitidos no repositório devem ser exclusivamente, documentos arquivísticos. Também será preciso identificar e distinguir os produtores, caso os documentos tenham mais de uma proveniência, e assim, registrar com precisão os procedimentos utilizados

durante a aquisição. Isto irá manter a proveniência dos acervos, respeitando os princípios arquivísticos.

4.2.1.2 Estrutura organizacional e de pessoal

Compreende a gestão das competências de pessoal necessárias para o cumprimento das funções do repositório. Definir o organograma organizacional no qual explícita a divisão de funções e responsabilidades. Além disso, incentiva o desenvolvimento pessoal, auxilia a formação continuada para desenvolver habilidades e gerar novos conhecimentos. Desta forma, a equipe do arquivo deve estar em constante atualização, visto que os documentos em ambiente digital impõem novos desafios frente ao profissional arquivista, o qual vivencia uma transição dos acervos analógicos para acervos mistos (analógicos e digitais).

a) **Identificar e estabelecer as funções que deve executar, bem como dispor de pessoal com qualificação e experiência para tal**: a equipe de ser composta por pessoal apto para desenvolver as atividades. Desta forma, o repositório deve documentar as habilidades e cargos necessários através de planos de desenvolvimento, organogramas, descrições de funções, políticas relacionadas e procedimentos necessários à sua operação contínua (CCSDS, 2011; ISO 16363:2012). Os funcionários devem ser capacitados conforme surjam as demandas relacionadas à evolução das tecnologias. Este ponto é fundamental, pois as tecnologias da informação e comunicação evoluem em um ritmo cada vez mais acelerado. Tal fato tem ocasionado ciclos de obsolescência cada vez mais curtos, o que torna o processo de atualização dos funcionários tão essencial quanto à atualização tecnológica;

   - **Identificar e estabelecer seus deveres**: assegura que o repositório pode completar todas as tarefas relacionadas à preservação de longo prazo e a gestão dos objetos de dados. Para isto, podem-se definir as competências necessárias, bem como elaborar um plano de desenvolvimento pessoal da equipe. Dentre os aspectos pertinentes a serem considerados, ressalta-se a manutenção de *hardware*, *software*, a capacidade de migrar os dados dos suportes, e a capacidade de negociar acordos de direitos de

propriedade intelectual (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve estar ciente de suas atividades e demonstrar capacidade de cumpri-las, a fim de garantir a sua sustentabilidade no logo prazo;

- **Ter o número adequado de funcionários para realizar todas as funções e serviços**: consiste em garantir níveis adequados de pessoal para preservar o conteúdo digital, fornecendo um ambiente seguro e de qualidade. Para isto é preciso definir as funções e as responsabilidades atribuídas aos funcionários conforme as exigências, além de demonstrar avaliação da eficácia de seus funcionários frente aos serviços prestados (CCSDS, 2011; ISO 16363:2012). No contexto de um RDC-Arq, ressalta-se a necessidade de uma equipe interdisciplinar/multidisciplinar. Assim, profissionais de diversas áreas dialogando entre si, corroboram para o cumprimento das atividades do repositório, e com isso, eleva-se a qualidade dos serviços prestados;

- **Colocar em prática um programa de desenvolvimento profissional ativo que oferece oportunidades de desenvolvimento de competências ao pessoal**: isto garante que as habilidades do pessoal irão acompanhar a evolução da tecnologia e os procedimentos de preservação do repositório. Isto pode ser demonstrado com metas de desempenho, documentos que comprovem gastos com treinamentos, e planos de desenvolvimento pessoal e relatórios (CCSDS, 2011; ISO 16363:2012). Este é um requisito de aprendizagem, pelo qual o repositório acompanha a evolução das tecnologias, dos procedimentos e da própria comunidade designada. Todo arquivo que preserva documentos em um repositório digital deve manter um plano de atualização tecnológica. Isto se faz necessário por causa da constante evolução das tecnologias aliado a necessidade de fornecer acesso aos conteúdos autênticos e inteligíveis.

4.2.1.3 Políticas de responsabilidade e preservação

Os requisitos desta subseção preconizam que o repositório deve assegurar às partes interessadas (consumidores, produtores, e colaboradores), que irá

corresponder às suas necessidades enquanto um repositório digital confiável. Para isto, deve criar uma documentação que reflita, fundamentalmente, sua missão, seu plano estratégico e suas atividades rotineiras. Desta forma, a documentação de todos os processos do repositório, as tomadas de decisão e a definição de objetivos devem ser fornecidas as partes interessadas (CCSDS, 2011; ISO 16363:2012).

O repositório deve definir a comunidade designada e a base de conhecimento, além de possuir políticas para o cumprimento dos serviços, acompanhar a evolução das tecnologias e da comunidade designada, e receber o *feedback* de produtores e consumidores. Outro fator pertinente é manter ações transparentes de preservação, registro das transformações da informação e da avaliação de integridade, desta forma, é possível manter um calendário regular para certificação.

a) **Definir a sua comunidade designada e a base de conhecimento associada, e manter essas definições de forma acessível**: permite testar se o repositório atende às necessidades de sua comunidade designada. Para isto pode-se usar uma definição escrita a fim de formalizar (CCSDS, 2011; ISO 16363:2012). No caso de um RDC-Arq, a comunidade designada, a qual corresponde ao arquivo e seus usuários potenciais, assume um caráter muito abrangente e genérico. Logo, os documentos preservados correspondem, por vezes, desde uma parcela significativa da sociedade até a nação como um todo;

b) **Ter políticas de preservação para garantir que seu plano estratégico de preservação será cumprido**: assegura que o repositório pode cumprir sua missão relacionada à preservação. Para comprovar este requisito podem ser utilizadas as definições da política de preservação, assim como a missão do repositório (CCSDS, 2011; ISO 16363:2012). As políticas irão mostrar como o repositório cumpre os requisitos do plano estratégico de preservação. Desta forma, as políticas de preservação do arquivo devem ter claras menções ao repositório e aos documentos digitais;

   - **Ter mecanismos de revisão, atualização e desenvolvimento permanente das suas políticas de preservação, os quais irão**

monitorar o crescimento do repositório, assim como a evolução da tecnologia e da prática da comunidade: mantém políticas e procedimentos atualizados capazes de refletir as exigências para preservação de sua comunidade designada. Para isto, deve documentar as políticas de preservação, o plano estratégico de preservação, os fluxos de trabalho e demais procedimentos e demonstrar que possui um ciclo de revisão para esta documentação (CCSDS, 2011; ISO 16363:2012). Tais políticas devem ser compreensíveis pela equipe do repositório a fim de auxiliar no trabalho. Logo, a revisão deve centrar-se em manter o caráter arquivístico dos documentos, de modo que as tecnologias sejam adaptadas aos princípios da Arquivística, e nunca o contrário;

c) **Manter um histórico documentado das alterações em suas operações, procedimentos, *software* e *hardware***: proporciona uma "trilha de auditoria", de modo que as partes interessadas podem identificar e esquematizar as decisões tomadas pelo repositório. Para isto, pode-se usar documentação referente a versões anteriores das políticas e procedimentos, minutas de reuniões, e aos inventários de bens de capital, aquisição, implementação, atualização e retirada de *hardware*/*software* em estado crítico. Esta documentação pode incluir decisões sobre a infraestrutura técnica e organizacional, e pode explicar as práticas e o fluxo de trabalho do repositório (CCSDS, 2011; ISO 16363:2012). A preservação de documentos arquivísticos requer o constante monitoramento e registro dos procedimentos, a fim de verificar a sua evolução, seja de tecnologia, seja de procedimentos. Isto possibilita futuras análises sobre as decisões tomadas, verificando os pontos assertivos e os equívocos;

d) **Manter a transparência e responsabilidade em todas suas ações, além de apoiar a operação e a gestão do repositório no que tange a preservação de conteúdos digitais no longo prazo**: a transparência, no sentido de estar disponível aos interessados, é a melhor garantia de que o repositório opera de acordo com normas e práticas amplamente aceitas. Tal requisito pode ser evidenciado por meio de relatórios de auditorias e certificações técnicas e financeiras, avaliações independentes, contratos de

financiamento, acordos com fornecedores e serviços críticos realizados. A organização deve se comprometer em divulgar seus métodos de preservação à comunidade designada e demais partes interessadas, para demonstrar que está cumprindo todos os requisitos atuais (CCSDS, 2011; ISO 16363:2012). Além dos padrões amplamente conhecidos pela comunidade de preservação digital, o RDC-Arq pode demonstrar que segue recomendações como as do Conselho Nacional de Arquivos, tem práticas orientadas ao projeto INTERPARES, entre outros estudos pertinentes;

e) **Definir, coletar, rastrear e fornecer adequadamente as suas medições de integridade das informações**: consiste em fornecer a documentação comprovando o desenvolvimento ou adaptação de medidas adequadas para garantir a integridade. As evidências consistem em definições por escrito que comprovem a implementação de mecanismos de monitoramento que irão verificar a integridade como, por exemplo, *checksum*[44] e *hash*[45]. Os mecanismos para medir a integridade vão evoluir junto com a tecnologia, desta forma, pode fornecer uma documentação comprovando o desenvolvido de regras e mecanismos incorporados ao repositório, demonstrando assim, a implementação de medidas de integridade (CCSDS, 2011; ISO 16363:2012). A verificação da integridade é um procedimento essencial para repositórios arquivísticos, de modo que estes documentos em ambiente digital tornam-se extremamente vulneráveis, e podem ser modificados/falsificados com facilidade e sem deixar vestígios aparentes;

[44] Código usado para verificar a integridade dos dados armazenados por determinado período. É realizado ao calcular a soma de verificação dos dados antes do armazenamento, e recalculando-os aos recuperar os dados armazenados. Caso o valor obtido seja o mesmo, significa que as informações não sofreram alterações, logo, não houve corrupção de dados. As funções de *checksum* podem facilmente detectar falhas acidentais, porém caso a integridade dos dados seja uma questão de segurança, torna-se necessário implementar uma função mais robusta.

[45] Sequência de *bits* gerada por um algoritmo de dispersão, que mapeia dados de comprimento variável para dados de comprimento fixo. Em geral, esta sequência é representada em base hexadecimal. O *hash* é a transformação de uma grande quantidade de dados em uma pequena quantidade de informações. Essa sequência é capaz de identificar um objeto digital unicamente. Além disso, as funções usadas em criptografia garantem que não é possível retornar à informação original a partir de um valor de *hash*. Ressalta-se que a sequência do *hash* é limitada, logo, podem existir duplicidades no código, desta forma, quanto maior for a dificuldade de se criar duplicidades intencionais, melhor será o algoritmo.

f) **Comprometer-se a um calendário regular de autoavaliação e certificação externa**: assegura que o repositório mantém-se confiável e não há ameaças aos seus conteúdos. Para tal, a confiabilidade deve ser demonstrada periodicamente, de modo que seja um compromisso no longo prazo. As evidências para este requisito consistem em auditorias de terceiros, certificados de cumprimento de normas ISO (CCSDS, 2011; ISO 16363:2012). Um RDC-Arq deve se submeter a auditorias periódicas para que possa ser denominado como “confiável”. Ressalta-se que este não é um procedimento definitivo, o qual precisa ser reafirmado por meio de nova auditoria e consequente certificação. Assim, por meio uma constante caracterização de confiança, o repositório mantém-se confiável perante a comunidade de preservação e comunidade designada.

4.2.1.4 Sustentabilidade financeira

Compreende a definição de processos de planejamento para curto e longo prazo, com ajustes periódicos. Assim, preconizam-se procedimentos financeiros transparentes com auditoria, além de monitorar continuamente os riscos, benefícios, investimentos e despesas, buscando solução para problemas de financiamento.

a) **Dispor de processos de planejamento de negócios no curto e no longo prazo, para garantir a sustentabilidade ao longo do tempo**: assegura a viabilidade do compromisso que o repositório assumiu diante da comunidade designada, que consiste em fornecer acesso aos seus conteúdos no longo prazo. Este requisito pode ser evidenciado através de planos de negócios, declarações financeiras auditadas anualmente, previsões financeiras com vários cenários de orçamento, planos de contingência e análises de mercado análise (CCSDS, 2011; ISO 16363:2012). Em se tratando de um RDC-Arq, este tem o compromisso inato com a preservação e o acesso á documentos no longo prazo. Isto porque a finalidade da Arquivística consiste em preservar e garantir acesso;

b) **Ter procedimentos financeiros transparentes, em conformidade com normas e práticas contábeis relevantes, e ser auditado por terceiros, em**

conformidade com os requisitos legais de seu respectivo território: consiste em proteger o repositório contra a má fé ou atividades desfavoráveis, que possam ameaçar sua viabilidade econômica. Este requisito pode ser evidenciado por meio de requisitos de contabilidade, e por demonstrações financeiras, como as auditorias anuais. Os requisitos de confidencialidade podem proibir que determinadas informações sobre as finanças tornem-se públicas, entretanto, o repositório deve seguir o princípio da transparência, e ser capaz de demonstrar que está satisfazendo as necessidades de sua comunidade designada (CCSDS, 2011; ISO 16363:2012). Este requisito está estreitamente ligado a questões administrativas e contábeis do RDC-Arq. A transparência atua como um meio para gerar confiança na gestão financeira, não entrando em aspectos do campo teórico da Arquivística;

c) **Comprometer-se em analisar e informar continuamente sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos)**: consiste em demonstrar que o repositório é capaz de identificar e responder aos riscos, descrever e alavancar benefícios, especificar e equilibrar os investimentos, e antecipar e se preparar para os gastos. Este requisito pode ser evidenciado pela documentação referente às ameaças potenciais percebidas, planejamento de investimentos em infraestrutura de tecnologia, análises custo/benefício, licenças, contratos e revisões com base nos riscos (CCSDS, 2011; ISO 16363:2012). Desta forma, o repositório irá manter o equilíbrio adequado entre o risco e benefício, investimentos e retorno. Assim, um RDC-Arq deve manter uma estrutura próxima do ideal, de modo a considerar a relação custo/benefício. No entanto, a otimização de recursos não deve se sobrepor a necessidade de implementação de determinados requisitos necessários à preservação e garantia de acesso a documentos autênticos.

4.2.1.5 Contratos, licenças e passivos

Consiste em manter contratos ou acordos de depósito apropriados aos materiais digitais de outra organização, capazes de especificar e transferir todos os direitos de preservação necessários. Da mesma forma, permite rastrear e gerenciar

os direitos de propriedade intelectual e possíveis restrições sobre o uso do conteúdo, definindo as políticas com base na legislação para conteúdos digitais com propriedade ou direitos não especificados claramente.

a) **Manter contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e/ou fornece acesso**: assegura que o repositório tem os direitos e autorizações necessários que lhe permitem recolher e preservar conteúdos digitais ao longo do tempo, tornar essas informações disponíveis à sua comunidade designada e demonstrar esses direitos quando contestado. Este requisito pode ser evidenciado por meio de contratos de depósito, políticas sobre as modalidades de depósito de terceiros, definições dos níveis de serviço e usos permitidos, e procedimentos regulares para revisar convênios, contratos e licenças. É preciso demonstrar que os contratos e demais acordos estão sendo seguidos, além de reconhecer firma a fim de formalizá-los. Idealmente, acordos e contratos devem ser gerenciados e estar acessíveis em uma base de dados (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve possuir as permissões legais (autorizações, contratos e licencas) necessárias para recolher e preservar uma determinada informação, corroborando com formação da sua imagem enquanto custodiador;

- **Ter contratos de depósito que especificam a transferência de todos os direitos de preservação necessários, e que esses direitos estejam documentados**: permite ter um controle suficiente para preservação da informação, além de limitar a exposição do repositório a responsabilidades ou prejuízos legais e financeiros. Este requisito pode ser evidenciado através de contratos de depósito, declarações sobre os direitos necessários à preservação dos conteúdos. Por vezes, o direito de realizar alterações na informação digital é limitado pelo criador, entretanto, o repositório pode adquirir tais direitos para executar as alterações necessárias à preservação (CCSDS, 2011; ISO 16363:2012). Alterar a informação digital é uma tarefa necessária para preservá-la em um RDC-Arq. Determinadas tecnologias tornam-se obsoletas, logo é necessário

migrar para novos suportes e formatos de arquivo para continuar acessando os conteúdos;

- **Especificar todos os aspectos relevantes de aquisição, manutenção, acesso e retirada de conteúdos, através de acordos documentados com os depositantes e outras partes relevantes**: assegura que durante o depósito de conteúdo digital e consequente transferência de responsabilidade para preservação, as funções relativas do repositório, dos produtores e dos colaboradores, são compreendidas e aceitas por todas as partes. Este requisito pode ser evidenciado com acordos de submissão, contratos de depósito e procedimentos operacionais padronizados. Os contratos de depósito devem especificar todos os aspectos necessários ao gerenciamento dos conteúdos digitais, por exemplo, poderá haver um único acordo que contemple todos os depósitos ou acordos específicos para cada depósito. Assim, os acordos podem atribuir responsabilidades aos depositantes, tais como padronização dos pacotes SIP, de modo que o repositório possa recusar o SIP que não atender aos padrões. Em outros casos, o repositório pode assumir a responsabilidade de adequar o SIP para ser admitido, ressalta-se que esta divisão de responsabilidades deve ser documentada de forma clara (CCSDS, 2011; ISO 16363:2012). O RDC-Arq assume a responsabilidade da preservação, manutenção e garantia de acesso aos documentos, e paralelamente, negocia aspectos da submissão do SIP junto aos produtores de conteúdos. Desta forma, é possível estabelecer que os conteúdos submetidos devam estar em conformidade com determinadas normas ou padrões recomendados pelo repositório;

- **Ter políticas documentadas que indiquem quando ele aceita a responsabilidade de preservação dos conteúdos de cada conjunto de objetos de dados submetidos**: evita incompreensões entre o repositório e o produtor/depositante durante a transferência de responsabilidade dos conteúdos digitais. Tal requisito pode ser evidenciado com acordos de submissão, contratos de depósito e recibos de confirmação enviados pelo repositório aos produtores/depositantes (CCSDS, 2011; ISO 16363:2012).

Este requisito formaliza a aceitação da responsabilidade pela custódia dos materiais submetidos ao RDC-Arq, e fornece documentação para as partes interessadas comprovando a transferência e as condições para que o compromisso seja firmado;

- **Ter políticas para atender as responsabilidades e os desafios relacionados às questões de propriedade/direitos**: minimiza as responsabilidades potenciais e os desafios de direito aplicados ao repositório. Tal requisito pode ser evidenciado por meio de definições de direitos, leis e regulamentos pertinentes, licenças e permissões obtidas junto aos produtores (CCSDS, 2011; ISO 16363:2012). Desta forma, ter políticas de preservação que mantenham a conformidade com leis e requisitos pertinentes irá minimizar as responsabilidades potenciais do repositório. Logo, o repositório terá maior controle dos documentos arquivísticos custodiados, o que corrobora para cumprir suas atividades relacionadas á preservação e garantia de acesso;

b) **Controlar e gerenciar os direitos de propriedade intelectual e restrições à utilização do conteúdo conforme exigido pelo contrato, acordo de depósito ou licença**: permite que o repositório tenha um mecanismo para rastrear e verificar os direitos e as restrições de uso dos objetos digitais armazenados. Tal requisito pode ser evidenciado por meio de acordos de depósito, metadados que capturam informações de direitos, e declarações das políticas de preservação definindo e especificando os requisitos para o processo de gestão de direitos da propriedade intelectual (CCSDS, 2011; ISO 16363:2012). Isto permite que o RDC-Arq identifique quaisquer impedimentos relacionados ao processo de preservação e acesso, de modo que defina políticas para solucionar tais problemas. Assim, verificam-se restrições com relação à alteração das informações, bem como as restrições para difusão e acesso de conteúdos.

4.2.2 Gestão de objetos digitais

A seção gestão de objetos digitais compreende aspectos relacionados à aquisição de conteúdo, criação do pacote de arquivamento, plano da preservação, preservação e manutenção dos AIP's, gestão da informação, e gestão de acesso.

4.2.2.1 Admissão: aquisição de conteúdo

Permite identificar as propriedades significativas dos objetos digitais que serão preservadas, para isto, são associadas às informações necessárias ao pacote SIP. As fontes de proveniência dos objetos admitidos devem ser autenticadas, e devem-se executar as correções necessárias a cada SIP submetido. Além disso, é preciso obter controle físico dos objetos digitais para preservá-los, e fornecer respostas adequadas ao produtor durante o processo de submissão.

a) **Identificar as informações de conteúdo e as propriedades da informação que serão preservadas**: apresentam-se aos financiadores, depositantes e usuários, quais responsabilidades são assumidas e quais aspectos são excluídos. Além disso, informa aos produtores/depositantes quais informações são necessárias. Tal requisito pode ser evidenciado através de uma declaração de missão, acordos de submissão, contratos de depósito, documentação das propriedades que devem ser preservadas, fluxo de trabalho e políticas de preservação (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq define quais aspectos da informação de conteúdo são pertinentes à preservação, informando assim, aos seus colaboradores;

   - **Ter procedimento(s) para identificar as propriedades da informação que serão preservadas**: estabelece junto com depositantes, financiadores, e comunidade designada, como o repositório determina e verifica quais características e propriedades serão preservadas em longo prazo. Estes procedimentos serão necessários para confirmar ou refutar a autenticidade dos registros preservados. Tal requisito pode ser demonstrado com acordos de submissão, contratos de depósito, políticas de preservação, documentação de fluxo de trabalho e a definição clara

das propriedades de informações que devem ser preservadas (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq estabelece os métodos e fatores utilizados para determinar os aspectos de diferentes tipos de informação de conteúdo para os quais assume a responsabilidade de preservação frente à comunidade designada. Ressalta-se que tais características são essenciais para a presunção de autenticidade, bem como para a interpretação/representação da informação de conteúdo;

- **Ter um registro das informações de conteúdo e das propriedades de informação que serão preservadas**: identificar e documentar as informações de conteúdo e as respectivas propriedades da informação dos registros sobre os quais se tem responsabilidade de preservar. Tal requisito pode ser evidenciado por meio de políticas de preservação, manuais de processamento, registros dos tipos de informação de conteúdo, estratégias de preservação adquiridos e planos de ação. Logo, o repositório deve demonstrar que estabelece e mantém uma compreensão de suas coleções digitais suficiente para garantir a preservação das propriedades a que se comprometeu. Esta informação poderá ser utilizada para determinar a eficácia das suas atividades de preservação no longo prazo (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq terá definido o que será preservado, e assim, firmar o compromisso com tais tipos de informação previamente definidas. Posterirormente, a demonstração do cumprimento deste requisito é um importante passo para demonstrar a capacidade de preservar documentos de forma confiável;

b) **Especificar claramente, no momento do depósito, qual informação precisa ser respectivamente associada com a informação de conteúdo**: compreender claramente o que precisa ser adquirido junto ao produtor. Tal requisito pode ser evidenciado por meio de requisitos de transferência, acordos entre o produtor e o repositório, e o fluxo de trabalho realizado para produzir o AIP. Desta forma, é preciso especificar exatamente os objetos digitais que são transferidos, qual a documentação está associada, assim como as restrições de acesso (CCSDS, 2011; ISO 16363:2012). O nível de

precisão destas especificações irá variar conforme as políticas de cobrança e sua relação aos produtores. Logo, o RDC-Arq deverá buscar junto ao produtor toda a informação necessária para representar corretamente os documentos recolhidos;

c) **Ter especificações adequadas que permitam reconhecer e analisar os SIP's**: garante que o repositório é capaz de extrair a informação dos SIP's. Tal requisito pode ser evidenciado pela informação de empacotamento do SIP's, informação de representação para os conteúdos dos SIP's, e especificações dos formatos de arquivo documentados. Logo, o repositório deve ser capaz de reconhecer o conteúdo de um SIP e confirmar se está dentro do esperado, se suas informações de conteúdo estão corretamente identificadas, e se as propriedades da informação de conteúdos foram selecionadas corretamente (CCSDS, 2011; ISO 16363:2012). Desta forma, o repositório poderá analisar o conteúdo de um determinado objeto digital e verificar se a sua estrutura lógica corresponde ao formato de arquivo que representa. Tal procedimento é pertinente, pois os formatos de arquivo podem não refletir o que realmente são. Um documento de texto pode estar equivocadamente representado em um formato de imagem, o que resulta em erro de interpretação/representação da informação de conteúdo;

d) **Ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais**: evita atribuir proveniência errônea às informações preservadas. Tal requisito pode ser evidenciado com procedimentos de autenticação, adição de vínculo jurídico aos acordos de submissão/contratos de depósito, e procedimentos e rotinas tecnológicas apropriadas (CCSDS, 2011; ISO 16363:2012). Isto garante que o RDC-Arq irá determinar corretamente a procedência de cada SIP recebido, mantendo um dos princípios essenciais da Arquivística, o princípio da proveniência;

e) **Ter um processo de admissão que verifique a integralidade e precisão de cada SIP**: detecta e corrige erros de criação e transmissão do SIP. Tal requisito pode ser evidenciado através de políticas de preservação, implementação do plano de preservação, registros detalhados das

transferências, definições de integridade e precisão. Desta forma, as informações coletadas durante o processo de admissão podem ser comparadas com informações coletadas anteriormente, que retratem as expectativas do produtor/depositante. A correção do SIP irá depender do conhecimento que o repositório tem sobre o mesmo e quais ferramentas estão disponíveis para verificar a precisão. Isto inclui verificar se os formatos de arquivo são o que eles afirmam ser ou verificar o seu conteúdo. O repositório também pode rejeitar a transferência, somente admitindo o SIP após reparar os erros (CCSDS, 2011; ISO 16363:2012). Um RDC-Arq deve ter um rígido controle de admissão de conteúdos, de modo que os pacotes AIP reflitam as informações de conteúdos dos pacotes SIP. Isto é essencial para demonstrar que o repositório está cumprindo com seus compromissos de preservação da integridade e demais compromissos firmados frente aos produtores;

f) **Obter controle suficiente sobre os objetos digitais para preserva-los**: assegura controle legal e físico para realizar as atividades de preservação. Tal requisito pode ser evidenciado por meio de documentos que comprovem o nível de controle físico do repositório e um catálogo em forma de banco de dados que seja capaz de listar todos os objetos digitais e seus respectivos metadados necessários para validar a integridade. Com este controle, o repositório poderá executar planos de preservação para os materiais custodiados tornem-se acessíveis aos consumidores (CCSDS, 2011; ISO 16363:2012). Um RDC-Arq necessita obter o controle dos documentos a fim de efetuar as atividades necessárias para sua preservação, assim como para prover o acesso à comunidade designada. Isto requer o controle legal e físico/lógico, de modo que isto seja suficiente para tomada de decisões relativas às suas atividades;

g) **Fornecer ao produtor/depositante respostas apropriadas aos pontos que foram definidos durante os processos de admissão**: assegura que o produtor pode verificar que não existem lapsos de comunicação que possam ocasionar a perda de SIP's. Tal requisito pode ser evidenciado por meio de acordos de submissão, contratos de depósito, documentação de fluxo de

trabalho e demais relatos de evidência por meio de memorandos e e-mails. O repositório deve fornecer relatórios de progresso ao produtor/depositante especificando os pontos definidos durante o processo de admissão, assim, deve informar relatório de erros, correções e qualquer transferência de custódia (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá manter o produtor informado sobre os procedimentos de admissão, de modo que seja possível demonstrar a conformidade com as questões definidas previamente;

h) **Ter registros contemporâneos de ações e processos de administração que são relevantes para aquisição de conteúdo**: garante que a documentação capturada é exata e verdadeira, e caso seja necessário, pode ser utilizada em uma auditoria. Tal requisito pode ser evidenciado através de documentação relativa a decisões, metadados de preservação que sejam armazenados e associados a objetos digitais, e possuir recibos de confirmação que são enviados aos fornecedores. Estes registros podem ser criados de forma automática ou inseridos por indivíduos autorizados, de qualquer modo, compete ao repositório demonstrar que todas as ações relevantes são realizadas (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve registrar todos os procedimentos administrativos para manter um histórico das ações realizadas, servindo para comprovar a execução de determinado procedimento. Ressalta-se que tais procedimentos administrativos são essenciais na presunção de autenticidade, e o seu registro adiciona confiabilidade ao ambiente informatizado.

4.2.2.2 Admissão: criação do AIP

Durante a criação do AIP define-se um identificador único de nomenclatura geral para cada AIP ou classe de informação, que demonstra a preservação de suas propriedades significativas. As transformações dos SIP's em AIP's são descritas, além de manter os identificadores únicos previamente associados. Um contexto semântico entre objetos digitais armazenados é estabelecido, e as informações de representação admitidas são registradas. Assim, devem-se documentar os processos de aquisição e gerenciamento dos metadados de preservação para as informações de conteúdo associadas, além de adquirir outros metadados

necessários à preservação. O processo de criação do AIP ainda requer a verificação da compreensão da informação de conteúdo, da integridade e da precisão de cada AIP. De forma complementar, deve-se fornecer um mecanismo para auditoria da integridade dos materiais custodiados, e manter registros de metadados de processos administrativos pertinente à preservação.

a) **Ter para cada AIP ou classe de AIP preservada, uma definição associada adequada para analisar o AIP e contemplar suas necessidades de preservação de longo prazo**: assegura que o AIP e sua definição associada, incluindo a informação de empacotamento apropriada, sempre poderão ser localizados, processados e gerenciados dentro do arquivo (CCSDS, 2011; ISO 16363:2012). Com isto, o RDC-Arq terá mais informações e assim poderá complementar as atividades de preservação;

   - **Ter capacidade de identificar qual definição se aplica para qual AIP**: assegura que a definição apropriada é usada ao analisar/interpretar um AIP. Tal requisito pode ser evidenciado pela documentação que relacione claramente cada AIP ou classe de AIP à sua definição (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq pode usar o método que considerar mais apropriado para associar as definições e os AIP's;

   - **Ter uma definição adequada de cada AIP para sua preservação no longo prazo, permitindo identificar e analisar todos os componentes necessários dentro desse AIP**: possibilita mostrar explicitamente que os AIP's estão apropriados à sua finalidade, sendo que cada componente de um AIP foi concebido adequadamente e executado, e os planos para a manutenção de cada AIP estão definidos. Tal requisito pode ser evidenciado por demonstrações do uso das definições para extrair informações de conteúdo e PDI do AIP. Desta forma, a documentação deve identificar cada classe de AIP e descrever como cada um é implementado no ambiente do repositório, e relacionar os componentes necessários para a preservação do AIP, garantindo aos produtores/depositante e consumidores que as propriedades significativas do AIP serão preservadas. Além disso, a documentação identifica

claramente que componentes do AIP podem ser geridos, bem como a necessidade de criar novas versões do AIP para cumprir sua finalidade (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq deverá identificar e manter uma relação dos componentes necessários para preservar as propriedades significativas dos AIP's. Além disso, será necessário demonstrar, periodicamente por meio da revisão, que tais componentes satisfazem as necessidades de preservação;

b) **Ter uma descrição de como o AIP é construído a partir SIP**: assegura que os AIP's representam adequadamente as informações relativas aos SIP's, para isto será necessário uma descrição precisa das ações, suficiente até mesmo para as transformações complexas. Tal requisito pode ser evidenciado pela documentação sobre a relação entre SIP's e AIP's, explicitando como os AIP's são derivados dos SIP's (CCSDS, 2011; ISO 16363:2012). Isto permite que o RDC-Arq demonstre que a informação de conteúdo armazenada na forma de AIP está em conformidade com aquela submetida originalmente pelo produtor na forma de SIP. Para tal, é necessário detalhar como ocorreram as transformações necessárias ao armazenamento. Esta descrição corrobora para demonstrar a autenticidade das informações de conteúdo, pois justifica as suas possíveis transformações, relacionando-as à necessidade de alterar a informação digital para melhor preservá-la. O registro destas ações também auxilia no processo de presunção de autenticidade dos documentos;

c) **Documentar a disposição final de todos os SIP's**: o RDC-Arq deve registrar os procedimentos relativos ao tratamento dos SIP's, e assim, indicar sua localização enquanto AIP ou eliminação, em casos especiais;

   - **Seguir os procedimentos documentados, caso um SIP não seja incorporado em um AIP ou descartado, deve-se justificar o motivo**: assegura que os SIP's recebidos foram tratados de forma apropriada, e que não ocorreram perdas acidentais. Tal requisito pode ser evidenciado através de registros de eliminação, acordos com depositantes, sistema de rastreamento da proveniência e documentação sobre como os AIP's são

derivadas do SIP's. Também se deve manter a informação descritiva apropriada sobre a proveniência de todos os objetos digitais (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq terá de registrar o motivo das exclusões de SIP's submetidos de forma equivocada, quando houver, visto que os documentos arquivísticos submetidos/recolhidos ao repositório não devem ser eliminados ou recusados de forma arbitrária. Logo, é necessário justificar a natureza do equívoco/erro ou mesmo inconformidade dos SIP's com as normas de submissão definidas previamente pelo repositório;

d) **Utilizar uma convenção que gera identificadores únicos para todos os AIP's**: com os identificadores únicos para cada AIP e componentes, o RDC-Arq poderá fazer verificações, inibindo duplicações;

- **Identificar cada AIP de forma exclusiva no repositório**: garante precisão no processo de busca e recuperação da informação de conteúdo;

- **Ter identificadores exclusivos**: evita duplicações dos AIP's e otimiza a sua localização no sistema;

- **Ceder e manter identificadores persistentes do AIP e de seus componentes, de modo a ser exclusivo dentro do contexto do repositório**: evita a dispersão dos componentes digitais relacionados ao AIP;

- **Descrever todos os processos utilizados para realizar alterações em tais identificadores**: acrescenta confiabilidade ao sistema de identificadores;

- **Fornecer uma lista completa de todos os identificadores e fazer verificações pontuais para identificar duplicações**: permite verificar continuamente a presença de informações duplicadas no RDC-Arq,

além de localizar os conteúdos com precisão, desta forma, auxilia na otimização do trabalho técnico e do armazenamento;

- O sistema de identificadores deve ser adequado para comportar a demanda atual do repositório e as previsíveis necessidades futuras, tais como números de objetos: assegurar que cada AIP pode ser inequivocamente encontrado no futuro e pode ser distinguido de todos os outros AIP's do repositório. Tal requisito pode ser evidenciado pela documentação que descreve a nomenclatura utilizada (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq garante a capacidade de recuperar a informação de conteúdo desejada com alto grau de precisão, o que é essencial para que comunidade designada demonstre confiabilidade quanto á preservação. A identificação está prevista pela Norma Brasileira de Descrição Arquivística (NOBRADE) (BRASIL, 2006), em seus elementos de descrição pode-se observar que o item "1 área de identificação" possui o subitem "1.1 código de referência" o qual tem como objetivo identificar a unidade de descrição. Esta identificação[46] perpassa, obrigatoriamente, o registro do código do país (BR), o código da entidade custodiador e o código específico da unidade de descrição (BRASIL, 2006). Com a Resolução nº 28, de 17 de fevereiro de 2009, publicada pelo Conarq, a instituição terá esta identificação ao realizar o Cadastro Nacional de Entidades Custodiadoras de Acervos Arquivísticos (CODEARQ) a qual deverá ser solicitada ao Conarq. Por consequência, os acervos cadastrados terão códigos padronizados o que facilita a distinção entre as instituições cadastradas. Esta resolução também recomenda o suso da NOBRADE aos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR) (BRASIL, 2009);

- **Ter um sistema confiável de ligação/localização para encontrar o objeto identificado exclusivamente, independentemente da sua**

[46] Por exemplo, o código "BR AN Q6.LEG.COR,TEL" pertence a instituição "Arquivo Nacional do Brasil", e corresponde a a subsérie Telegramas, nível 3,5, do fundo Floriano Peixoto, seção Governo Legal, série Correspondência (BRASIL, 2006).

localização física: rastrear as ações relacionadas ao AIP no longo do tempo, considerando as alterações do sistema e as mudanças de armazenamento. Tal requisito pode ser evidenciado através de documentação que descreva a convenção de nomenclatura e evidência física de sua aplicação. Identificadores únicos para uso interno e externo auxiliam o repositório a oferecer maior visibilidade no entendimento de gestores e auditores. O ideal é que os identificadores sejam gerados no momento da criação do AIP, caso contrário, deve haver rastreabilidade (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq deve localizar o AIP e seus respectivos componentes mesmo que sejam realizadas atualizações no sistema, na mídia ou local de armazenamento. Ou seja, deve haver um monitoramento contínuo capaz de recuperar tais informações;

e) **Ter acesso a ferramentas e recursos para fornecer informação de representação de autoridade necessária para todos os objetos digitais armazenados**: identificar os formatos de arquivo dos objetos digitais a fim de fornecer a informações de representação necessária a comunidade designada;

- **Identificar o tipo de arquivo de todos os objetos de dados submetidos**: isto permite que o RDC-Arq controle os formatos de arquivo em que os documentos são submetidos. Esta informação de monitoramento poderá ser útil para buscar melhores técnicas de tratamento para um determinado formato de arquivo;

- **Determinar a informação de representação necessária para tornar cada objeto de dados compreensível à comunidade designada**: o RDC-Arq deve reunir toda a informação necessária para a correta interpretação/representação dos objetos digital pela comunidade designada. Desta forma, além de cumprir as funções de preservação será necessário fornecer acesso de forma inteligível à documentação;

- **Ter acesso à informação de representação necessária**: o RDC-Arq deve buscar a informação de representação necessária junto aos produtores, desta forma, um processo de organização da informação determinará os componentes digitais que serão relacionados aos AIP's;

- **Assegurar que os requisitos da informação de representação são persistentemente associados aos objetos de dados relevantes**: garante que os objetos digitais do repositório são compreensíveis à comunidade designada. Tal requisito pode ser evidenciado por meio de acesso a registros da informação de representação, registros de bases de dados que incluem informação de representação e uma persistente ligação para objetos digitais relevantes. Contudo, este requisito não exige que cada repositório tenha suas próprias ferramentas e recursos, mas que tem acesso a eles. Isto permite reduzir os custos de manutenção no longo prazo e melhorar o controle de qualidade do repositório (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq terá a informação de representação suficiente para manter os objetos digitais acessíveis à comunidade designada. Para isto deverá ter acesso a ferramentas que executem tais atividades;

f) **Ter processos documentados para aquisição de PDI, conforme os processos documentados, para sua informação de conteúdo associada**: o RDC-Arq deve assegurar a reunião de todos os componentes de PDI necessários, e manter um mecanismo padronizado para coleta destes dados;

- **Ter processos documentados para a aquisição de PDI**: RDC-Arq definirá os procedimentos padronizados para adquirir a PDI necessária à representação da informação de conteúdo;

- **Executar processos documentados para a aquisição de PDI**: o RDC-Arq seguirá seus procedimentos de aquisição de PDI conforme definido previamente.

- **Assegurar que a PDI é persistentemente associada às informações do conteúdo relevantes**: mantém uma trilha de auditoria para apoiar reivindicações de autenticidade, de modo que mudanças não autorizadas nos materiais digitais podem ser detectadas. Desta forma, os objetos digitais possam ser identificados e recolocados no seu contexto apropriado. Tal requisito pode ser evidenciado através de procedimentos operacionais padronizados, manuais dos procedimentos de admissão, documentação sobre aquisição e gerenciamento da PDI. Além de auxiliar o repositório a garantir que a informação de conteúdo não foi corrompida (fixidez) e é encontrável (informação de referência), a PDI auxilia na compreensão da informação de conteúdo. Para isto, fornece uma perspectiva histórica (informação de procedência) assim como as relações com outras informações (informação de contexto). Assim, ressalta-se que a PDI deve ser permanentemente associada com a informação de conteúdo (CCSDS, 2011; ISO 16363:2012). Com isto, o RDC-Arq irá registrar informações adicionais e autorizadas, capazes de corroborar com a autenticidade dos conteúdos. Este fluxo de constante associação adicionará confiabilidade aos procedimentos de aquisição de PDI;

g) **Assegurar que as informações de conteúdo do AIP, no momento de sua criação, são compreensíveis à comunidade designada**: é essencial que o RDC-Arq crie AIP's já compreensíveis a comunidade designada. Assim, caso haja solicitações de acesso, o repositório irá dispor de toda a informação necessária que permita aos usuários interpretar corretamente a informação de conteúdo;

- **Ter um processo documentado para testar, no momento de sua criação, se a informação de conteúdo do AIP é compreensível à comunidade designada**: o RDC-Arq deve verificar logo no momento da criação do AIP, se a informação de conteúdo está acessível à comunidade designada. Assim, poderá inserir mais informações caso seja necessário para representar/interpretar as informações de conteúdo.

- **Executar um teste para cada classe de informação de conteúdo dos AIP's**: após reunir todos os componentes considerados necessários para a compreensão da informação de conteúdo pela comunidade designada é preciso executar testes para verificar cada componente do AIP;

- **Em caso de falha no teste de compreensibilidade, o repositório deve colocar as informações de conteúdo dos AIP's no nível de compreensão necessário**: assegura que um dos testes preliminares de preservação pode ser cumprido, e que os materiais digitais do AIP são compreensíveis pela comunidade designada. Caso o material admitido não seja compreensível, devem-se admitir informações adicionais. Tal requisito pode ser evidenciado por procedimentos de teste executados sobre os materiais digitais para garantir o nível de compreensão definido à comunidade designada. Assim, os registros destes testes, de evidência de recolhimento ou identificação da informação de representação para preencher lacunas de inteligibilidade, e da retenção de indivíduos com expertise da disciplina irão comprovar a conformidade com este requisito (CCSDS, 2011; ISO 16363:2012). Assim, caso as informações de conteúdo do AIP não sejam compreensíveis à comunidade designada, o RDC-Arq ficará responsável por buscar informações adicionais e acrescentá-las ao pacote AIP;

h) **Verificar a integralidade e exatidão de cada AIP no momento de sua criação**: assegura que os materiais mantidos em longo prazo podem ser rastreados com as informações fornecidas pelos produtores. Tal requisito pode ser evidenciado pela descrição do procedimento que verifica integralidade e a exatidão dos AIP's, observa-se que este procedimento tem início na recepção do SIP[47] (CCSDS, 2011; ISO 16363:2012). Assim o RDC-Arq deve manter uma descrição capaz de relacionar o AIP armazenado com o SIP submetido pelo produtor, de modo que este consiga recuperar as informações de conteúdo com integridade e precisão;

[47] Desta forma, caso o repositório tenha um processo de verificação (integridade e exatidão) do SIP, basta demonstrar como um AIP é derivado de um SIP que tenha sido previamente verificado.

i) **Fornecer um mecanismo independente para verificar a integridade do conjunto de conteúdos do repositório**: é de responsabilidade do repositório escolher um mecanismo para realizar a auditoria da integridade do conjunto como um todo. Tal requisito pode ser evidenciado através da documentação de acordos entre o produtor e o repositório, e pelos relatórios de verificações periódicas. Desta forma, o repositório deve ser capaz de demonstrar, para cada item, qual é o seu AIP do qual é derivado. Entretanto, pode ser necessário, em casos específicos, mostrar que não há AIP para um item, porque a admissão ainda está em andamento, ou porque o item foi rejeitado por algum motivo (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq deverá ter um mecanismo independente para verificar a integridade do acervo, identificando cada AIP e seus componentes relacionados. Isto é relevante para garantir princípios arquivísticos como o da proveniência e da integridade dos fundos. Tal verificação auxilia para reunir toda a informação necessária para a correta interpretação/representação das informações de conteúdo pela comunidade designada;

j) **Ter registros contemporâneos das ações e processos de administração que são relevantes à criação do AIP**: assegura um meio independente para verificar se todos os AIP's foram criados de acordo com os procedimentos documentados, e que nenhuma ação relevante foi omitida. Este requisito justifica as práticas do repositório e pode ser evidenciado pela documentação de decisões e medidas tomadas, e por registros de metadados de preservação referenciando os objetos digitais. Desta forma, o repositório deve demonstrar, por meio destes registros, que todas as ações pertinentes são realizadas (CCSDS, 2011; ISO 16363:2012). O RDC-Arq demonstra que segue uma política de criação de AIP's previamente definida. Além disso, poderá registrar ações relevantes com o uso de metadados de preservação devidamente associados a todos os componentes digitais.

4.2.2.3 Planejamento da preservação

Dentre as questões relacionadas ao planejamento da preservação, ressalta-se que o repositório irá identificar e documentar as estratégias de preservação

executadas. Irá notificar quando a informação de representação adquirir risco de obsolescência, alterar os planos de preservação conforme os resultados do monitoramento, e podem fornecer evidências da eficácia do planejamento da preservação.

a) **Ter uma documentação sobre as estratégias de preservação relevantes ao acervo**: isto fornecer um meio para verificar e validar o trabalho de preservação do repositório. Da mesma forma, define como o repositório pretende garantir que as informações permanecerão disponíveis e utilizáveis às gerações futuras. Tal requisito pode ser evidenciado por uma documentação que identifique cada risco da preservação e a respectiva estratégia para lidar com esse risco (CCSDS, 2011; ISO 16363:2012). Tais estratégias definidas pelo RDC-Arq em seu plano estratégico de preservação buscam solucionar riscos como a degradação dos meios de armazenamento, a obsolescência das unidades de mídia, e a obsolescência ou inadequação da informação de representação (incluindo formatos de arquivo).Desta forma, o repositório terá registrado todas as estratégias pertinentes à preservação e manutenção da autenticidade dos documentos;

b) **Ter mecanismos para monitorar o ambiente de preservação**: permite que o repositório possa reagir às mudanças e assegurar que as informações preservadas continuam sendo compreensíveis e utilizáveis pela comunidade designada. Além de ter um mecanismo para acompanhar e notificar quando as informações de representação estiverem se tornando potencialmente obsoletas, incluindo os formatos de arquivo. Tal requisito pode ser evidenciado por meio de inquéritos da comunidade designada (CCSDS, 2011; ISO 16363:2012). Com o monitoramento do ambiente de preservação o RDC-Arq poderá tomar as decisões mais adequadas para realizar a manutenção dos objetos digitais, e minimizar os efeitos da obsolescência. Assim, irá assegurar a que a comunidade designada será capaz de compreender e utilizar os materiais preservados;

- **Ter mecanismos para monitorar e notificar quando a informação de representação está inadequada à compreensão dos dados pela**

comunidade designada: garante que a informação preservada permaneça compreensível e utilizável pela comunidade designada. Tal requisito pode ser evidenciado com a assinatura de um serviço de registo das informações de representação, por meio de pesquisas na comunidade designada, e por de processos relevantes para lidar com esta informação (CCSDS, 2011; ISO 16363:2012). Logo, o RDC-Arq deve manter mecanismos para verificar a obsolescência no que tange a base de conhecimento da comunidade designada. E desta forma, poderá atualizar ou adicionar a informação de representação necessária para garantir a correta interpretação/representação da informação de conteúdo;

c) **Ter mecanismos para mudar o plano de preservação conforme os resultados das atividades de monitoramento**: demonstra que o repositório está preparado para variações no ambiente externo, sendo capaz alterar o curso do seu plano de preservação conforme as informações de monitoramento. Tal requisito pode ser evidenciado através de planos de preservação vinculados ao monitoramento tecnológico; processos de preservação voltados ao curto prazo; documentação que comprove as atualizações frequentes das políticas e planos de preservação; e políticas que definam como os planos podem ser atualizados. Da mesma forma, o repositório pode usar as informações coletadas pelo monitoramento e criar informações de representação adicionais e/ou PDI (CCSDS, 2011; ISO 16363:2012). Com o monitoramento do ambiente de preservação, o RDC-Arq terá condições previstas para alterar o planejamento definido e se adequar aos imprevistos e as novas necessidades que surjam durante a execução do plano de preservação. Da mesma, forma poderá reunir informações adicionais que corroborem com a preservação e interpretação dos objetos digitais;

- **Ter mecanismos para criar, identificar ou reunir qualquer informação de representação adicional que seja necessária**: garante que a informação preservada permaneça compreensível e utilizável pela comunidade designada, evitando a obsolescência. Tal requisito pode ser evidenciado pelo plano de preservação e pela definição de um serviço de registro de formato e de um serviço de monitoramento tecnológico

(CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq identificará a informação de representação e os formatos de arquivo potencialmente obsoletos e, por conseguinte, proceder à atualização ou adicionar maiores informações que auxiliem no processo de preservação;

d) **Apresentar provas da eficácia das atividades de preservação**: assegura que o repositório será capaz de tornar a informação disponível e utilizável à comunidade designada no médio, e no longo prazo. Tal requisito pode ser evidenciado por meio de registros de metadados de preservação, prova de usabilidade[48] dos objetos digitais, e histórico de demonstração para reter objetos digitais utilizáveis no longo prazo (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq demonstrará capacidade de preservação continuada da informação de conteúdo ao permitir auditorias (testes aleatórios) que comprovam a eficácia dos métodos, além de garantir a sua correta representação/interpretação.

4.2.2.4 Preservação do AIP

Preservar as informações de conteúdo dos AIP's requer a implementação de estratégias de preservação documentadas por meio de metadados adequados registrando as ações aplicadas para especificar o seu tratamento. Além disso, o RDC-Arq deve monitorar continuamente a integridade dos AIP's, e manter o registro de ações e processos administrativos pertinentes à preservação.

a) **Ter especificações sobre a forma como os AIP's são armazenados até o nível de *bit***: garante que a informação pode ser extraída a partir do AIP no longo prazo. Tal requisito pode ser evidenciado pela documentação que especifica o formato do AIP. Desta forma, as informações de representação devem especificar os conteúdos de cada componente do AIP até o nível de *bit*, além de especificar como estes componentes são empacotados (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq poderá recuperar as informações

[48] Os objetos são selecionados aleatoriamente e o teste é realizado dentro do próprio sistema.

de conteúdo do AIP devido ao conhecimento sobre os formatos, de modo que poderá extrair a informação contida no AIP em qualquer tempo;

- **Preservar as informações de conteúdo do AIP**: a missão fundamental de um repositório consiste em preservar as informações de conteúdo para suas comunidades designadas. Desta forma, é preciso demonstrar que os AIP's refletem fielmente as informações de conteúdo que foram capturadas durante a admissão e que quaisquer transformações planejadas subsequentes ou futuras continuarão a preservar todas as propriedades das informações requeridas. Logo, é preciso ter uma política especificando que os AIP's não podem ser excluídos a qualquer momento, assim, preservam-se as ligações entre os AIP's que foram admitidos, e as novas versões que tenham sido transformadas ou alteradas posteriormente. Tal requisito pode ser evidenciado com a documentação sobre os procedimentos do fluxo de trabalho, documentação sobre a política de preservação especificando o gerenciamento dos AIP's, e através da capacidade de demonstrar a sequência de conversões realizada sobre um AIP para qualquer objeto digital (CCSDS, 2011; ISO 16363:2012). Com isto o RDC-Arq manterá um registro de todas as transformações realizadas sobre as informações de conteúdo recebidas. Caso sejam necessárias conversões ou informações adicionais, todos estes procedimentos estarão registrados, compondo um testemunho do histórico dos objetos digitais. Logo, este registro irá garantir a autenticidade dos conteúdos em custódia.

- **Monitorar ativamente a integridade do AIP**: protege a integridade dos objetos digitais no longo do tempo. Tal requisito pode ser evidenciado ao se adicionar informações de fixidez para cada objeto digital admitido. Assim, o repositório demonstra que verifica a integridade de forma regular, captura todas as alterações do AIP e realiza ação corretiva o mais breve possível (CCSDS, 2011; ISO 16363:2012). O RDC-Arq manterá um processo regular de verificação da integridade para cada objeto digital admitido e adicionará informações de fixidez, as quais irão auxiliar na

presunção de autenticidade, além de reparar os objetos que estão corrompidos;

b) **Ter registros contemporâneos das ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIP's**: garante que a documentação não é omitida, errónea ou de autenticidade questionável. Tal requisito pode ser evidenciado por meio da documentação de medidas tomadas, metadados de preservação associados aos objetos digitais. Dependendo da natureza das ações descritas, o registro desses dados pode ser realizado de forma automatizada ou por indivíduos (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq deverá demonstrar, através de documentação e registros de metadados, que todas as ações relevantes são realizadas. Tal procedimento agregará confiabilidade às decisões administrativas relacionadas aos AIP's;

- **Ter procedimentos definidos para todas as ações tomadas em um AIP**: assegura que quaisquer ações realizadas sobre um AIP não alteram suas informações de uma forma inaceitável à comunidade designada. Tal requisito pode ser evidenciado por uma documentação formalizada desde o projeto do repositório, que descreva todas as ações que podem ser executadas sobre um AIP, e que também defina processos de monitoramento para estas ações (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq deve respeitar uma variabilidade limitada, a qual é um parâmetro entre as necessidades de alterar as informações de conteúdo e de manter as propriedades significativas. Com isto, a informação de conteúdo poderá sofrer alterações desde que mantenham as propriedades significativas requeridas para manutenção da sua autenticidade. Logo, as transformações realizadas pelo repositório não devem descaracterizar os objetos digitais com relação à sua representação, para isto, deve-se considerar um conjunto de alterações aceitáveis, e registrar todas as ações de alteração;

- **Demonstrar que as medidas tomadas em um AIP estão em conformidade com as especificações dessas ações**: assegura que

quaisquer ações realizadas sobre um AIP não alteram suas informações de forma inaceitável à comunidade designada. Tal requisito pode ser evidenciado por meio de metadados de preservação que estejam registrados e vinculados aos objetos digitais, e sua respectiva documentação sobre as ações realizadas. Assim com, auditorias que demonstram que todas as ações do repositório estão em conformidade com os processos documentados (CCSDS, 2011; ISO 16363:2012). Logo, quaisquer ações que afetem os conteúdos armazenados no RDC-Arq devem seguir procedimentos previamente estabelecidos, além de serem registrados por metadados. Desta forma, é possível demonstrar que as ações registradas pelos metadados estão em conformidade com o que foi definido previamente como “alterações aceitáveis”.

4.2.2.5 Gestão da informação

Na gestão da informação o RDC-Arq captura ou cria os metadados de descrição necessários, e os associa ao AIP, para que a comunidade designada identifique os materiais de interesse. Assim, será capaz de demonstrar que a integridade referencial é criada e mantida entre todos os AIP’s e suas informações descritivas associadas.

a) **Especificar os requisitos mínimos de informação para permitir que a comunidade designada descubra e identifique o material de interesse**: permite a descoberta de materiais no repositório, de modo que seja possível lidar com solicitações da comunidade designada. Tal requisito pode ser evidenciado através de informações descritivas e de recuperação, e demais documentação que descreva os objetos. Assim, os metadados de recuperação localizam os objetos e a informação descritiva irá descrever o que foi encontrado (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq deve acrescentar informações descritivas aos objetos digitais admitidos, de modo a auxiliar no processo de busca e recuperação da informação de conteúdo desejada pela comunidade designada. Logo, ressalta-se a necessidade de definir padrões de metadados assim como um vocabulário controlado para otimizar a precisão das buscas;

b) **Capturar ou criar informação descritiva mínima e assegurar que ela está associada ao AIP**: garante que a informação descritiva está associada ao AIP. Tal requisito pode ser evidenciado por metadados descritivos, identificadores únicos (internos ou externos) para cada AIP, documentação e arquitetura técnica, acordos de depósito, documentação do fluxo de trabalho, política de metadados documentada incorporando detalhes dos requisitos e uma declaração de responsabilidade por sua aquisição. Desta forma, o repositório irá mostrar que associa o mínimo de informação descritiva a cada AIP, sendo que esta associação não deve, necessariamente, ser armazenada com o AIP (CCSDS, 2011; ISO 16363:2012). Logo, o RDC-Arq deverá associar a informação descritiva necessária para cada AIP, esta informação adicional não precisa, necessariamente, estar inserida no pacote de informação. No entanto, é essencial que a informação descritiva esteja relacionada com cada AIP, e poderá atuar por meio de identificadores únicos para estes. Da mesma forma, a informação descritiva poderá fornecer detalhes adicionais relacionados às responsabilidades advindas do processo de admissão de conteúdos, ressalta-se que no caso do RDC-Arq, a descrição seguira os padrões preconizados pela Arquivística;

c) **Manter ligação bidirecional entre cada AIP e sua informação descritiva**: assegura que todos os AIP's podem ser localizados e recuperados. Tal requisito pode ser evidenciado por metadados descritivos, identificador único/localizador associado ao AIP, documentação sobre a relação entre o AIP e seus metadados, documentação do sistema e arquitetura técnica, e documentação do fluxo de trabalho (CCSDS, 2011; ISO 16363:2012). Desta forma, o RDC-Arq deve estabelecer e manter informações descritivas associadas para cada AIP. Com uma relação bidirecional, pode-se localizar a informação descritiva através do AIP, como também, pode-se localizar o AIP a partir da informação descritiva;

- **Manter associação entre o AIP e as suas informações descritivas ao longo do tempo**: assegura que todos os AIP's podem continuar sendo localizados e recuperados. Tal requisito pode ser evidenciado através do

detalhamento da manutenção contínua ou verificação da integridade dos dados e as suas relações com a informação descritiva associada, especialmente após a reparação ou modificação do AIP. Além de outras questões como a documentação do sistema e da arquitetura técnica, documentação dos processos de fluxo de trabalho, registro de informações descritivas, persistência do identificador/localizador, e documentação sobre a relação ente o AIP e sua respectiva informação descritiva (CCSDS, 2011; ISO 16363:2012). De forma geral, o RDC-Arq deve identificar qualquer interrupção entre os dados e a informação descritiva associada, para assim, garantir que ela pode ser restaurada, e com isso, os AIP's poderão ser recuperados.

4.2.2.6 Gestão de acesso

Com a gestão de acesso, o repositório irá documentar e comunicar opções de acesso e entrega que estão disponíveis à comunidade designada. Todas as solicitações de acesso devem são registradas, e visam atender aos requisitos do repositório e dos produtores, além de cumprir os acordos relacionados às condições de acesso. A gestão de acesso irá definir e implementar uma política de acesso segura via sistema de gerenciamento, aos contratos de depósito. Desta forma, irá demonstrar que todas as solicitações de acesso resultam em uma resposta de aceitação ou rejeição, e assim, registrar todas as falhas de gerenciamento de acesso e analisar os casos de negação de acesso.

a) **Cumprir políticas de acesso**: resolver todos os aspectos do uso que podem afetar a confiabilidade do repositório, particularmente, com referência ao suporte à comunidade de usuários. Tal requisito pode ser evidenciado por meio de trilhas de auditoria sobre solicitações de acesso, testes explícitos de alguns tipos de acesso, disponibilização das políticas para as comunidades de usuários, e informações sobre as capacidades dos usuários (matrizes de autenticação). Desta forma, definem-se condições e mecanismos de controle de acesso relacionado à autenticação, autorização e registro de acesso (CCSDS, 2011; ISO 16363:2012). Logo, o RDC-Arq deverá demonstrar que cumpre as políticas de acesso, de modo que atende todas as solicitações da

comunidade designada e mantem mecanismos de autenticação de usuários para controlar o acesso;

- **Registrar e analisar todas as falhas e anomalias de gerenciamento de acesso**: identifica ameaças de segurança e falhas no sistema de gerenciamento de acesso. Tal requisito pode ser evidenciado através da demonstração da capacidade do sistema para usar ferramentas de análise/monitoramento automatizado e gerar mensagens de problema/erro. Além das notas de avaliações realizadas ou medidas tomadas como resultado de comentários. Desta forma, o repositório precisa ter um mecanismo automatizado para rastrear negações anómalas ou incomuns, e usá-las para identificar ameaças ou falhas de segurança no sistema de gestão de acesso (CCSDS, 2011; ISO 16363:2012). Assim, o RDC-Arq irá descobrir todas as falhas relacionadas ao acesso que afetam a sua confiabilidade. Com a identificação das anomalias e vulnerabilidades o repositório poderá concentrar esforços para solucionar estas falhas;

b) **Seguir políticas e procedimentos que permitam a disseminação objetos de digitais os quais sejam rastreáveis aos originais, com evidência de sua autenticidade**: estabelece uma cadeia de autenticidade auditável do AIP para objetos digitais disseminados. Tal requisito pode ser evidenciado com procedimentos de orientação, e por meio de documentação dos requisitos para evidência de autenticidade. As evidencias adequadas são fundamentais para avaliar o grau de autenticidade, demonstrando que os materiais admitidos não perdem informações durante as transformações. Desta forma, devem-se registrar os processos de construção do DIP a partir do AIP, sendo derivado de transformação ou cópia idêntica, mas sempre refletindo o seu conteúdo (CCSDS, 2011; ISO 16363:2012). Com isto, o RDC-Arq deverá gerar pacotes DIP's em conformidade com os AIP's dos quais são derivados. Logo, torna-se fundamental definir procedimentos padronizados para a criação do DIP garantindo a sua fidedignidade frente ao AIP;

- **Registar e agir de acordo com relatórios de problemas sobre erros nos dados ou respostas para usuários**: ser considerado uma fonte de confiança de informação por seus utilizadores. Tal requisito pode ser evidenciado pela documentação sobre o projeto do sistema, e com a documentação dos relatórios de erros e das ações tomadas. Desta forma, estima-se que o usuário irá receber uma versão do objeto digital utilizável em conformidade com o que foi requerido. Caso ocorram quaisquer problemas que sejam levados ao seu conhecimento, estes vão ser investigados e executados. Ressalta-se que essa resposta é essencial para o repositório ser considerado confiável (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá considerar os relatórios de erros sobre as solicitações de acesso. Sendo assim, a sua confiabilidade estará relacionada à capacidade de investigar e tomar decisões com relação a tais erros. Logo, as ações tomadas pelo repositório para solucionar problemas de acesso irão agregar confiança frente à comunidade designada.

4.2.3 Infraestrutura e segurança da gestão de riscos

A seção de infraestrutura e segurança da gestão de riscos compreende aspectos relacionados à infraestrutura técnica do sistema, e gestão de riscos.

4.2.3.1 Gestão de riscos de infraestrutura técnica

As funções de repositório devem ser suportadas pelos principais sistemas operacionais, de modo que seja possível assegurar suporte de *hardware* e *software* adequado às funcionalidades de *backup* e suficientes aos conteúdos armazenados. Assim, é possível gerenciar as quantidades e as localizações das cópias de todos os objetos digitais, e sincronizar as cópias dos objetos digitais. Além disso, o repositório irá detectar a corrupção ou perda de *bits* ao utilizar mecanismos de análise de erro, e informar à administração todos estes incidentes e as medidas adotadas para reparar ou substituir os dados afetados. Os processos de atualização das mídias de armazenamento, do *hardware* e da segurança *software* devem ser definidos, e registrar a gestão de mudanças, sendo necessário um processo para testar o efeito

de mudanças críticas ao sistema. Desta forma, o repositório possuirá tecnologias de *hardware* e *software* apropriadas aos serviços que presta à comunidade designada, bem como, procedimentos para monitorar e avaliar a necessidade de mudanças nas tecnologias de *hardware* e/ou *software* utilizadas.

a) **Identificar e gerir os riscos às suas operações de preservação e os objetivos associados com a infraestrutura do sistema**: garante uma infraestrutura segura e confiável. Tal requisito pode ser evidenciado por inventários de infraestrutura do sistema, avaliações tecnológicas periódicas, estimativas de vida útil dos componentes do sistema, utilização de *softwares* amplamente suportados pela comunidade, e com a recriação de arquivos de *backups*. Desta forma, o repositório deve gerir os riscos relacionados à infraestrutura de *hardware*, *software* e os procedimentos operacionais. Além disso, deve fornecer mecanismos para minimizar a dependência do sistema, mantendo-se capaz de evoluir por meio da substituição de tecnologias sem transtornos ao sistema como um todo. Neste sentido o repositório deve suportar novos formatos, e ser capaz de exportar sua participação a um novo custodiador futuro, além de recriar os materiais após um erro de substituição/exclusão de conteúdos (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá preconizar uma infraestrutura confiável, para isso, irá gerir os riscos relacionados às plataformas de *hardware* e *software*, buscando minimizar a dependência do sistema. Sua infraestrutura tecnológica deve ser expansível, além de possibilitar a execução de um plano de sucessão futuro, caso seja necessário;

- **Empregar relógios de tecnologia ou outra tecnologia para sistemas de notificação de monitoramento**: rastreia quando os componentes de *hardware* ou *software* se tornam obsoletos, o que torna necessária a migração para novas infraestruturas. Tal requisito pode ser evidenciado pela gestão periódica dos relatórios de avaliação da tecnologia, e por meio da comparação da tecnologia existente a cada nova avaliação. Desta forma, é possível identificar os riscos de obsolescência, permitindo a migração para novas tecnologias (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve manter um monitoramento contínuo das plataformas

tecnológicas, acompanhado de avaliação para identificar potenciais vulnerabilidades nos componentes do sistema;

- **Ter tecnologias de *hardware* adequadas aos serviços que presta para sua comunidade designada**: facilita a admissão e a difusão por meio de interfaces apropriadas, além do gerenciamento dos objetos digitais, soluções de preservação (como a migração) e segurança do sistema. Tal requisito pode ser evidenciado pelo o fornecimento de largura de banda suficiente para suportar a admissão e uso de demandas; análise sistemática do *hardware* e adequação do serviço conforme *feedback* recebido, e manutenção de inventário do *hardware* atual. O repositório deve estar ciente de questões relacionadas ao armazenamento, gestão de dados, preservação e dos serviços que presta a sua comunidade designada, considerando inclusive a mídia na qual os conteúdos são disponibilizados o *hardware* disponível. Desta forma, objetiva-se controlar as mudanças nas exigências dos serviços prestados, em especial, com relação às tecnologias de *hardware* e políticas de admissão ao exigirem novas capacidades (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá manter plataformas de *hardware* adequadas para os serviços que presta, e considerar o *feedback* recebido par realizar ajustes no sistema. Além disso, deve-se ressaltar que a adequação dos componentes de *hardware* irá impactar em todas as funções do repositório;

- **Dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças na tecnologia de *hardware***: garante que os níveis de serviço contratados são seguros e mantém conformidade com o esperado. Tal requisito pode ser evidenciado através de auditorias sobre as taxas de erro observadas e a capacidade *versus* uso real, documentação das avaliações de monitoramento tecnológico e das atualizações tecnológicas dos fornecedores. Desta forma, os componentes de *hardware* devem ser monitorados constantemente, verificando suas possíveis vulnerabilidades assim como os níveis de interoperabilidade com o

repositório. Logo, o objetivo consiste em controlar as mudanças de *hardware* necessárias aos procedimentos de admissão, preservação e acesso (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá monitorar as mudanças nas plataformas de *hardware* a fim manter uma infraestrutura capaz de realizar suas funções relativas a admissão, armazenamento e acesso. O ponto fundamental deste requisito é manter a interoperabilidade entre a plataforma de *hardware* e as funções executadas pelo repositório para desenvolvê-las conforme o esperado;

- **Dispor de procedimentos para avaliar quando é necessário atualizar o *hardware* atual**: garante que o repositório tenha a capacidade de tomar decisões atempadas, quando houver informação indicando a necessidade de um novo *hardware*. Tal requisito pode ser evidenciado por meio da avaliação de processos, e ao documentar a experiência da equipe em cada subsistema de tecnologia. Desta forma, o repositório deve ter conhecimentos para avaliar a necessidade de um novo *hardware*, monitorando o desenvolvimento de sistemas que minimizem riscos/custos e melhorem o desempenho do sistema (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá antecipar as atualizações de *hardware*, ao manter um constante monitoramento do sistema, verificando meios para reduzir custos e falhas;

- **Ter procedimentos, compromissos e financiamentos para substituir *hardware* quando a avaliação indicar tal necessidade**: garante a substituição de *hardware* em tempo hábil, evitando a falha do sistema ou insuficiência de desempenho. Ressalta-se que o repositório deve ter mecanismos de avaliação de eficácia dos novos sistemas antes da implementação no sistema de produção. Tal requisito pode ser evidenciado através de ativos financeiros reservados para aquisição de *hardware*, e da demonstração de economia de recursos por meio do custo amortizado por um novo sistema. Desta forma, o repositório demonstra que tem capacidade de

incorporar novas tecnologias, assim como possui recursos financeiros para tal, e que avalia as capacidades dos novos sistemas (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve realizar a substituição do *hardware* logo após identificar tal necessidade. Sendo assim, deve haver o compromisso da instituição, de modo que o RDC-Arq disponha de recursos financeiros suficientes, como também poderá demonstrar que o novo *hardware* será capaz de economizar recursos no decorrer de seu uso;

- **Ter tecnologias de *software* apropriadas para os serviços que proporciona a sua comunidade designada**: fornece níveis de serviço seguros incluindo: facilidade de admissão e difusão pelos depositantes e usuário; interfaces apropriadas e tecnologias como mecanismos de carregamento; gerenciamento de objetos digital; soluções de preservação, como a migração; e segurança do sistema. Tal requisito pode ser evidenciado pelo fornecimento de sistemas de *software* adequados para apoiar a admissão e as demandas de uso; incentivar uma sistemática de *feedback* com relação ao *software* e à adequação do serviço; manutenção de um inventário de *software* atual. Desta forma, tem-se por objetivo controlar quando as mudanças nas exigências de serviços da comunidade designada exigem uma mudança correspondente nos componentes de *software*, quando as alterações nas políticas de admissão requerem suporte para novos formatos de dados e quando as alterações na tecnologia de *software* requerem novas capacidades para migração de formato. Isto pode ser conduzido por alterações nos requisitos de acesso, por mudanças nos mecanismos de entrega, e alterações no número e tamanho dos registros arquivados que requerem *software* mais escalável (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve manter as tecnologias de *software* apropriadas para desempenhar as funções como interfaces e ferramentas para migração. Logo, é preciso considerar, em especial, o *feedback* da comunidade designada em relação aos *softwares* utilizados para a localização e recuperação/interpretação da informação de conteúdo;

- **Dispor de procedimentos para monitorar e receber notificações quando alterações de *software* são necessários**: garante que os níveis de serviço contratados são seguros e mantém conformidade com o esperado. Tal requisito pode ser evidenciado por auditorias da capacidade *versus* o uso real, auditorias de taxas de erro observado, auditorias de desempenho relacionado aos limites da capacidade para atender aos requisitos de acesso da comunidade de usuários, e documentação das avaliações de monitoramento tecnológico, inclusive das atualizações de *software* dos fornecedores. Desta forma, busca-se controlar as mudanças exigidas nos serviços por parte da comunidade designada em virtude de uma mudança correspondente na tecnologia de *software*, em especial quando houver alterações nas políticas de admissão bem como a exigência de capacidades expandidas de preservação. Assim, o repositório deve monitorar a evolução do *software* e suas vulnerabilidades, bem como a interoperabilidade com o *hardware* (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá ter procedimentos pré-estabelecidos para verificar erros, vulnerabilidades e buscar atualizações para os *softwares* que integram o sistema de preservação digital. Além disso, é preciso atender a mudanças solicitadas pela comunidade designada para facilitar o processo de busca, recuperação e interpretação dos conteúdos. E por fim, buscar a interoperabilidade entre as plataformas de *hardware* e *software*;

- **Dispor de procedimentos para avaliar a necessidade de atualização do *software* atual**: ter capacidade de tomar decisões antecipadas quando houver necessidade de um novo *software*. Tal requisito pode ser evidenciado com procedimentos de avaliação, e documentação que comprove a experiência da equipe em cada tecnologia do subsistema. Desta forma, o repositório coletará informação de monitoramento, logo, deverá ter procedimentos estabelecidos e conhecimentos para avaliar esses dados e tomar decisões sobre a necessidade de um novo *software*. O monitoramento da tecnologia minimizará os riscos e os custos, além de melhorar o

desempenho do sistema. A avaliação deve identificar quando o risco de usar a nova tecnologia supera o benefício esperado, e quando a nova tecnologia é suficientemente sedimentada para minimizar o risco (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve antecipar a necessidade de atualização de *software* ao monitorar a evolução das plataformas tecnológicas. Tal ação irá minimizar riscos, evitar custos adicionais e melhorar o desempenho do sistema. Este procedimento previamente estabelecido fundamenta-se em evitar que os *softwares* utilizados no sistema tornem-se obsoletos e comprometam as atividades desenvolvidas no âmbito do repositório;

- **Ter procedimentos, definir compromissos e garantir financiamentos para substituir o *software* quando a avaliação indica tal necessidade**: garante a substituição do *software* em tempo hábil, de modo a evitar falhas do sistema ou insuficiência de desempenho. Logo, o repositório deve ter mecanismos para avaliação da eficácia dos novos sistemas antes da implementação no sistema de produção. Tal requisito pode ser evidenciado por uma declaração de compromisso em fornecer os níveis de serviço esperados no contrato, demonstração de ativos financeiros reservados para aquisição de *software*, demonstração de economia de recursos através do custo amortizado pelo novo sistema. Desta forma, demonstra-se a capacidade para incorporar novas tecnologias, tanto financeiramente, quanto operacionalmente, visto que há recursos financeiros e capacidade de incorporação de novos sistemas (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deverá substituir o *software* de modo a evitar falhas e consequentes perdas de dados. Assim, deve-se demonstrar a capacidade e os recursos suficientes para incorporar novas tecnologias;

- **Ter *hardware* adequado e suporte de *software* suficiente para realização do *backup* para proteger os conteúdos do repositório e acompanhar suas funções de preservação**: garante o acesso contínuo aos objetos digitais em custódia, e acompanha as funções de preservação

aplicadas. Tal requisito pode ser evidenciado através de documentação comprovando a realização do *backup*, inventário de *backups*, validação de *backups* concluídos, plano para recuperação de desastres, testes de *backups*, contratos de suporte de *hardware* e *software* para *backup*, preservação dos metadados do sistema, tais como controles de acesso, localização de cópias, trilhas de auditoria, verificação em *checksum*. Desta forma, demonstra-se a adequação dos processos, do *hardware* e do *software* aos sistemas de *backup*, assim como toda a gama das funções de admissão, preservação e disseminação, necessárias em um repositório confiável para preservação em longo prazo. Logo, mecanismos simples de *backup* devem preservar não apenas o conteúdo principal repositório, mas também o sistema metadados gerados pelas funções de preservação. O repositório precisa desenvolver planos de *backup* para garantir a continuidade de suas operações em todas as situações de falha (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve possuir plataformas de *hardware* e *software* capazes de realizar o *backup* dos objetos digitais e dos sistemas. Com o desenvolvimento de planos de backup será possível retomar as funções de preservação em todas as situações que ocorrerem falhas, independente do nível (objetos digitais, mídias de armazenamento, *hardwares* ou *softwares*);

- **Ter mecanismos eficazes para detectar a corrupção ou perda de *bits***: assegura que o AIP e os metadados estão em conformidade com as políticas definidas pelo repositório, logo, não devem estar corrompidos e não há perdas de dados detectadas. Tal requisito pode ser evidenciado com a documentação que especifica os mecanismos de detecção de erro nos *bits* e de correções utilizadas, análises de riscos, relatórios de erros, e análise periódica da integridade dos conteúdos do repositório. Desta forma, objetivo consiste em tratar, em sua essência, as causas das perdas de dados. Logo, qualquer dado perdido deve ser recuperado pelo procedimento de *backup*. As falhas sistemáticas não devem ser acumuladas, isto garante um nível tolerável de perda de dados definido nas políticas (o qual pode ser restaurado com o *backup*). Para tal, podem-se usar mecanismos como assinaturas digitais e *checksums* para detectar

as perdas de bits e auxiliar na validação da integridade do repositório (CCSDS, 2011; ISO 16363:2012). O RDC-Arq não deve tolerar perdas de dados em seus AIP e informações relacionadas. Para isto, deverá manter mecanismos que identifiquem as possíveis perdas ou corrupção de dados e executem a restauração;

- **Registrar e reportar à administração, todos os incidentes de corrupção ou perda de dados, e quais medidas de reparo/substituição de dados corrompidos/perdidos, deverão ser tomadas**: garante que a administração do repositório está sendo informada sobre incidentes e ações de recuperação, da mesma forma, permite a identificação das fontes de corrupção ou perda de dados. Tal requisito pode ser evidenciado com procedimentos de notificação de incidentes aos administradores, registros de metadados de preservação, relatórios de erros, rastreamento das fontes de incidentes, e ações corretivas tomadas para eliminar as fontes de incidentes. Desta forma, com mecanismos eficazes é possível detectar a corrupção dos *bits* dentro do repositório. Além do registro e reparação dos danos à integridade, deve-se comunicar os incidentes à administração, possibilitando revisões sistemas de *software* e *hardware* ou políticas e procedimentos, para minimizar tais vulnerabilidades relatadas (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve informar à administração sobre as perdas de dados e o respectivo processo de recuperação executado. Com isto, é possível identificar as fontes de falhas e reparar as vulnerabilidades em nível de *hardware*, *software*, suportes e procedimentos;

- **Ter um processo para registrar a disponibilidade de novas atualizações de segurança com base na avaliação do risco/benefício**: protege a integridade dos objetos armazenados, não autorizando alterações ou exclusões. Tal requisito pode ser evidenciado através do registro de riscos, evidência de processos de atualização, e documentação relacionada à instalação de atualizações. As decisões para aplicar atualizações de segurança são resultado da avaliação do risco/benefício.

Cada atualização de segurança, automática ou manual, considerada necessária, deve ser documentada quando concluída. Ressalta-se que as atualizações de segurança não se limitam ao nível de *software* (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve evitar as alterações e exclusões de conteúdos não autorizadas. Além disso, deve realizar atualizações de segurança em sua infraestrutura tecnológica para minimizar os riscos;

- **Definir processos para a mídia de armazenamento e/ou alteração de *hardware***: assegura que os dados não serão perdidos quando houver falha em ambos os meios de comunicação, ou quando o suporte ao *hardware* não puder mais ser usado para acessar os dados. Tal requisito pode ser evidenciado pela documentação dos processos de migração, políticas relacionadas ao suporte (manutenção e substituição) de *hardware*, documentação de ciclos de vida de suporte esperados do fabricante de *hardware*. Assim, o repositório deve ter estimativas da velocidade de acesso e a quantidade de informações para cada tipo de mídia de armazenamento. Da mesma forma, deverá ter estimativas de vida útil confiável das mídias de armazenamento, e estimar o tempo necessário para a migração ou refrescamento da mídia de armazenamento. Além disso, deve-se considerar a obsolescência em todos os componentes de *hardware* dentro do sistema de repositório como potenciais eventos para proceder à migração (CCSDS, 2011; ISO 16363:2012). É fundamental que o RDC-Arq mantenha um processo de migração para as mídias de armazenamento com base nas estimativas de vida útil e análise de conservação física. Ressalta-se que no longo prazo, há maior dificuldade em se obter suporte aos componentes de *hardware*, o que aumenta a responsabilidade do RDC-Arq em buscar alternativas;

- **Identificar e documentar os processos críticos que afetam a capacidade de cumprir as responsabilidades obrigatórias**: assegurar que os processos críticos podem ser controlados para cumprir as responsabilidades obrigatórias, além de examinar e testar quaisquer alterações aos processos. Tal requisito pode ser evidenciado através da matriz de rastreabilidade entre os processos e os requisitos obrigatórios.

Entre estes processos críticos, incluem-se o gerenciamento de dados, o acesso, o armazenamento de arquivo, a admissão, e os demais processos de segurança. Já a rastreabilidade torna possível compreender os processos necessários para atender cada uma das responsabilidades obrigatórias (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve ter um controle sobre todos os processos críticos que podem afetar suas responsabilidades obrigatórias, de modo seja possível compreender a necessidade destes fluxos de informação. Assim, é possível manter uma revisão buscando a melhora contínua destes procedimentos;

- **Ter um processo de gestão da mudança documentado, que identifica as alterações em processos críticos, os quais afetam potencialmente a capacidade do repositório para cumprir suas responsabilidades obrigatórias**: assegura a capacidade de especificar, não só os processos atuais, mas também os processos anteriores que foram aplicados ao acervo. Tal requisito pode ser evidenciado pela documentação sobre a avaliação do risco associado ao processo de alteração, e sobre a análise do impacto esperado em um processo de mudança. Entre estes processos de mudança, incluem-se o gerenciamento de dados, o acesso, o armazenamento de arquivo, a admissão, e os demais processos de segurança. Logo, devem-se saber, essencialmente, quais e quando as mudanças foram realizadas. Já a rastreabilidade torna possível compreender como são efetuadas as alterações no sistema. Com este registro é possível reverter alterações ou pelo menos documentar as alterações que foram realizadas (CCSDS, 2011; ISO 16363:2012). O repositório deverá ter especificações sobre os processos aplicados ao acervo relacionados às mudanças em seus processos críticos. Desta forma, é possível compreender como as mudanças foram efetuadas no sistema, e consequentemente, aprender com as mudanças. E caso seja necessário, será possível reverter ações que comprometam as atividades do RDC-Arq;

- **Ter um processo para testar e avaliar o efeito das mudanças em seus processos críticos**: protege a integridade dos processos críticos do repositório para manter a sua capacidade de atender aos requisitos obrigatórios. Tal requisito pode ser evidenciado através de documentação de procedimentos de teste, documentação que comprove alterações realizadas com base nos testes anteriores, e análise do impacto de uma mudança de processo. Desta forma, as alterações críticas nos sistemas devem ser testadas previamente e separadamente. Após as alterações, os sistemas devem ser monitorados para identificar um possível comportamento inesperado e inaceitável. Caso tal comportamento seja descoberto, as mudanças devem ser revertidas. Assim, testes de todo o sistema ou testes de unidade podem atender a esse requisito (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve avaliar as mudanças em seus processos críticos. Isto se torna essencial, pois estes processos se referem às funções primordiais que ele executa. Assim, as alterações devem ser testadas antes de sua implementação, após implementar devem ser monitoradas e caso seja necessário devem ser revertidas;

b) **Gerir o número e a localização das cópias de todos digitais objetos**: afirma que o repositório fornece uma cópia autêntica de um determinado objeto digital. Tal requisito pode ser evidenciado por testes de recuperação aleatória, validação da existência de objeto para cada local registado, validação de um local registrado para cada objeto no sistema de armazenamento, verificação da informação de proveniência e fixidez. Desta forma, o repositório pode ter diferentes políticas de preservação para diferentes classes de objetos, motivadas pelo seu produtor, tipo de informação custodiada, ou mesmo valor. Pode existir um número diferente de cópias para cada classe, assim como requisitos de identificação adicionais caso seja necessário usar as cópias alternativas para substituição. Também descrever a localização dos objetos com precisão, seja no nível físico, dentro da mídia de armazenamento, no sistema ou em um subsistema. As informações de proveniência devem ser mantidas/atualizadas a fim de controlar a cadeia de custódia e garantir que

as cópias fornecidas pelo repositório, de um determinado objeto, são autênticas (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve ser capaz de gerir seus *backups*, de modo que consiga localizar as cópias de segurança de todos os objetos digitais custodiados. Esta localização deverá ser descrita com elevado grau de precisão, e assim considerar a localização física, o armazenamento lógico na mídia, nos sistemas e nos subsistemas;

- **Ter mecanismos para garantir que todas as cópias dos objetos digitais são sincronizadas**: assegura que as cópias múltiplas de um objeto digital permanecem idênticas, dentro de um tempo aceitável conforme estabelecido pelo repositório, e que uma cópia pode ser utilizada para substituir uma versão do objeto corrompido. Tal requisito pode ser evidenciado por fluxos de trabalho de sincronização, análise do tempo que o sistema requer para sincronizar as cópias, procedimentos documentados sobre os processos de sincronização. No caso do plano de recuperação de desastres, este deve abordar o que fazer se um desastre e uma atualização coincidirem. Os mecanismos para sincronizar as cópias devem ser capazes de detectar a corrupção dos *bits* e verificar a fixidez antes de realizar a sincronização (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve garantir que possui cópias sincronizadas de todos os objetos digitais, para os casos em que seja necessário executar o plano para recuperação de desastres. Isto é fundamental para garantir a proteção do acervo contra sinistros e corrupções de dados, da mesma forma, o repositório deve identificar e reparar os dados corrompidos para que estes não sejam indevidamente sincronizados na forma de cópias de *backup*, ocasionando um grave erro no sistema.

4.2.3.2 Gestão do risco de segurança

A gestão do risco de segurança auxilia o repositório a manter uma análise sistemática em relação a dados, sistemas, pessoal, planta física e segurança. O repositório determina funções, responsabilidades e autorizações relacionadas à implementação de mudanças no sistema, além de ter um plano de preparo e recuperação de desastres.

a) **Manter uma análise sistemática dos fatores de risco da segurança associada a dados, sistemas, pessoal e instalações físicas**: garante um serviço contínuo e ininterrupto à comunidade designada. Tal requisito pode ser evidenciado pela análise de riscos. Com isto, é possível avaliar os riscos regularmente e manter a segurança adequada em conformidade com os níveis de serviços contratados, que pode fazer uso da ISO/IEC 27000:2009[49] *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Neste sentido, é preciso definir sistemas de proteção contra incêndios e detecção de inundação, e os meios para avaliar a equipe, os procedimentos de gestão e de administração, os recursos, bem como a prestação de serviços. Um treinamento interno e uma avaliação externa devem ser realizados para mensurar a qualidade dos serviços e a pertinência aos usuários da comunidade atendida. Já a realização de auditorias financeiras periódicas devem averiguar questões éticas, as práticas jurídicas e manutenção de recursos operacionais necessários, incluindo a perda de receita. Outra questão pertinente é o direito de propriedade intelectual, o qual deve ser revisado constantemente. De uma forma geral, a avaliação de riscos do repositório pode ser realizada com o auxílio de ferramentas como o DRAMBORA (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve manter uma análise contínua dos riscos relacionados ao ambiente de preservação como um todo. Isto compreende a segurança física e lógica dos dados, e sua relação com sistemas, pessoal e instalações físicas;

b) **Implementar controles para tratar adequadamente cada um dos os riscos de segurança definidos**: assegura que os controles satisfazem as necessidades da segurança do repositório. Tal requisito pode ser evidenciado através da conformidade com a ISO/IEC 27000:2009 (atualmente ISO/IEC

[49] Atualmente revisada e equivalente à ISO/IEC 27000:2018. Padrão aplicável a todos os tipos e tamanhos de organização, que fornece um modelo a seguir na configuração e operação de um sistema de gerenciamento. Este modelo incorpora características que os especialistas definiram em consenso como sendo o estado da arte internacional. Desta forma, as organizações podem desenvolver e implementar uma estrutura para gerenciar a segurança de seus ativos de informações, incluindo informações financeiras, propriedade intelectual, detalhes dos funcionários, e ainda, informações confiadas a eles por clientes ou terceiros (ISO/IEC 27000:2018).

27000:2018), um sistema de listas de controle, análises de riscos, por meio de controles de detecção e avaliação permanente do risco, e ainda, pela conformidade com a ISO/IEC 17799:2005[50] *Information technology – Security techniques – Code of practice for information security management*. Desta forma, é possível demonstrar como se tem lidado com os requisitos de segurança. O repositório também poderá guardar a informação de ataques à sua segurança, descrevendo os procedimentos tomados para possíveis ações futuras, assim como para evitar ocorrências semelhantes. Outra questão pertinente é a realização periódica de testes, atualizações e revisões dos planos de emergência (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve tratar cada um dos riscos identificados, para isto, pode usar normas como a ISO/IEC 27000:2018 e a ISO/IEC 17799:2005. Da mesma forma, pode-se manter um registro de problemas relacionados a ataques para prevenir sua recorrência e revisar constantemente os planos de emergência;

c) **Definir papéis, responsabilidades e autorizações relacionadas com a implementação de mudanças no sistema**: assegura que os indivíduos têm a autoridade e recursos adequados para implementar alterações, além de especificar quais indivíduos serão responsáveis pela implementação de determinada mudança. Tal requisito pode ser evidenciado com o uso da norma ISO/IEC 27000:2018, por meio de organogramas, documentação relativa a autorizações do sistema, e certificação com a norma ISO/IEC 17799:2005. Desta forma, as autorizações justificadas devem definir as permissões dos indivíduos, dentre elas, adicionar usuários, alteração de metadados e/ou acessar trilhas de auditoria (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve atribuir as responsabilidades e recursos para implementar mudanças no ambiente. Neste sentido, as normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir, respectivamente, na atribuição de responsabilidades e posterior certificação;

[50] Padrão que estabelece as diretrizes e os princípios gerais para implementar, manter e melhorar o gerenciamento de segurança da informação em uma organização. Fornece orientações gerais sobre controles em áreas de gerenciamento de segurança da informação. Seus objetivos e controles devem ser implementados para atender aos requisitos identificados por uma avaliação de risco. Assim, destina-se a ser uma base comum de orientações práticas para o desenvolvimento de padrões de segurança organizacionais e práticas efetivas de gerenciamento de segurança para ajudar a criar confiança nas atividades interorganizacionais (ISO/IEC 17799:2005).

d) **Ter uma preparação adequada para desastres e um plano de recuperação documentado, incluindo pelo menos um *backup off-site*[51] de todas as informações preservadas, juntamente com uma cópia do plano de recuperação, fora do local de armazenamento**: garante que as capacidades de *backup* e restauração são suficientes para preservação contínua, para acesso aos sistemas e ao conteúdo, com interrupção limitada dos serviços. Tal requisito pode ser evidenciado através da conformidade com a norma ISO/IEC 27000:2018, de planos de recuperação de desastres, comprovante de existência de uma cópia de *backup off-site* de todas as informações, plano de continuidade dos serviços, documentação definindo as atividades, avaliações geológicas, geográficas ou meteorológicas sobre o local, e certificação da norma ISO/IEC 17799:2005. O nível de detalhamento do plano de desastre, e os riscos específicos contemplados precisam ser adequados aos riscos que repositório está sujeito (CCSDS, 2011; ISO 16363:2012). O RDC-Arq deve manter o *backup* e uma cópia do plano de recuperação em um local seguro e separado do acervo, de modo a garantir a continuidade dos serviços do repositório. As normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir para minimizar os riscos do ambiente de preservação. Além disso, o repositório deve definir claramente o seu plano de desastres, considerando todos os riscos aos quais está sujeito. Desta forma, o plano de recuperação se tornará mais eficaz, caso seja necessário executá-lo.

Um repositório digital deverá realizar uma série de procedimentos previstos na auditoria, para demonstrar os níveis de confiabilidade. Posteriormente, a certificação toma como base os dados obtidos no processo de auditoria para definir se o repositório atingiu os níveis de confiança esperados, e para que assim seja certificado com um “repositório digital confiável”.

Conforme observado no decorrer deste estudo, e considerando o documento das “Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis – RDC-Arq”, elaborado pelo Conarq, o qual recomenda proceder às atividades de

[51] Cópia de segurança realizada em local geograficamente separado do acervo.

auditoria e certificação de repositório digitais confiáveis com base na ISO 16363:2012. Pode-se observar que este é o padrão mais completo se comparado aos seus "equivalentes" e pode ser complementado com outras normas ISO, e com o DRAMBORA com relação à gestão de riscos e segurança do sistema. Desta forma, o ACTDR – ISO 16363:2012 se configura como a principal ferramenta para auditar repositórios digitais em conformidade com o modelo de referência OAIS – ISO 14721:2012, além disso, o ACTDR prepara os repositórios digitais para uma posterior certificação.

4.3 RDC-ARQ, OAIS E ACTDR: UMA CONVERGÊNCIA

A literatura técnica da preservação digital perpassa questões essenciais como as estratégias, os repositórios, a custódia confiável, e a auditoria e certificação de repositórios digitais. Logo, existe a necessidade de aproximar essas abordagens da Arquivística, a qual está inserida em um contexto de reformulação epistemológica e pragmática. A documentação em ambiente digital catalisa um processo de (re)definição de princípios teórico-práticos, e assim, reforça a quebra do paradigma arquivístico, essencialmente analógico e custodial.

As transformações sobre os registros contemporâneos refletem diretamente na concepção de patrimônio, incorporando agora, o patrimônio em ambiente digital. Desta forma, surge a necessidade de preservar documentos arquivísticos digitais que serão as principais fontes de pesquisa e informação do futuro.

> Estamos na era do primitivismo digital. Tudo que fazemos agora terá um impacto nos registros que serão acessados no futuro. Porém, parte dessa história corre o perigo de se perder em sequências de *bits*, estruturadas em *bytes* sem leitura no futuro. É a obsolescência tecnológica. Para cuidar dela, usamos técnicas de preservação digital que poderão, daqui a alguns anos, ajudar nossos descendentes a entenderem os dias de hoje (LUZ, 2015, p.19).

A fragilidade dos documentos arquivísticos em ambiente digital implica na necessidade de implementar sistemas informatizados que contemplem desde a produção documental; perpassando a destinação final; a preservação de longo prazo; e promovendo o acesso contínuo aos conteúdos preservados.

Inicialmente, a implementação de um sistema informatizado para gestão de documentos arquivísticos digitais irá envolver a conformidade com leis, decretos,

portarias, resoluções do Conarq, diretrizes do INTERPARES, normas ISO, e a conformidade com o *Model Requirements for the Management of Electronic Records* (MoReq) (KANTORSKI; KROTH, 2015). Ressalta-se que o MoReq tem por objetivo fornecer um conjunto de requisitos abrangente e simples, que seja de fácil compreensão, voltado para um sistema de registros, que será adaptável e aplicável à atividades de negócios, setores industriais e diversos tipos de organizações. O MoReq define um conjunto comum de serviços básicos que são compartilhados por diferentes tipos de sistema de registros, mas que também são modulares e flexíveis, possibilitando a sua incorporação em aplicativos especializados e dedicados, os quais podem não ter sido previamente reconhecidos como sistemas de registros (DLM, 2010).

Com o auxílio dos sistemas informatizados é possível monitorar e tratar a documentação desde o momento da sua produção ou captura, de modo que o seu ciclo de vida seja constantemente monitorado. Com isto, é possível intervir quando necessário, com o intuito de garantir a manutenção da autenticidade e acesso em longo prazo.

As atividades de preservação devem ser consideradas antes mesmo da produção dos documentos, pois não há como prever, evitar e nem é possível ignorar os avanços das tecnologias da informação. Entretanto, sabe-se que todas as tecnologias contemporâneas se tornarão obsoletas, e se não houver intervenções humanas, as informações serão perdidas com o tempo (SANTOS; FLORES, 2017).

A preservação de documentos arquivísticos em ambientes digitais envolve a interoperabilidade entre os sistemas informatizados para gestão, preservação e acesso. Logo, será necessário envolver todo o ciclo de vida documental em uma linha de custódia ininterrupta. Desta forma, é possível monitorar todas as alterações e tramitações, para registrar os eventos pertinentes.

Após cumprir o respectivo prazo de guarda, os documentos armazenados nos sistemas de gestão serão submetidos ao processo de avaliação. Parte destes documentos será eliminada, e outra parte, dotada de valor permanente, será transferida/recolhida ao RDC-Arq.

O RDC-Arq será o ambiente confiável para preservação de longo prazo, onde será realizada a maior parte das atividades de preservação digital. No entanto, é preciso comprovar que o RDC-Arq cumpre os requisitos arquivísticos, bem como os relacionados à confiabilidade. Além disto, será preciso estabelecer a

interoperabilidade entre os sistemas para gestão e preservação, respectivamente SIGAD e RDC-Arq. A relação entre SIGAD e RDC-Arq, bem como o controle sobre os seus fluxos de informações será capaz de manter uma cadeia de custódia confiável.

> O lugar para a perspectiva custodial tem finalidades específicas: manter o vínculo arquivístico entre os documentos, isto é, assegurar a sua preservação em um conjunto, e garantir a sua segurança, de modo que possam ser acessados e utilizados como documentos autênticos, seja para fins de prova ou de referência (SILVA, 2016, p. 22).

Logo, é possível implementar um ambiente de preservação confiável, para isto, deve-se estabelecer uma cadeia de custódia ininterrupta na relação entre o SIGAD e o RDC-Arq, e considerar: os modelos e-Arq, MoReq e OAIS, os princípios arquivísticos (proveniência, autenticidade, organicidade e unicidade), o padrão de auditoria ACTDR, a legislação vigente, as diretrizes do Conarq, os estudos pertinentes sobre o tema, e as demais normas ISO relacionadas à informação e documentação. Posteriormente, a plataforma de acesso surge como um complemento ao sistema de preservação, que irá fornecer meios para o atingimento dos objetivos de um sistema de arquivo: preservar e garantir acesso em longo prazo.

A oferta de informação é responsável por criar a demanda, pois o consumidor desconhece os conteúdos armazenados nos acervos. Logo, o consumidor não sabe exatamente o que deseja, entretanto, ele conhece, com alguma lucidez, a informação que necessita (BARRETO, 2009). Desta forma, ressalta-se que as plataformas de acesso devem facilitar o acesso aos usuários, de modo que tenham diversas opções para delimitação da pesquisa. Compete ao RDC-Arq disponibilizar instrumentos de pesquisa e mecanismos que facilitem o acesso à informação para sua comunidade designada, que é respectivamente, todos os usuários potenciais.

Nesse contexto de transição do paradigma arquivístico, e considerando o cenário brasileiro, este estudo tem como produto um "**manual para auditoria de repositórios arquivísticos digitais confiáveis**". Esse manual realça aspectos consagrados em outros estudos como: Câmara Técnica de Documentos Eletrônicos – Brasil (2015), CCSDS (2011, 2012), SAAI – ABNT/NBR 15472:2007, OAIS – ISO 14721:2012 e ACTDR – ISO 16363:2012.

O manual fornece subsídios teóricos para facilitar a compreensão do processo de auditoria por parte dos profissionais de arquivo, e consequentemente,

prepara o repositório para o processo de certificação. Para isto, é perpassada a relação entre OAIS, ACTDR e a cadeia de custódia arquivística, a fim de demonstrar a relação entre as normas no âmbito do ciclo de vida dos documentos. Assim se faz necessário, pois o OAIS e o ACTDR são orientados genericamente para "repositórios digitais", logo, se tornam necessárias adaptações que os coloque no contexto dos arquivos. Isto porque o OAIS e o ACTDR possuem uma linguagem direcionada aos profissionais da informática e aos administradores do repositório.

Compreender estas necessidades é essencial para definir um sistema de arquivos, além de promover um diálogo interdisciplinar. Sendo assim, o manual encontra-se no "Apêndice B – Manual para auditoria de RDC-Arq's" o qual apresenta uma síntese das necessidades de um arquivo digital em busca da confiabilidade e consequente certificação.

Por fim, este capítulo verificou a conformidade do OAIS com os princípios da Arquivística com ênfase nas sete funções tradicionalmente preconizadas por Rousseau e Couture; discutiu a pertinencia dos critério do ACTDR para auditoria de RDC-Arq's; e apresentou o produto deste estudo, o manual para auditoria de RDC-Arq's, localizado no "Apendice B". A seguir, o capítulo "conclusão" faz uma retomada dos objetivos propostos a fim de ressaltar os atingimentos e fazer apontamentos gerais sobre a temática discutida.

5 CONCLUSÃO

O *corpus* teórico da preservação digital vem agregando novas práticas recomendadas, e muito disto se deve aos avanços na área das tecnologias da informação e às discussões realizadas no âmbito da comunidade de preservação. As atividades que antes eram orientadas exclusivamente às estratégias, como por exemplo, emulação, migração e refrescamento, agora são orientadas aos sistemas para gestão e preservação de documentos. Tal mudança surge em torno da necessidade de agregar confiança aos documentos custodiados, para isto, os sistemas informatizados e as políticas de preservação digital são peças-chave para garantir o acesso em longo prazo a documentos arquivísticos autênticos.

Entretanto, a implementação de um RDC-Arq requer ir além da conformidade do repositório digital com o modelo OAIS. A rápida evolução das tecnologias da informação e comunicação, aliada ao surgimento de documentos complexos trouxe significativos desafios quanto à preservação dos documentos digitais. Desta forma, ressalta-se que é preciso auditar e certificar os repositórios digitais a fim de adicionar confiabilidade aos registros custodiados.

A análise do modelo funcional OAIS perpassou aspectos relacionados aos conceitos básicos, responsabilidades, entidades funcionais e as estruturas dos objetos de informação. Embora não haja claras menções à Arquivística, ao ser analisado na perspectiva das sete funções propostas por Rousseau e Couture (1998), o OAIS demonstra conformidade com os pressupostos teóricos tradicionais, e de certa forma, preenche lacunas teóricas, notavelmente criadas pelo advento do documento arquivístico digital.

Estas lacunas se relacionam ao próprio ambiente digital visto que os referenciais tradicionais da Arquivística eram orientados aos documentos em suportes analógicos. Assim, com o modelo OAIS é possível identificar um tratamento adequando para documentos arquivísticos digitais, visto que possui conceitos bem formulados e que refletem as definições da comunidade de pesquisa.

A definição de um conjunto de responsabilidades obrigatórias circunscreve os requisitos mínimos que o ambiente de preservação deve atender. Com isto, os administradores do repositório poderão definir as questões mais urgentes no desenvolvimento do repositório digital confiável. Já os mecanismos de apoio constituem possíveis alternativas para cumprir esta série de requisitos.

A implementação de um repositório digital em conformidade com o modelo OAIS compreende o primeiro passo para a preservação de documentos arquivísticos digitais autênticos em longo prazo. Conforme demonstrado, as entidades funcionais, os processos internos e a estrutura dos objetos de informação do OAIS compreendem um complexo fluxo de informação, no qual os documentos arquivísticos e seus respectivos componentes digitais são transportados em pacotes de informação (SIP, AIP e DIP); desde o produtor, até o consumidor.

Os documentos em ambiente digital necessitam de um conjunto de informações para representar corretamente a sua informação de conteúdo, isto demonstra a característica de recursividade. Assim, modelo lógico da informação arquivada permite identificar os componentes dos objetos de informação, pois localiza as informações que deve ser adicionadas aos objetos para obter a sua correta representação/interpretação. A informação adicional irá contribuir para a presunção de autenticidade dos documentos, pois identifica o seu histórico de custódia e modificações realizadas. Além disso, podem-se vincular informações que irão auxiliar na sua preservação, identificar o seu armazenamento e descrever o seu conteúdo para facilitar o processo de busca e recuperação da informação.

Um repositório digital que segue o modelo OAIS poderá estabelecer parcerias para minimizar custos, unir esforços financeiros e intelectuais com objetivo de potencializar as atividades de preservação de ambos os envolvidos. Para isto, será preciso definir níveis interoperabilidade entre sistemas de gestão, preservação e acesso que serão implementados. E caso seja firmada uma parceria de compartilhamento de recursos de infraestrutura, será preciso definir claramente qual é o acervo de cada repositório, respeitando assim, a responsabilidade de custódia de cada um. Tal aspecto também comporta um princípio arquivístico, o princípio da proveniência. Tais possibilidades de parcerias são peculiaridades do ambiente digital, visto que é possível compartilhar a mesma estrutura tecnológica, mesmo em longas distâncias geográficas.

O repositório arquivístico digital deve ser entendido como o ambiente confiável para preservação em longo prazo que irá garantir a correta interpretação/representação das informações digitais pelas suas comunidades designadas. Manter conformidade com o modelo OAIS é um ponto fundamental na busca por um fluxo de informação confiável, orientado para preservação e acesso de documentos digitais autênticos.

O modelo OAIS apresenta-se como a principal norma no âmbito da preservação digital, um estudo de fundamentação muito sólida, envolvendo diversos profissionais com propriedade no tema; além de ser desenvolvido no âmbito do CCSDS, o qual possui um complexo acervo, e que necessita de acesso contínuo no longo prazo. A conformidade com o modelo funcional e modelo de informação do OAIS permite aos repositórios digitais desenvolver um sistema robusto para preservação da informação digital no longo prazo.

No entanto, a conformidade com o OAIS não será um fim em si mesma, ou seja, será preciso demonstrá-la por meio de auditorias e certificações que confirmam o cumprimento dos requisitos do OAIS, e assim, a auditoria será capaz de mensurar o grau de confiabilidade do repositório digital. Desta forma, o ACTDR, configura-se como a ferramenta recomendada para proceder ao processo de auditoria e consequente certificação.

A análise do padrão de auditoria ACTDR perpassa os aspectos estruturais deste documento, de modo que cada requisito é abordado individualmente. Com isto, tornou-se possível contextualizar a aplicabilidade do ACTDR na Arquivística. A ausência de menções diretas do ACTDR a Arquivística é semelhante a razão do OAIS, ambos são orientações genéricas, destinadas a “repositórios digitais” em seu sentido mais amplo. Por isto, buscou-se uma aproximação, inserindo os requisitos do ACTDR no contexto da auditoria de um “repositório arquivístico digital confiável”.

Inicialmente, a seção “infraestrutura organizacional” contém os requisitos relacionados à política de preservação do repositório. Neste ponto, são definidas todas as implicações relativas à missão e comprometimento com a preservação de conteúdos. Da mesma forma, é preciso definir os recursos financeiros para garantir a longevidade do repositório, devem-se buscar os contratos e as licenças necessárias a fim de obter o controle necessário para preservar a informação de conteúdo, além de manter uma equipe qualificada para as suas atividades.

Ao cumprir os requisitos definidos na seção de “infraestrutura organizacional”, o RDC-Arq terá um planejamento estratégico suficiente para tomar decisões e promover soluções que garantam a continuidade da preservação das informações de conteúdo. Planos de sucessão e consequentes alterações da cadeia de custódia devem ser considerados, para que os documentos armazenados sejam transferidos caso seja necessário. Logo, deve haver políticas documentadas que garantam a preservação ininterrupta dos conteúdos.

Posteriormente, a seção “gestão de objetos digitais”, contém os requisitos relacionados ao tratamento dos objetos digitais. Isto compreende requisitos necessários desde a aquisição das informações de conteúdo até os meios para garantir acesso à comunidade designada. Assim, após a aquisição, são perpassadas questões relativas ao processo de criação do AIP: às políticas de preservação e seu planejamento, as atividades de preservação dos AIP’s, e o gerenciamento das informações por meio de metadados associados aos objetos digitais, chegando assim ao acesso.

Ao cumprir os requisitos definidos na seção “gestão de objetos digitais”, o RDC-Arq demonstra que segue procedimentos padronizados para tratamento dos pacotes AIP, e mantém conformidade com os fluxos de informação preconizados pelo OAIS. Esta seção tem um caráter orientado para as atividades realizadas diretamente nos objetos digitais, ou seja, criação do AIP, migrações, inserção de metadados, entre outras. Logo, estes requisitos auxiliam o auditor na verificação da conformidade do RDC-Arq como as entidades funcionais preconizadas pelo OAIS, ressaltando o cumprimento de seus requisitos.

Por fim, a seção “infraestrutura e segurança da gestão de riscos”, contém os requisitos necessários para proteger o RDC-Arq. Essa proteção pode ser definida em nível de documentos e sistemas, ou seja, avalia riscos da infraestrutura e da segurança da informação. A infraestrutura de *hardware* e *software* deve ser monitorada, e assim, o RDC-Arq irá minimizar as vulnerabilidades identificadas.

Além disso, é preciso manter um *backup* dos documentos e dos sistemas, de modo que, independente da falha que ocorrer, as atividades de preservação digital possam ser retomadas do ponto onde foram interrompidas. Tal procedimento agrega confiabilidade ao RDC-Arq, visto que o sistema será restaurado em seu estado atual, juntamente com os documentos armazenados. O que permite prosseguir as atividades de aquisição, custódia e disseminação de conteúdos.

Em linhas gerais, o ACTDR contém um conjunto de requisitos capaz de abranger três ramos pertinentes a um repositório digital: as políticas de preservação, o tratamento dos objetos digitais e a segurança dos dados e dos sistemas. Com isto, o auditor poderá avaliar os níveis de confiabilidade do repositório arquivístico digital e, caso atinja os níveis de confiabilidade esperados, será certificado como um RDC-Arq.

Dentre os atingimentos da pesquisa já podem ser citados o artigo publicado na revista argentina *Palabra Clave* e o manual para auditoria de RDC-Arq's. O artigo consiste, essencialmente, no capítulo de revisão de literatura, e apresenta uma reflexão sobre a preservação dos documentos arquivístico em ambiente digital considerando o seu caráter patrimonial. O produto desta pesquisa consiste no "manual para auditoria de repositórios arquivísticos digitais" localizado no "Apêndice B". Este manual apresenta o processo para auditoria de repositórios arquivísticos digitais, tendo por base os requisitos do ACTDR. Sendo assim, o ACTDR é contextualizado para ser aplicado a um RDC-Arq que segue o modelo OAIS, e está envolvido em uma cadeia de custódia confiável.

Neste manual, o modelo OAIS é abordado inicialmente, e destacam-se as suas responsabilidades obrigatórias, assim como, apresenta-se uma breve descrição dos fluxos de informação realizados pelas entidades funcionais. Posteriormente, aborda-se a cadeia de custódia documental, para destacar os principais requisitos e padrões arquivísticos pertinentes na implementação de um sistema de gestão documental.

Após apresentar a relação entre o RDC-Arq, o modelo OAIS e a cadeia de custódia documental, o manual prossegue à contextualização dos critérios para auditoria do ACTDR no âmbito da Arquivística. Assim, obtém-se uma base para que arquivistas compreendam os critérios do ACTDR, no entanto, é ressaltado que o manual não substitui a leitura e compreensão do OAIS e do ACTDR. Com a contextualização de cada critério do ACTDR tem-se uma base auxiliar para que os arquivistas dialoguem com os demais profissionais envolvidos no planejamento e implementação de um RDC-Arq.

Desta forma, estima-se que o manual seja capaz de incentivar o diálogo em torno dos RDC-Arq's, visto que a literatura sobre repositórios digitais, no sentido genérico do termo, está bem avançada; ao passo que a caracterização "repositório arquivístico" ainda carece de literatura própria. Logo, o manual consiste em uma aproximação entre RDC-Arq, OAIS, ACTDR e cadeia de custódia documental; logo, objetiva incentivar a reflexão a auxiliar nos processos de planejamento e implementação de RDC-Arq's.

Por fim, este estudo, em um primeiro momento, elucidou aos requisitos que um RDC-Arq deve seguir para estar em conformidade com o modelo OAIS, Posteriormente, avançou quanto ao processo de auditoria, descrevendo os

requisitos do ACTDR. Com isto, um RDC-Arq pode ser desenvolvido a partir da conformidade com OAIS e seguindo auditorias periódicas com o ACTDR, respeitando os princípios da Arquivística. Com base nisto, é possível apontar futuros estudos que podem ser realizados a parir dos resultados obtidos nesta pesquisa. Dentre estes estudos, é possível destacar: á tradução da norma ACTDR – ISO 16363 para língua portuguesa; a aplicação do manual em um repositório arquivístico; e a discussão sobre o processo de certificação dos repositórios digitais.

REFERÊNCIAS

ABREU, R. **A fabricação do imortal**: memória, história e estratégia de consagração no Brasil. Rio de Janeiro: Rocco, 1996.

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

BARRETO, A. A. Os documentos de amanhã: a metáfora, a escrita e a leitura nas narrativas em formato digital. **DataGramaZero**, v. 10, n. 1, 2009, Rio de Janeiro. Disponível em: <http://ridi.ibict.br/handle/123456789/159>. Acesso em 19 dez. 2017.

BELLOTO, H. L. Constituição, dispersão e reintegração de fundos. In: **Arquivo**: estudos e reflexões. p. 80-93. Belo Horizonte: UFMG, 2014.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO. **Presidência da República**: Casa Civil. Distrito Federal: Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em 22 de Julho de 2017.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de documentos eletrônicos. **Diretrizes para a implementação de repositórios digitais confiáveis de documentos arquivísticos**. Rio de Janeiro: Arquivo Nacional, 2014. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/publicacoes/resol_conarq_39_repositorios.pdf>. Acesso em: 13 ago. 2014.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de documentos eletrônicos. **Carta para a Preservação do Patrimônio Arquivístico Digital**. Rio de Janeiro: Arquivo Nacional, 2004. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf>. Acesso em: 10 ago. 2014.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de documentos eletrônicos. **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/publicacoes/earq/conarq_earqbrasil_model_requisitos_2009.pdf>. Acesso em: 05 ago. 2014.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de documentos eletrônicos. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/diretrizes_presuncao_autenticidade_publicada.pdf>. Acesso em: 20 jun. 2014.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de documentos eletrônicos. **Gestão Arquivística de Documentos Eletrônicos.** Rio de Janeiro:

Arquivo Nacional, 2004b. Disponível em: <http://pt.scribd.com/doc/37174068/Gestao-Arquivistica-de-Documentos-Eletronicos-CONARQ-Por-Claudia-Rocha>. Acesso em: 09 jul. 2014.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de documentos eletrônicos. **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis – RDC-Arq**. Rio de Janeiro: Arquivo Nacional, 2015. Disponível em: <http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf>. Acesso em: 10 jun. 2016.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara técnica de normalização da descrição arquivística. **Norma brasileira de descrição arquivística (Nobrade)**. Rio de Janeiro: Arquivo Nacional, 2006.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. **Resolução nº 28, de 17 de fevereiro de 2009**. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from_info_index=21&infoid=273&sid=46>. Acesso em: 22 abr. 2018.

BRASIL. LEI, Nº 8159, de 09 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial da União**. Brasília, 1991. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8159.htm>. Acesso em: 27 de novembro de 2016.

BRASIL. LEI, Nº 12527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI). **Diário Oficial da União**, Brasília, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso em 10 mar. 2017.

CANDAU, J. O jogo social da memória e da identidade (2). In: CANDAU, J. **Memória e identidade**. São Paulo: Contexto, 2014, p. 137-180.

CASANOVAS, I. **Gestión de documentos electrónicos**. Buenos Aires: Alfagrama, 2008.

CHOAY, F. **A alegoria do patrimônio**. 3. Ed. São Paulo: Unesp, 2006.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Audit and Certification of Trustworthy Digital Repositories (ACTDR)**. Magenta Book. Washington, Sep. 2011. Disponível em: <http://public.ccsds.org/publications/archive/652x0m1.pdf>. Acesso em: 13 nov. 2014.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Reference Model for an Open Archival Information System (OAIS)**. Magenta Book. Washington, Jun. 2012. Disponível em: <http://public.ccsds.org/publications/archive/650x0m2.pdf>. Acesso em: 13 mai. 2014.

CORRÊA, A. M. G. **Preservação digital**: autenticidade e integridade de documentos em bibliotecas digitais de teses e dissertações. 2010. 96 f. Dissertação (Mestrado em Ciência da Informação) – Universidade de São Paulo, São Paulo, 2010. Disponível em: <http://www.teses.usp.br/teses/disponiveis/27/27151/tde-05112010-105831/pt-br.php>. Acesso em: 3 jul. 2014.

DE SORDI, J. O. **Administração da informação**: fundamentos e práticas para uma nova gestão do conhecimento. São Paulo: Saraiva, 2008.

DIGITAL CURATION CENTRE; DIGITAL PRESERVATION EUROPE (DCC/DPE). **Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)**. v. 1.0, fev. 2007. Disponível em: <http://www.repositoryaudit.eu/download>. Acesso em: 13 nov. 2014.

DOCUMENT LIFECYCLE MANAGEMENT (DLM). Forum Foundation. The European Commission: 2010. Disponível em: <http://moreq.info/files/moreq2010_vol1_v1_1_en.pdf>. Acesso em: 27 mai. 2018.

FERREIRA, M. **Introdução à preservação digital**: conceitos, estratégias e atuais consensos. Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>. Acesso em: 2 ago. 2014.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2010.

GONÇALVES, J. R. S. O patrimônio como categoria de pensamento. In: ABREU, R.; CHAGAS, M. **Memória e patrimônio**: ensaios contemporâneos. Rio de Janeiro: Lamparina, 2009, p. 25-33.

INNARELLI, H. C. **Instrumenta 2**: Preservação de Documentos Digitais. Associação dos Arquivistas de São Paulo. São Paulo: ARQ-SP, 2012.

INNARELLI, H. C. Preservação digital e seus dez mandamentos. *In:* SANTOS, V. B. (Org.). **Arquivística**: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. 3. Ed. Distrito Federal: SENAC, 2009, p. 21-75.

INNARELLI, H. C. Preservação digital: a influência da gestão dos documentos digitais na preservação da informação e da cultura. **Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, v. 8, n. 2, p. 72-87, jan./jun. 2011. Disponível em: <http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/view/487/330>. Acesso em: 7 jul. 2014.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721:2012**. Space data and information transfer systems: open archival information system – Reference model.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363:2012**. Space data and information transfer systems: audit and certification of trustworthy digital.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 17799:2005**. Information technology: security techniques – Code of practice for information security management.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000:2018**. Information technology: security techniques – Information security management systems: overview and vocabulary.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (INTERPARES 2 PROJECT). **Diretrizes do preservador**. A preservação de documentos arquivísticos digitais: diretrizes para organizações. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. 2002-2007a. Disponível em: <http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf>. Acesso em: 9 ago. 2014.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (INTERPARES 2 PROJECT). **Diretrizes do produtor**. A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. 2002-2007b. Disponível em: <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf>. Acesso em: 9 ago. 2014.

JESSUA, C. **Capitalismo**. Porto Alegre: L&PM, 2016.

KANTORSKI, G.; KROTH, M. Proposta de informatização da gestão, preservação e acesso a documentos arquivísticos de uma instituição de ensino superior. In: **XV Colóquio Internacional de Gestão Universitária**. Argentina: 2015. Disponível em: <https://repositorio.ufsc.br/xmlui/handle/123456789/136155>. Acesso em 20 fev. 2018.

LÉVY, P. **As tecnologias da inteligência**: o futuro do pensamento na era da informática. 2. Ed. São Paulo: Editora 34, 2010.

LOPES, V. **Preservação digital**. Portugal: Universidade do Minho, Guimarães, 2008. Disponível em: <http://www.vitorlopes.com/Trabalhos/Preservacao_Digital-Vitor_Lopes.pdf>. Acesso em: 28 ago. 2012.

LUNA, S. V. **Planejamento de pesquisa**: uma introdução. São Paulo: EDUC, 1997.

LUZ, C. **Primitivos digitais**: uma abordagem arquivística. Salvador: 9Bravos, 2015.

MÁRDERO ARELLANO, M. Á. **Critérios para a preservação digital da informação científica**. 2008. 354f. Tese (Doutorado em Ciência da Informação) – Universidade Federal de Brasília, Departamento de Ciência da Informação, 2008. Disponível em:

<http://bdtd.bce.unb.br/tedesimplificado/tde_busca/arquivo.php?codArquivo=4547>. Acesso em: 15 jun. 2014.

MÁRDERO ARELLANO, M. Á. Preservação de documentos digitais, **Ciência da Informação**, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: <http://revista.ibict.br/ciinf/index.php/ciinf/article/view/305>. Acesso em: 25 jul. 2014.

NETWORK OF EXPERTISE IN LONG-TERM STORAGE (NESTOR). nestor Working Group on Trusted Repositories Certification: **Catalogue of Criteria for Trusted Digital Repositories**, Version 1 (draft for public comment). Frankfurt am Main: Jun 2006. nestor c/o Deutsche Nationalbibliothek. Disponível em: <http://files.d-nb.de/nestor/materialien/nestor_mat_08-eng.pdf>. Acesso em: 13 nov. 2014.

PAES, M. L. **Arquivo**: teoria e prática. 3. Ed. Rev. Ampl. Rio de Janeiro: FGV, 2004.

RESEARCH LIBRARIES GROUP; U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (RLG/NARA). **Trustworthy repositories audit & certification.** RLG, OCLC, Feb. 2007. Disponível em: <http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf>. Acesso em 08 set. 2014.

ROCHA, C. L.; SILVA, M. Padrões para Garantir a Preservação e o Acesso aos Documentos Digitais. **Acervo**, Rio de Janeiro, v. 20, nº 1-2, p. 113-124, jan/dez 2007. Disponível em: <http://www.revistaacervo.an.gov.br/seer/index.php/info/article/view/142>. Acesso em: 07 set. 2014.

RONDINELLI, R. C. **Gerenciamento arquivístico de documentos eletrônicos**: uma abordagem teórica da diplomática arquivística contemporânea. 4. ed. Rio de Janeiro: Fundação Getúlio Vargas, 2005.

ROUSSEAU, J-Y; COUTURE, C. **Os fundamentos da disciplina arquivística**. Lisboa: Publicações Dom Quixote, 1998.

SANTOS, H. M.; FLORES, D. O documento digital no contexto das funções arquivísticas. **Páginas a&b**, Porto, v. 3, n. 5, p. 165-177, 2016. Disponível em: <http://ojs.letras.up.pt/index.php/paginasaeb/article/view/1477>. Acesso em: 11 mar. 2017.

SANTOS, H. M.; FLORES, D. Os impactos da obsolescência tecnológica frente à preservação de documentos digitais. **Brazilian Journal of Information Science**, Marília, v. 11, n. 2, p, 28-37, 2017. Disponível em: <http://www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5550/4511>. Acesso em: 25 mai. 2018.

SARAMAGO, M. L. Metadados para preservação digital e aplicação do modelo OAIS. In: CONGRESSO NACIONAL DE BIBLIOTECARIOS, ARQUIVISTAS E DOCUMENTALISTAS, 8., 2004. **Anais eletrônicos**... Estoril: [s. n.], 2004. Disponível em:

<http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/640/637>. Acesso em: 4 jul. 2014.

SAYÃO, L. F. Repositórios digitais confiáveis para a preservação de periódicos eletrônicos científicos. **Ponto de Acesso**, Salvador, v. 4, n. 3, p. 68-94, dez. 2010. Disponível em: <http://www.portalseer.ufba.br/index.php/revistaici/article/view/4709>. Acesso em: 8 ago. 2014.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 13 jun. 2014.

SILVA, M. **O arquivo e o lugar**: custódia arquivística e a responsabilidade pela proteção aos arquivos. Niterói: Eduff, 2016. (Série Nova Biblioteca, 17).

SOUSA, R. T. B. A classificação como função matricial do que-fazer arquivístico. In*:* SANTOS, V. B. (Org.). **Arquivística**: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. 3. Ed. Brasília: SENAC, 2009, p. 79-172.

THOMAZ, K. P. **A preservação de documentos eletrônicos de caráter arquivístico**: novos desafios, velhos problemas. 2004. 389 p. Tese (Doutorado em Ciência da Informação) – Escola de Ciência da Informação. Universidade Federal de Minas Gerais, 2004. Disponível em: <http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/VALA-68ZRKF/doutorado___katia_de_padua_thomaz.pdf>. Acesso em: 28 jul. 2014.

THOMAZ, K. P. Documentos eletrônicos de caráter arquivístico: fatores condicionantes da preservação. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 10, n. 1, p. 34-53, jan./jun. 2005. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/301>. Acesso em: 7 set. 2014.

THOMAZ, K. P. Repositórios digitais confiáveis e certificação. **Arquivística.net**, Rio de janeiro, v. 3, n. 1, p. 80-89, jan./jun. 2007. Disponível em: <http://www.brapci.inf.br/_repositorio/2010/05/pdf_fed0720dbb_0010726.pdf>. Acesso em: 7 set. 2014.

THOMAZ, K. P. Gestão e preservação de documentos eletrônicos de arquivo: revisão de literatura – parte 2. **Arquivística.net**, Rio de Janeiro, v.2, n.1, p.114-131, jan./.jun. 2006. Disponível em: <www.brapci.ufpr.br/download.php?dd0=6733>. Acesso em: 07 set. 2014.

VELHO, G. Patrimônio, negociação e conflito. In: BELTRÃO, J. (Orgs.). **Antropologia e patrimônio cultural**: diálogos e desafios contemporâneos. Blumenau: Nova Letra, 2007, p. 249-262.

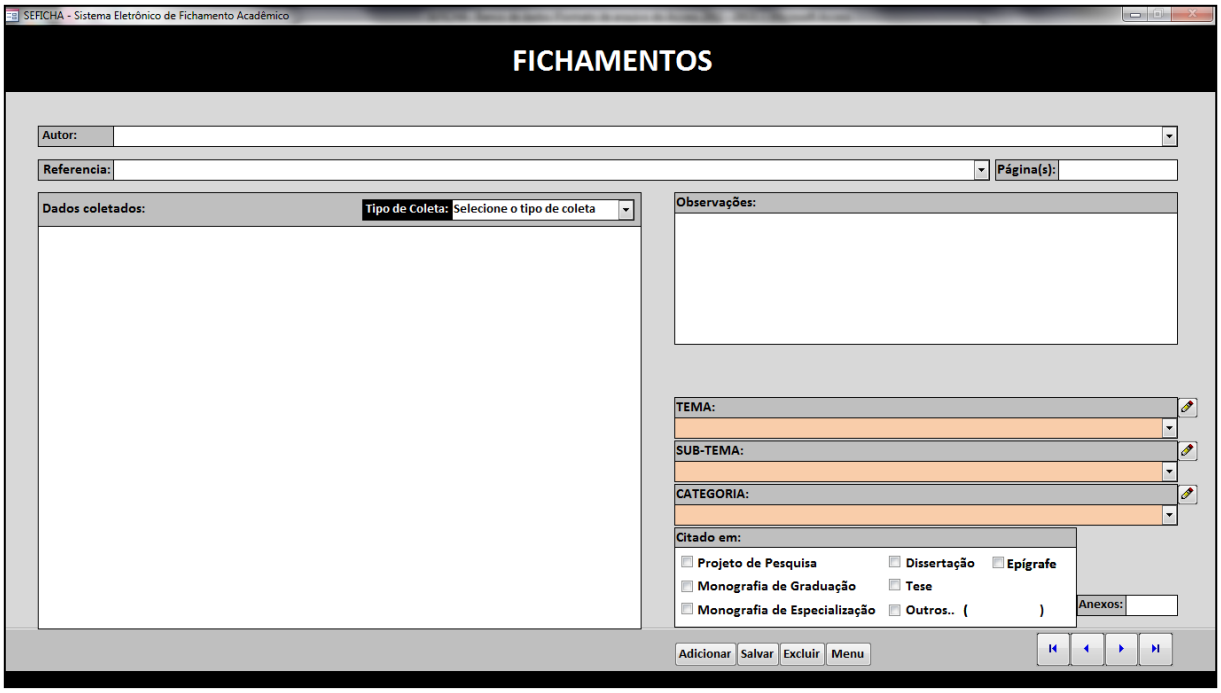
WEBB, C. **Guidelines for the Preservation of Digital Heritage**. Preparado pela Biblioteca Nacional da Austrália para a Divisão de Sociedade de Informação,

UNESCO, relatório n. CI-2003/WS/3. 2003. Disponível em: <http://unesdoc.unesco.org/images/0013/001300/130071e.pdf>. Acesso: em 17 Ago. 2014.

APÊNDICES

APÊNDICE A – MODELO DE FICHAMENTO PARA COLETA E TABULAÇÃO DE DADOS

Figura 29 – Modelo de fichamento para coleta e tabulação de dados



Fonte: Elaborado pelo autor.

APÊNDICE B – MANUAL PARA AUDITORIA DE RDC-ARQ'S

2018

MANUAL PARA AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Henrique Machado dos Santos

MANUAL PARA AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

É preciso ressaltar que a Arquivística se encontra em um momento de reformulação de suas teorias, e com a abordagem dos documentos digitais, surge à necessidade de adaptar e produzir teorias capazes de comportar os universos “analógico” e “digital”. Com este processo de reformulação teórico-prático, surgem diversas discussões e questionamentos que os arquivistas, inevitavelmente, terão de imergir e propor respostas ainda que provisórias, pois, se tratando de ciência, nada é definitivo, tudo está em constante transformação.

2018

MANUAL PARA AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Henrique Machado dos Santos

Como citar este documento:

SANTOS, Henrique Machado. Manual para auditoria de repositórios arquivísticos digitais confiáveis. Disponível em: <furg.academia.edu/HenriqueMachadodosSantos>.

As coisas que concebemos de maneira muito clara e distinta são todas verdadeiras; há apenas alguma dificuldade em observar bem quais são aquelas que concebemos distintamente.
(René Descartes).

Para que a vida seja boa de se assistir, seu espetáculo deve ser bem interpretado: para tal, porém, são necessários bons atores.
(Friedrich Nietzsche)

Não há como prever, evitar e nem mesmo ignorar os avanços das tecnologias, só há uma certeza: tudo que é contemporâneo se tornará obsoleto, e se não for preservado, será perdido com o tempo.
(Henrique Machado dos Santos & Daniel Flores).

O avanço tecnológico mudou radicalmente os mecanismos de registro e de comunicação da informação nas instituições e, consequentemente, seus arquivos também mudaram.
(Rosely Curi Rondinelli).

SUMÁRIO

APRESENTAÇÃO

A implementação de um Repositório Digital Confiável requer a conformidade com requisitos do modelo *Open Archival Information System* (OAIS) – ISO 14721:2012 e que sejam devidamente auditados e certificados com o padrão *Audit and Certification of Trustworthy Digital Repositories* (ACTDR) – ISO 16363:2012. No entanto, a implementação de um Repositório "Arquivístico" Digital Confiável (RDC-Arq), além de considerar estas normas, deverá estar em conformidade com princípios e peculiaridades inatas aos documentos arquivísticos. Dentre estes princípios e peculiaridades, podem-se mencionar os princípios da proveniência, organicidade, unicidade e integridade, além de peculiaridades como a forma fixa e o conteúdo estável.

Considerando estas questões mencionadas, realizou-se uma pesquisa partindo da análise das normas OAIS e ACTDR, com objetivo de propor um instrumento que facilite a compreensão dos requisitos necessários à implementação de um RDC-Arq. Sendo assim, este manual consiste no produto de uma dissertação de mestrado, intitulada "Auditoria de repositórios arquivísticos digitais confiáveis: uma análise das normas ISO 14721 e ISO 16363"; orientada pelo professor Daniel Flores, e defendida no Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural, da Universidade Federal de Santa Maria.

Desta forma, o "manual para auditoria de repositórios arquivísticos digitais" perpassa explicações gerais sobre o funcionamento de um arquivo digital em conformidade com o modelo OAIS, para preservação de documentos de caráter permanente. Ressalta a sua ligação com a gestão de documentos, assim como a necessidade de manter uma cadeia de custódia documental ininterrupta a fim de gerar confiabilidade.

Inicialmente, parte-se de uma abordagem geral do OAIS, para posteriormente, chegar a uma análise pontual dos requisitos de auditoria do ACTDR, de modo a ressaltar as necessidades de um RDC-Arq. Seu principal objetivo consiste em fornecer uma síntese dos requisitos de auditoria a fim de facilitar a compreensão dos arquivistas frente ao desafio de implementar e manter um RDC-Arq para preservação de documentos arquivísticos digitais autênticos, com garantia de acesso contínuo em longo prazo.

É preciso ressaltar que a Arquivística se encontra em um momento de reformulação de suas teorias, e com a abordagem dos documentos digitais, surge à necessidade de adaptar e produzir teorias capazes de comportar os universos "analógico" e "digital". Com este processo de reformulação teórico-prático, surgem diversas discussões e questionamentos que os arquivistas, inevitavelmente, terão de imergir e propor respostas ainda que provisórias, pois, se tratando de ciência, nada é definitivo, tudo está em constante transformação. Observa-se que a transformação não é menos intensa quanto aos documentos digitais, embora recentes, ainda não há um *corpus* teórico sedimentado, de modo que qualquer questionamento fundamentado será um divisor de opiniões potencial.

Este manual surge como um produto de reflexão acadêmica para instigar os profissionais e pesquisadores a compreenderem palavras-chave como: documento arquivístico digital, OAIS, ACTDR, cadeia de custódia, autenticidade, confiabilidade, auditoria e repositório arquivístico digital confiável. Com este manual, espera-se alavancar as discussões em torno dos RDC-Arq's, assim, como fornecer subsídios aos arquivistas que desejam compreender o processo de auditoria.

OBJETIVOS

O que este manual pretende: este manual visa orientar o processo de auditoria de RDC-Arq's, partindo da análise do OAIS e do ACTDR. Desta forma, enfatiza aspectos da Arquivística que devem ser considerados pela administração do repositório. Este manual visa aproximar o diálogo entre OAIS, ACTDR e Arquivística, isto porque, a linguagem utilizada nestas normas e a sua abrangência é tida como genérica, ou seja, destinada para repositórios digitais de diversas naturezas. Sendo assim, busca-se enfatizar os requisitos arquivísticos que estão implícitos tanto no OAIS, quanto no ACTDR. Dizem-se implícitos, pois, não há menções significativas à Arquivística, entretanto, há conceitos e princípios do OAIS que se enquadram na preservação de documentos arquivísticos digitais. Sendo assim, apresenta-se uma definição complementar capaz de resumir os requisitos que um RDC-Arq deve seguir.

O que este manual não pretende: este manual não pretende esgotar a discussão em torno da auditoria e certificação de RDC-Arq's, seu principal objetivo está centrado em promover a discussão. Da mesma forma, não pretende dispensar a leitura do OAIS e do ACTDR, pois seu princípio parte da compreensão destes e verticaliza para a visão arquivística. A leitura do OAIS é indispensável, pois será a partir de seus requisitos e orientações que o repositório será desenvolvido. Já a leitura do ACTDR é fundamental ao auditor, pois este precisa compreender os requisitos para qualquer repositório digital confiável. Sendo assim, este manual não substitui a leitura do OAIS e do ACTDR, apenas atuará de modo complementar para facilitar o diálogo com a Arquivística.

1. INTRODUÇÃO

O processo de auditoria torna-se essencial para demonstrar que um RDC-Arq está em conformidade com o modelo OAIS e que segue princípios arquivísticos. A realização de auditorias periódicas aliadas a uma certificação irá demonstrar que o RDC-Arq é confiável.

Inicialmente, é preciso estar ciente de que o processo de preservação digital começa antes da submissão dos documentos arquivísticos aos RDC-Arq. Isto reque a pré-existência de um Sistema Informatizado para Gestão Arquivística de Documentos (SIGAD), responsável pelas fases corrente e intermediária. Depois de encerrada esta fase "administrativa", os documentos devem ser recolhidos aos RDC-Arq, que será o arquivo permanente digital. E este será responsável por preservar e garantir o acesso contínuo no longo prazo.

Posteriormente, torna-se essencial compreender o modelo OAIS a fim de proceder a sua implementação em um RDC-Arq. Esta etapa deve considerar aspectos tecnológicos e políticos, de modo a abranger fluxos de informação, requisitos obrigatórios e entidades funcionais do OAIS; além de princípios fundamentais da Arquivística, como proveniência, unicidade e integridade.

Finalmente, o RDC-Arq deve ser auditado a fim de mensurar seus níveis de confiabilidade para que possa ser certificado pelo órgão competente. O processo de auditoria deve considerar o padrão ACTDR, o qual verifica a definição de políticas, a gestão de objetos digitais e os níveis de segurança dos dados armazenados. Assim, verifica-se a conformidade do RDC-Arq com o modelo OAIS para que seja mensurado o seu nível de confiabilidade.

Nesse contexto, o presente manual tem por objetivo fornecer subsídios teóricos para compreensão do modelo OAIS e do padrão ACTDR, com ênfase nos requisitos para auditoria de RDC-Arq's. Da mesma forma, busca-se esclarecer os requisitos arquivísticos que estão subentendidos no RDC-Arq, realçando sua pertinência durante o processo de auditoria.

2. MODELO OAIS

Há uma série de responsabilidades obrigatórias a serem atendidas por um repositório em conformidade com o modelo OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Desta forma, um RDC-Arq deverá:

- Negociar e aceitar informações adequadas junto ao produtor;
- Obter o controle das informações fornecidas para garantir a preservação em longo prazo;
- Participar da definição da comunidade designada[1], e estabelecer sua base de conhecimento para compreender as informações fornecidas;
- Garantir que a comunidade designada é capaz de compreender as informações preservadas sem necessidade de recursos especiais ou do auxílio dos produtores;
- Seguir políticas e procedimentos previamente documentados demonstrando confiabilidade na preservação da informação, além de restringir a exclusão de itens, exceto que permitido como parte de uma estratégia aprovada;
- Disponibilizar a informação preservada à comunidade designada, permitindo disseminá-la como cópia ou rastreável[2].

As responsabilidades obrigatórias são os propósitos do repositório digital, estão relacionadas a aquisição da informação digital e dos direitos para realizar a sua preservação em longo prazo. Além disso, há a definição da comunidade designada, de modo que esta seja capaz de interpretar as informações preservadas sem a necessidade de se recorrer a métodos complexos e específicos.

Em resumo, as responsabilidades irão definir o que será preservado e o seu respectivo direito para tal. Além disso, irão manter procedimentos para a

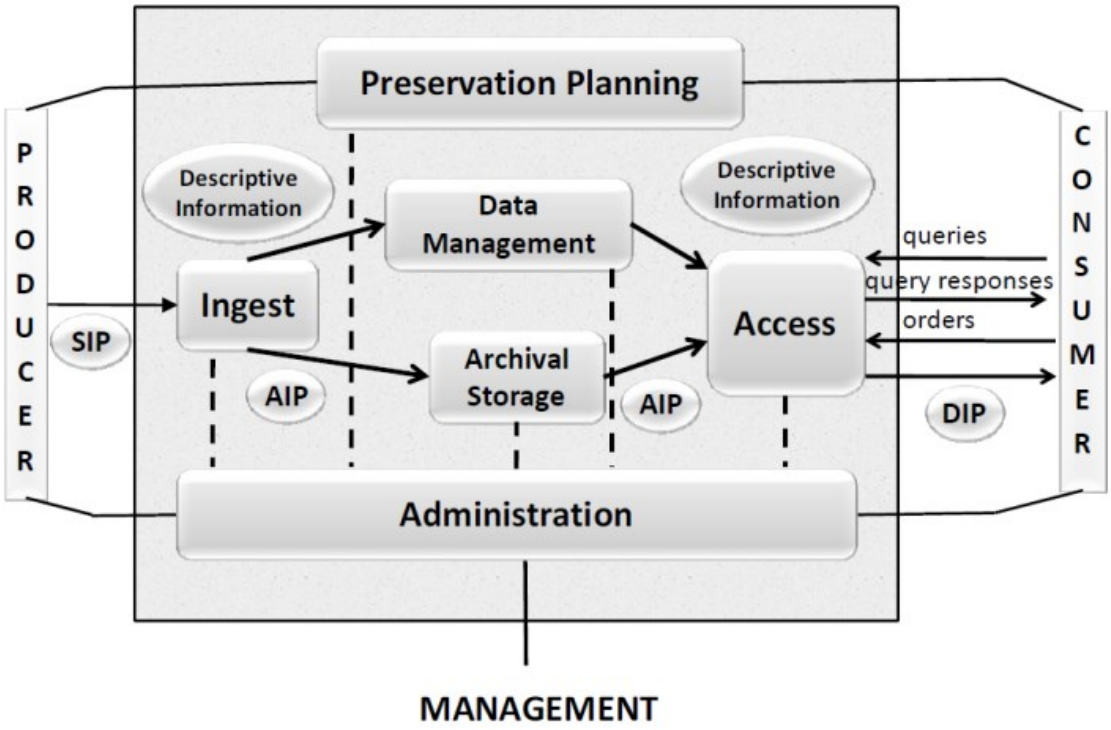
[1] Conjunto identificado de usuários potenciais capazes de entender um conjunto específico de informações. A comunidade designada pode ser composta por várias comunidades de usuários. Logo, o arquivo definirá a comunidade designada, e esta definição, poderá mudar com o tempo (CCSDS, 2012; ISO 14721:2012). No entanto, no âmbito da Arquivística, esta distinção de público não ocorre de forma rígida. O acesso à informação preservada é oferecido para quaisquer usuários que tenham interesse na informação de conteúdo. A visão arquivística da comunidade designada corresponde ao arquivo e seus usuários potenciais, ou seja, não há restrição de público. Logo, o objetivo é atender o maior número possível de usuários interessados, de modo que estes sejam capazes de interpretar corretamente as informações preservadas.

[2] Apontando para o objeto de dados originalmente submetido junto com os demais elementos que comprovam a sua autenticidade

preservação e definir quem irá usufruir deste material. Neste ponto, o modelo OAIS subentende a necessidade de assegurar a posse legal da informação digital, bem como conhecer previamente, a existência de uma comunidade potencialmente interessada na preservação e garantia de acesso ininterrupto à informação.

Com relação ao ambiente OAIS há seis entidades funcionais, que são: admissão (*ingest*), armazenamento arquivístico (*archival storage*), gestão de dados (*data management*), administração (*administration*), plano de preservação (*preservation planning*) e acesso (*access*). Neste ambiente, perpassam os pacotes de informação (*Submission Information Package* – SIP, *Archival Information Package* – AIP e *Dissemination Information Package* – DIP) nos quais são inseridas as informações descritivas (*descriptive information*) referentes às suas respectivas informação de conteúdo. A seguir, a "Figura 1 – Entidades funcionais do OAIS" apresenta uma esquematização simplificada da relação entre indivíduos, entidades funcionais e pacotes de informação.

Figura 1 – Entidades funcionais do OAIS



Fonte: (CCSDS, 2012, p. 4-1).

Há um conjunto de entidades internas e externas ao ambiente OAIS. As entidades internas são: admissão (*ingest*), armazenamento arquivístico (*archival*

storage), gestão de dados (*data management*), administração (*administration*), plano de preservação (*preservation planning*) e acesso (*access*). E as entidades externas são: produtor (*producer*), administrador (*management*) e consumidor (*consumer*).

O produtor (*producer*) se refere às pessoas ou sistemas que fornecem a informação que será preservada por meio da submissão de SIP's. O administrador (*management*) se refere àqueles que estabelecem as políticas gerais que governam o repositório pela entidade interna administração (*administrator*). Desta forma, os SIP's são transformados em AIP"s para serem arquivamentos. Já o consumidor (*consumer*) se refere às pessoas ou sistemas que interagem com os serviços oferecidos pelo OAIS para acessar a informação preservada através da entidade de acesso (*access*). Logo, para atender as demandas de acesso, o repositório irá gerar pacotes DIP, os quais são compostos por formatos de arquivos mais "leves", especiais para a disseminação via *Internet*.

Após o produtor (*producer*) submeter o SIP, a entidade de admissão (*ingest*) irá verificar a conformidade do pacote com os modelos previamente definidos nas políticas de preservação junto à entidade planejamento da preservação (*preservation planning*). Em caso de não conformidade, o pacote será rejeitado. Caso o pacote esteja de acordo com estas políticas, a entidade de administração (*administrator*) irá realizar a admissão dos conteúdos do SIP. Posterirormente, a informação descritiva (*descriptive information*) será inserida, com objetivo de registrar o histórico de custódia dos objetos digitais, relatando quaisquer aliterações realizadas juntamente com as informações adicionais utilizadas para preservação e garantia de acesso. Assim, o pacote SIP é transformado em AIP e encaminhado à entidade armazenamento arquivístico (*archival storage*).

Neste estágio, a entidade armazenamento arquivístico (*archival storage*) torna-se responsável por preservar os pocetes AIP's, enquanto a entidade gestão de dados (*data management*) irá gerenciar as informações descritivas dos objetos digitais. Assim a gestão de dados (*data management*) manterá um banco de dados atualizado sobre as informações relativas aos AIP's, corroborando com a manutenção de sua autenticidade, preservação e garantia de acesso ininterrupto no longo prazo.

A entidade de acesso (*access*) é a meio de comunicação entre o consumidor (*consumer*) e o repositório, podendo ser denominada como plataforma de acesso.

Neste ponto, ressalta-se que o consumidor (*consumer*) não tem acesso direto aos AIP's armazenados na entidade armazenamento arquivístico (*archival storage*), mas tão somente, à plataforma de acesso, comunicando-se indiretamente pela entidade de acesso (*access*). Tal procedimento é um fluxo de informação pertinente do OAIS visto que adicionam maior controle das ações e minimiza os riscos de invasão aos conteúdos preservados.

Desta forma, o consumidor solicita acesso a um determinado conteúdo e a entidade de acesso (*access*) encaminha a solicitação. O resultado da solicitação é enviado ao consumidor (*consumer*) pela entidade de acesso (*access*) por meio do pacote DIP; e segue as políticas de preservação e acesso definidas pelas entidades plano de preservação (*preservation planning*) e administração (*administrator*).

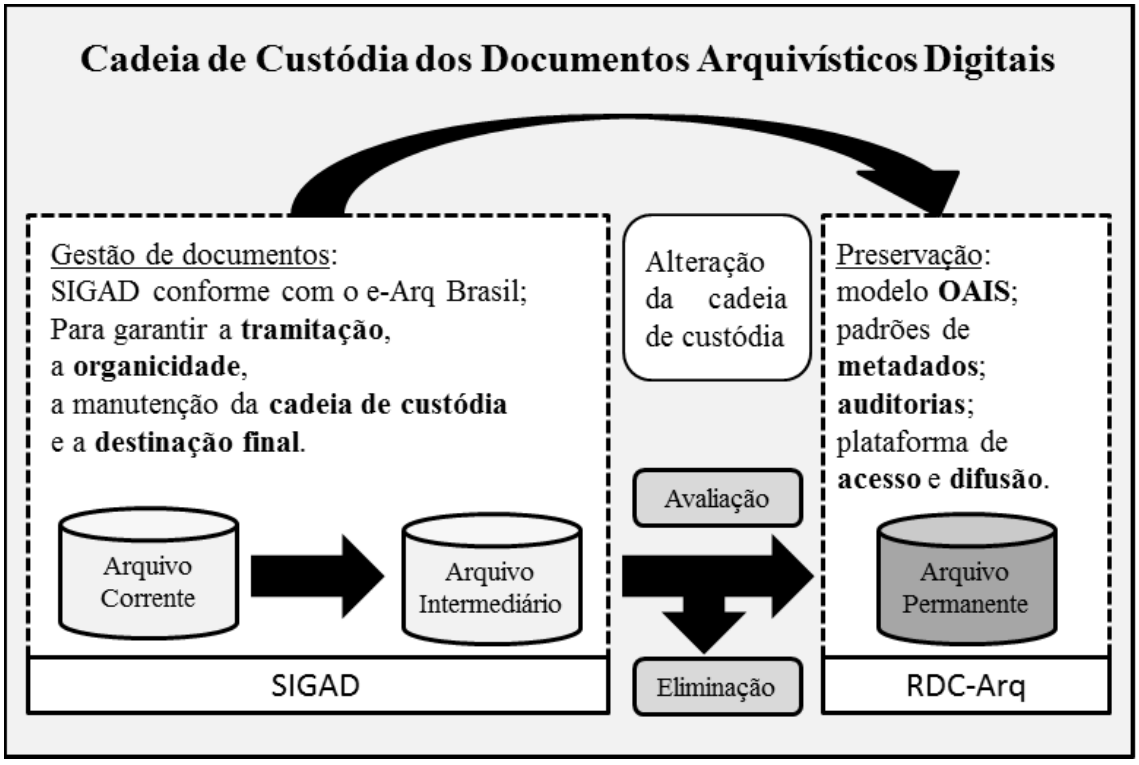
As responsabilidades do OAIS estão relacionadas às políticas de preservação digital, já o fluxo de informação, através das entidades, está relacionado ao gerenciamento dos objetos digitais admitidos, custodiados e disseminados. Tais questões são aprofundadas na ISO 14721:2012, além de definir um modelo lógico para os tipos de informações arquivadas.

Após esta breve explanação do OAIS na implementação de um RDC-Arq, procede-se a caracterização da cadeia de custódia para documentos arquivísticos em ambiente digital. Desta forma, contextualizam-se os principais componentes envolvidos no sistema de gestão de documentos, comportando desde a produção e tramitação até a preservação e acesso.

3. CADEIA DE CUSTÓDIA DOCUMENTAL

Os documentos arquivísticos em sua trajetória administrativa e histórica perpassam três fases que são: corrente, intermediária e permanente. Desta forma, têm-se dois sistemas informatizados distintos, que são o Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e o RDC-Arq, envolvidos em uma cadeia de custódia ininterrupta. Inicialmente, o SIGAD será responsável pelas fases corrente e intermediária, já o RDC-Arq será responsável pela fase permanente. A relação entre os sistemas informatizados é esquematizada na "Figura 2 – Cadeia de Custódia dos Documentos Arquivísticos Digitais".

Figura 2 – Cadeia de Custódia dos Documentos Arquivísticos Digitais



Fonte: adaptado de Flores, Rocco e Santos (2016).

As fases corrente e intermediária compõe o ambiente da gestão de documentos, enquanto a fase permanente compõe o ambiente da preservação e acesso. Assim, o SIGAD deverá considerar Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil), enquanto o RDC-Arq considerar o modelo OAIS. Estes dois ambientes distintos devem ser unidos por uma cadeia de custódia ininterrupta que irá corroborar na presunção de

autenticidade e confiabilidade do sistema para gestão de documentos no seu sentido mais amplo, o organizacional.

Neste sistema, o SIGAD será responsável pela tramitação dos documentos, e deverá manter sua classificação e organicidade. Além disso, o SIGAD deve implementar rotinas de presunção de autenticidade, garantindo que não foram realizadas alterações não autorizadas e nem documentadas. Depois de encerrado o valor primário dos documentos nas fases corrente e intermediária, estes serão avaliados pelo SIGAD com base em uma tabela de temporalidade previamente definida. Desta forma, documentos sem valor secundário serão eliminados do sistema, e os documentos que possuírem um valor secundário (valor histórico, social, probatório ou informativo) serão recolhidos ao arquivo permanente.

Este é um ponto crítico no sistema para gestão de documentos, visto que os documentos armazenados em um sistema são transferidos para outro (do SIGAD para o RDC-Arq). Além disso, poderá ocorrer a mudança do custodiador (abordagem pós-custodial), ou seja, uma instituição será responsável pelas fases corrente e intermediária e, outra instituição ficará responsável pela guarda dos documentos permanentes. Esta possibilidade rompe com um dos paradigmas Arquivísticos, pois tradicionalmente, a instituição produtora era a mesma responsável pela custódia de seus documentos permanentes. Assim, o advento do documento arquivístico digital traz este pertinente questionamento: a pós-custódia.

O ambiente de preservação consiste em um local denominado arquivo permanente, no qual será implementado o repositório digital em conformidade com o modelo OAIS, além de seguir princípios arquivísticos, sendo assim, um RDC-Arq. Este será o ambiente autêntico para preservação de longo prazo, e estará isolado dos usuários externos a fim de minimizar possíveis invasões. Para isto, utiliza uma plataforma de acesso pela qual os usuários irão solicitar acesso aos materiais. Este procedimento acrescenta maiores níveis de segurança, pois, o RDC-Arq será monitorado constantemente e os usuários não terão acesso direto aos seus conteúdos, somente à plataforma de acesso.

Caso a plataforma de acesso seja invadida não ocorrerão danos contra os materiais armazenados no RDC-Arq, pois é este quem envia os dados solicitados a plataforma. A plataforma de acesso não acessa os materiais armazenados no RDC-Arq, ela solicita o envio destes materiais que lhe são solicitados pelos usuários.

4. REQUISITOS DO ACTDR

Ao abordar repositórios arquivísticos, delimita-se o horizonte de aplicação do OAIS, e consequentemente, do ACTDR. Ambos os modelos fazem menções genéricas ao "repositório digital", não entrando em especificidades da área de arquivo. Desta forma, muitos princípios arquivísticos estão subentendidos nos requisitos do OAIS e do ACTDR, sendo assim, esta seção tem por objetivo ressaltar o ponto de vista arquivístico frente aos requisitos do ACTDR.

Para realizar a análise proposta optou-se por manter os requisitos estruturados conforme o próprio documento do ACTDR, mantendo os códigos da numeração adotada por este documento para facilitar o entendimento. Desta forma, apresenta-se uma breve definição, **complementar**, para cada seção, subseção e requisitos, que estabelece um diálogo entre o ACTDR e a Arquivística.

[3] **INFRAESTRUTURA ORGANIZACIONAL**

Estas questões estão diretamente relacionadas às políticas institucionais para preservação de documentos, e delineiam o planejamento organizacional e o funcionamento legal do arquivo responsável pela custódia documental.

[3.1] GOVERNANÇA E VIABILIDADE ORGANIZACIONAL

Consiste em definir a missão do repositório e assumir o compromisso com a preservação e o acesso em longo prazo. Para isto, são definidos de forma explícita, os planos de sucessão e a política de recolhimento para custódia. Um RDC-Arq deve declarar o seu compromisso com a preservação dos documentos de tal caráter, e definir previamente quaisquer alterações na custódia, de modo a designar os requisitos a serem cumpridos por um eventual "novo custodiador".

[3.1.1] **Ter uma declaração de missão que reflete um compromisso de preservação, de retenção no longo prazo, de gestão, e de acesso à informação digital**: tal declaração pode ser facilmente realizada por uma instituição arquivística, visto que esta tem o compromisso em preservar

documentos arquivísticos. Mesmo assim, destaca-se a importância de reafirmar este compromisso, com a menção de termos como “documentos arquivísticos digitais”, “repositório arquivístico digital”, o que define claramente um compromisso em preservar os registros em ambiente informatizado.

[3.1.2] **Ter um plano estratégico de preservação definido que o aproxime de sua missão apoiando o seu cumprimento no longo prazo**: a preservação de documentos arquivísticos digitais exige uma série de recursos para garantir a sustentabilidade do arquivo no longo prazo. Logo, é preciso que estes recursos estejam previamente definidos no plano estratégico de preservação.

[3.1.2.1] **Ter um plano de sucessão, contingência e/ou acordos judiciais apropriados caso em algum momento, o repositório cesse a sua atividade ou o governo ou instituição de financiamento altere substancialmente o seu âmbito**: é essencial definir previamente os possíveis rumos dos documentos preservados em caso de alterações que gerem impacto direto no custodiador. Alterar recursos financeiros ou mesmo o responsável pela custódia documental implica em reformular o processo de preservação. Para isto, deve garantir todas as informações e permissões necessárias para que o novo custodiador consiga executar as atividades de preservação necessárias.

[3.1.2.2] **Controlar seu ambiente organizacional para determinar quando deve executar o seu plano de sucessão, contingência e/ou acordos judiciais**: o arquivo enquanto instituição deve estar ciente das influências que circundam o ambiente de preservação, analisando questões políticas e econômicas para definir a viabilidade de continuar preservando tais conteúdos. Assim, caso não seja sustentável, o RDC-Arq deve proceder à sucessão dos conteúdos, e repassar a responsabilidade pela custódia;

[3.1.3] **Ter uma política de recolhimento ou documentação que especifique o tipo de informação que irá preservar e garantir acesso**: no caso de um

RDC-Arq, os conteúdos a serem admitidos devem ser exclusivamente, documentos arquivísticos. Também será preciso identificar e distinguir os produtores, caso os documentos tenham mais de uma proveniência, e assim, registrar com precisão os procedimentos utilizados durante a aquisição. Isto irá manter a proveniência dos acervos, respeitando os princípios arquivísticos.

[3.2] ESTRUTURA ORGANIZACIONAL E DE PESSOAL

Compreende a gestão das competências de pessoal necessárias para o cumprimento das funções do repositório. Definir o organograma qual explícita a divisão de funções e responsabilidades. Além disso, incentiva o desenvolvimento pessoal, auxilia a formação continuada para desenvolver habilidades e gerar novos conhecimentos. Desta forma, a equipe do arquivo deve estar em constante atualização, visto que os documentos em ambiente digital impõem novos desafios frente ao profissional arquivista, o qual vivencia uma transição dos acervos analógicos para acervos mistos (analógicos e digitais).

[3.2.1] **Identificar e estabelecer as funções que deve executar, bem como dispor de pessoal com qualificação e experiência para tal**: os funcionários devem ser capacitados conforme surjam as demandas relacionadas à evolução das tecnologias. Este ponto é fundamental, pois as tecnologias da informação e comunicação evoluem em um ritmo cada vez mais acelerado. Tal fato tem ocasionado ciclos de obsolescência cada vez mais curtos, o que torna o processo de atualização dos funcionários tão essencial quanto à atualização tecnológica.

[3.2.1.1] **Identificar e estabelecer seus deveres**: o RDC-Arq deve estar ciente de suas atividades e demonstrar capacidade de cumpri-las, a fim de garantir a sua sustentabilidade no logo prazo.

[3.2.1.2] **Ter o número adequado de funcionários para realizar todas as funções e serviços**: no contexto de um RDC-Arq, ressalta-se a necessidade de uma equipe interdisciplinar/multidisciplinar. Assim,

profissionais de diversas áreas dialogando entre si, corroboram para o cumprimento das atividades do RDC-Arq, e com isso, eleva-se a qualidade dos serviços prestados.

[3.2.1.3] **Colocar em prática um programa de desenvolvimento profissional ativo que oferece oportunidades de desenvolvimento de competências ao pessoal**: este é um requisito de aprendizagem, pelo qual o RDC-Arq acompanha a evolução das tecnologias, dos procedimentos e da própria comunidade designada. Todo arquivo que preserva documentos em um repositório digital deve manter um plano de atualização tecnológica. Isto se faz necessário por causa da constante evolução das tecnologias aliado a necessidade de fornecer acesso aos conteúdos autênticos e inteligíveis.

[3.3] POLÍTICAS DE RESPONSABILIDADE E PRESERVAÇÃO

O repositório deve definir a comunidade designada e a base de conhecimento, além de possuir políticas para o cumprimento dos serviços, acompanhar a evolução das tecnologias e da comunidade designada, e receber o *feedback* de produtores e consumidores. Outro fator pertinente é manter ações transparentes de preservação, registro das transformações da informação e da avaliação de integridade, desta forma, é possível manter um calendário regular para certificação.

[3.3.1] **Definir a sua comunidade designada e a base de conhecimento associada, e manter essas definições de forma acessível**: no caso de um RDC-Arq, a comunidade designada assume um caráter muito abrangente e genérico, visto que os documentos preservados correspondem, por vezes, desde uma parcela significativa da sociedade até a nação como um todo.

[3.3.2] **Ter políticas de preservação para garantir que seu plano estratégico de preservação será cumprido**: as políticas irão mostrar como o RDC-Arq cumpre os requisitos do plano estratégico de preservação. Desta

forma, as políticas de preservação do arquivo devem ter claras menções ao repositório e aos documentos digitais.

[3.3.2.1] **Ter mecanismos de revisão, atualização e desenvolvimento permanente das suas políticas de preservação, os quais irão monitorar o crescimento do repositório, assim como a evolução da tecnologia e da prática da comunidade**: tais políticas devem ser compreensíveis pela equipe do RDC-Arq para auxiliar no trabalho. Logo, a revisão deve centrar-se em manter o caráter arquivístico dos documentos, de modo que as tecnologias sejam adaptadas aos princípios da Arquivística, e nunca o contrário.

[3.3.3] **Manter um histórico documentado das alterações em suas operações, procedimentos, *software* e *hardware***: a preservação de documentos arquivísticos requer o constante monitoramento e registro dos procedimentos, a fim de verificar a sua evolução, seja de tecnologia, seja de procedimentos. Isto possibilita futuras análises sobre as decisões tomadas, verificando os pontos assertivos e os equívocos.

[3.3.4] **Manter a transparência e responsabilidade em todas suas ações, além de apoiar a operação e a gestão do repositório no que tange a preservação de conteúdos digitais no longo prazo**: além dos padrões amplamente conhecidos pela comunidade de preservação digital, o RDC-Arq pode demonstrar que segue recomendações como as do Conselho Nacional de Arquivos, e realiza práticas orientadas ao projeto InterPARES, entre outros estudos pertinentes.

[3.3.5] **Definir, coletar, rastrear e fornecer adequadamente as suas medições integridade das informações**: a verificação da integridade é um procedimento essencial para RDC-Arq's, de modo que estes documentos em ambiente digital tornam-se extremamente vulneráveis, e podem ser modificados/falsificados com facilidade e sem deixar vestígios aparentes.

[3.3.6] **Comprometer-se a um calendário regular de autoavaliação e certificação externa**: um repositório arquivístico deve se submeter a auditorias periódicas para que possa ser denominado como “confiável”, tornando-se um RDC-Arq. Ressalta-se que este não é um procedimento definitivo, o qual precisa ser reafirmado por meio de nova auditoria e consequente certificação. Assim, por meio uma constante caracterização de confiança, o repositório mantém-se confiável perante a comunidade de preservação e comunidade designada.

[3.4] SUSTENTABILIDADE FINANCEIRA

Compreende a definição de processos de planejamento para curto e longo prazo, com ajustes periódicos. Assim, preconizam-se procedimentos financeiros transparentes com auditoria, além de monitorar continuamente os riscos, benefícios, investimentos e despesas, buscando solução para problemas de financiamento.

[3.4.1] **Dispor de processos de planejamento de negócios no curto e no longo prazo, para garantir a sustentabilidade ao longo do tempo**: em se tratando de um RDC-Arq, este tem o compromisso inato com a preservação e o acesso á documentos no longo prazo. Isto porque a finalidade da Arquivística consiste em preservar e garantir acesso.

[3.4.2] **Ter procedimentos financeiros transparentes, em conformidade com normas e práticas contábeis relevantes, e ser auditado por terceiros, em conformidade com os requisitos legais de seu respectivo território**: este requisito está estreitamente ligado a questões administrativas e contábeis do RDC-Arq. A transparência atua como um meio para gerar confiança na gestão financeira, não entrando em aspectos do campo teórico da Arquivística.

[3.4.3] **Comprometer-se em analisar e informar continuamente sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos)**: desta forma, o repositório irá manter o equilíbrio

adequado entre o risco e benefício, investimentos e retorno. Assim, um RDC-Arq deve manter uma estrutura próxima do ideal, de modo a considerar a relação custo/benefício. No entanto, a otimização de recursos não deve se sobrepor a necessidade de implementação de determinados requisitos necessários à preservação e garantia de acesso a documentos autênticos.

[3.5] CONTRATOS, LICENÇAS E PASSIVOS

Consiste em manter contratos ou acordos de depósito apropriados aos materiais digitais de outra organização, capazes de especificar e transferir todos os direitos de preservação necessários. Da mesma forma, permite rastrear e gerenciar os direitos de propriedade intelectual e possíveis restrições sobre o uso do conteúdo, definindo as políticas com base na legislação para conteúdos digitais com propriedade ou direitos não especificados claramente.

[3.5.1] **Manter contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e/ou fornece acesso**: o RDC-Arq deve possuir as permissões legais (autorizações, contratos e licencas) necessárias para recolher e preservar uma determinada informação, corroborando com formação da sua imagem enquanto custodiador.

[3.5.1.1] **Ter contratos de depósito que especificam a transferência de todos os direitos de preservação necessários, e que esses direitos estejam documentados**: alterar a informação digital é uma tarefa necessária para preservá-la em um RDC-Arq. Determinadas tecnologias tornam-se obsoletas, logo é necessário migrar para novos suportes e formatos de arquivo para continuar acessando os conteúdos;

[3.5.1.2] **Especificar todos os aspectos relevantes de aquisição, manutenção, acesso e retirada de conteúdos, através de acordos documentados com os depositantes e outras partes relevantes**: o RDC-Arq assume a responsabilidade da preservação, manutenção e garantia de acesso aos documentos, e paralelamente, negocia aspectos da submissão

do SIP junto aos produtores de conteúdos. Desta forma, é possível estabelecer que os conteúdos submetidos devam estar em conformidade com determinadas normas ou padrões recomendados pelo repositório.

[3.5.1.3] **Ter políticas documentadas que indiquem quando ele aceita a responsabilidade de preservação dos conteúdos de cada conjunto de objetos de dados submetidos**: este requisito formaliza a aceitação da responsabilidade pela custódia dos materiais submetidos ao RDC-Arq, e fornece documentação para as partes interessadas comprovando a transferência e as condições para que o compromisso seja firmado.

[3.5.1.4] **Ter políticas para atender as responsabilidades e os desafios relacionados às questões de propriedade/direitos**: ter políticas de preservação que mantenham a conformidade com leis e requisitos pertinentes irá minimizar as responsabilidades potenciais do RDC-Arq. Logo, o RDC-Arq terá maior controle dos documentos arquivísticos custodiados, o que corrobora para cumprir suas atividades relacionadas á preservação e garantia de acesso.

[3.5.2] **Controlar e gerenciar os direitos de propriedade intelectual e restrições à utilização do conteúdo conforme exigido pelo contrato, acordo de depósito ou licença**: isto permite que o RDC-Arq identifique quaisquer impedimentos relacionados ao processo de preservação e acesso, de modo que defina políticas para solucionar tais problemas. Assim, verificam-se restrições com relação à alteração das informações, bem como as restrições para difusão e acesso de conteúdos.

[4] GESTÃO DE OBJETOS DIGITAIS

A seção gestão de objetos digitais compreende aspectos relacionados à aquisição de conteúdo, criação do pacote de arquivamento, plano da preservação, preservação e manutenção dos AIP's, gestão da informação, e gestão de acesso.

[4.1] ADMISSÃO: AQUISIÇÃO DE CONTEÚDO

Permite identificar as propriedades significativas dos objetos digitais que serão preservadas, para isto, são associadas às informações necessárias ao pacote SIP. As fontes de proveniência dos objetos admitidos devem ser autenticadas, e devem-se executar as correções necessárias a cada SIP submetido. Além disso, é preciso obter controle físico dos objetos digitais para preservá-los, e fornecer respostas adequadas ao produtor durante o processo de submissão.

[4.1.1] **Identificar as informações de conteúdo e as propriedades da informação que serão preservadas**: o RDC-Arq define quais aspectos da informação de conteúdo são pertinentes à preservação, informando assim, aos seus colaboradores.

[4.1.1.1] **Ter procedimento(s) para identificar as propriedades da informação que serão preservadas**: o RDC-Arq estabelece os métodos e fatores utilizados para determinar os aspectos de diferentes tipos de informação de conteúdo para os quais assume a responsabilidade de preservação frente à comunidade designada. Ressalta-se que tais características são essenciais para a presunção de autenticidade, bem como para a interpretação/representação da informação de conteúdo.

[4.1.1.2] **Ter um registro das informações de conteúdo e das propriedades de informação que serão preservadas**: o RDC-Arq terá definido o que será preservado, e assim, firmar o compromisso com tais tipos de informação previamente definidas. Posterirormente, a demonstração do cumprimento deste requisito é um importante passo para demonstrar a capacidade de preservar documentos de forma confiável.

[4.1.2] **Especificar claramente, no momento do depósito, qual informação precisa ser respectivamente associada com a informação de conteúdo**: o nível de precisão destas especificações irá variar conforme as políticas de cobrança e sua relação aos produtores. Logo, o RDC-Arq deverá buscar junto

ao produtor toda a informação necessária para representar corretamente os documentos recolhidos.

[4.1.3] **Ter especificações adequadas que permitam reconhecer e analisar os SIP's**: o repositório poderá analisar o conteúdo de um determinado objeto digital e verificar se a sua estrutura lógica corresponde ao formato de arquivo que representa. Tal procedimento é pertinente, pois os formatos de arquivo podem não refletir o que realmente são. Um documento de texto pode estar equivocadamente representado em um formato de imagem, o que resulta em erro de interpretação/representação da informação de conteúdo.

[4.1.4] **Ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais**: garante que o RDC-Arq irá determinar corretamente a procedência de cada SIP recebido, mantendo um dos princípios essenciais da Arquivística, o princípio da proveniência.

[4.1.5] **Ter um processo de admissão que verifique a integralidade e precisão de cada SIP**: o RDC-Arq deve ter um rígido controle de admissão de conteúdos, de modo que os pacotes AIP reflitam as informações de conteúdos dos pacotes SIP. Isto é essencial para demonstrar que o RDC-Arq está cumprindo com seus compromissos de preservação da integridade e demais compromissos firmados frente aos produtores.

[4.1.6] **Obter controle suficiente sobre os objetos digitais para preserva-los**: o RDC-Arq necessita obter o controle dos documentos a fim de efetuar as atividades necessárias para sua preservação, assim como para prover o acesso à comunidade designada. Isto requer o controle legal e físico/lógico, de modo que isto seja suficiente para tomada de decisões relativas às suas atividades.

[4.1.7] **Fornecer ao produtor/depositante respostas apropriadas aos pontos que foram definidos durante os processos de admissão**: o RDC-Arq deverá manter o produtor informado sobre os procedimentos de admissão,

de modo que seja possível demonstrar a conformidade com as questões definidas previamente.

[4.1.8] **Ter registros contemporâneos de ações e processos de administração que são relevantes para aquisição de conteúdo**: o RDC-Arq deve registrar todos os procedimentos administrativos para manter um histórico das ações realizadas, servindo para comprovar a execução de determinado procedimento. Ressalta-se que tais procedimentos administrativos são essenciais na presunção de autenticidade, e o seu registro adiciona confiabilidade ao ambiente informatizado.

[4.2] ADMISSÃO: CRIAÇÃO DO AIP

Durante a criação do AIP define-se um identificador único de nomenclatura geral para cada AIP ou classe de informação, que demonstra a preservação de suas propriedades significativas. As transformações dos SIP's em AIP's são descritas, além de manter os identificadores únicos previamente associados. Um contexto semântico entre objetos digitais armazenados é estabelecido, e as informações de representação admitidas são registradas. Assim, devem-se documentar os processos de aquisição e gerenciamento dos metadados de preservação para as informações de conteúdo associadas, além de adquirir outros metadados necessários à preservação. O processo de criação do AIP ainda requer a verificação da compreensão da informação de conteúdo, da integridade e da precisão de cada AIP. De forma complementar, deve-se fornecer um mecanismo para auditoria da integridade dos materiais custodiados, e manter registros de metadados de processos administrativos pertinente à preservação.

[4.2.1] **Ter para cada AIP ou classe de AIP preservada, uma definição associada adequada para analisar o AIP e contemplar suas necessidades de preservação de longo prazo**: o RDC-Arq terá mais informações e assim poderá complementar as atividades de preservação.

[4.2.1.1] **Ter capacidade de identificar qual definição se aplica para qual AIP**: o RDC-Arq pode usar o método que considerar mais apropriado para associar as definições e os AIP's.

[4.2.1.2] **Ter uma definição adequada de cada AIP para sua preservação no longo prazo, permitindo identificar e analisar todos os componentes necessários dentro desse AIP**: o RDC-Arq deverá identificar e manter uma relação dos componentes necessários para preservar as propriedades significativas dos AIP's. Além disso, será necessário demonstrar, periodicamente por meio da revisão, que tais componentes satisfazem as necessidades de preservação.

[4.2.2] **Ter uma descrição de como o AIP é construído a partir SIP:** permite que o RDC-Arq demonstre que a informação de conteúdo armazenada na forma de AIP está em conformidade com aquela submetida originalmente pelo produtor na forma de SIP. Para tal, é necessário detalhar como ocorreram as transformações necessárias ao armazenamento. Esta descrição corrobora para demonstrar a autenticidade das informações de conteúdo, pois justifica as suas possíveis transformações, relacionando-as à necessidade de alterar a informação digital para melhor preservá-la. O registro destas ações também auxilia no processo de presunção de autenticidade dos documentos.

[4.2.3] **Documentar a disposição final de todos os SIP's**: o RDC-Arq deve registrar os procedimentos relativos ao tratamento dos SIP's, e assim, indicar sua localização enquanto AIP ou eliminação, em casos especiais.

[4.2.3.1] **Seguir os procedimentos documentados, caso um SIP não seja incorporado em um AIP ou descartado, deve-se justificar o motivo**: o RDC-Arq terá de registrar o motivo das exclusões de SIP's submetidos de forma equivocada, quando houver, visto que os documentos arquivísticos submetidos/recolhidos ao RDC-Arq não devem ser eliminados ou recusados de forma arbitrária. Logo, é necessário justificar a natureza do equívoco/erro

ou mesmo inconformidade dos SIP's com as normas de submissão definidas previamente pelo RDC-Arq.

[4.2.4] **Utilizar uma convenção que gera identificadores únicos para todos os AIP's**: com os identificadores únicos para cada AIP e componentes, o RDC-Arq poderá fazer verificações, inibindo duplicações.

[4.2.4.1] **Identificar cada AIP de forma exclusiva no repositório**: garante precisão no processo de busca e recuperação da informação de conteúdo

[4.2.4.1.1] **Ter identificadores exclusivos**: evita duplicações dos AIP's e otimiza a sua localização no sistema.

[4.2.4.1.2] **Ceder e manter identificadores persistentes do AIP e de seus componentes, de modo a ser exclusivo dentro do contexto do repositório**: evita a dispersão dos componentes digitais relacionados ao AIP.

[4.2.4.1.3] **Descrever todos os processos utilizados para realizar alterações em tais identificadores**: acrescenta confiabilidade ao sistema de identificadores.

[4.2.4.1.4] **Fornecer uma lista completa de todos os identificadores e fazer verificações pontuais para identificar duplicações**: permite verificar continuamente a presença de informações duplicadas no RDC-Arq, além de localizar os conteúdos com precisão, desta forma, auxilia na otimização do trabalho técnico e do armazenamento.

[4.2.4.1.5] **O sistema de identificadores deve ser adequado para comportar a demanda atual do repositório e as previsíveis necessidades futuras, tais como números de objetos**: o RDC-Arq garante a capacidade de recuperar a informação de conteúdo desejada com alto grau de precisão, o que é essencial para que comunidade

designada demonstre confiabilidade quanto á preservação. A identificação está prevista pela Norma Brasileira de Descrição Arquivística (NOBRADE) (BRASIL, 2006), em seus elementos de descrição pode-se observar que o item "1 área de identificação" possui o subitem "1.1 código de referência" o qual tem como objetivo identificar a unidade de descrição. Esta identificação[3] perpassa, obrigatoriamente, o registro do código do país (BR), o código da entidade custodiador e o código específico da unidade de descrição (BRASIL, 2006). Com a Resolução nº 28, de 17 de fevereiro de 2009, publicada pelo Conarq, a instituição terá esta identificação ao realizar o Cadastro Nacional de Entidades Custodiadoras de Acervos Arquivísticos (CODEARQ) a qual deverá ser solicitada ao Conarq. Por consequência, os acervos cadastrados terão códigos padronizados o que facilita a distinção entre as instituições cadastradas. Esta resolução também recomenda o suso da NOBRADE aos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR) (BRASIL, 2009).

[4.2.4.2] **Ter um sistema de confiável de ligação/localização para encontrar o objeto identificado exclusivamente, independentemente da sua localização física**: o RDC-Arq deve localizar o AIP e seus respectivos componentes mesmo que sejam realizadas atualizações no sistema, na mídia ou local de armazenamento. Ou seja, deve haver um monitoramento contínuo capaz de recuperar tais informações.

[4.2.5] **Ter acesso a ferramentas e recursos para fornecer informação de representação de autoridade necessária para todos os objetos digitais armazenados**: identificar os formatos de arquivo dos objetos digitais a fim de fornecer a informações de representação necessária a comunidade designada.

[4.2.5.1] **Identificar o tipo de arquivo de todos os objetos de dados submetidos**: isto permite que o RDC-Arq controle os formatos de arquivo

[3] Por exemplo, o código "BR AN Q6.LEG.COR,TEL" pertence a instituição "Arquivo Nacional do Brasil", e corresponde a a subsérie Telegramas, nível 3,5, do fundo Floriano Peixoto, seção Governo Legal, série Correspondência (BRASIL, 2006).

em que os documentos são submetidos. Esta informação de monitoramento poderá ser útil para buscar melhores técnicas de tratamento para um determinado formato de arquivo.

[4.2.5.2] **Determinar a informação de representação necessária para tornar cada objeto de dados compreensível à comunidade designada**: o RDC-Arq deve reunir toda a informação necessária para a correta interpretação/representação dos objetos digital pela comunidade designada. Desta forma, além de cumprir as funções de preservação será necessário fornecer acesso de forma inteligível à documentação.

[4.2.5.3] **Ter acesso à informação de representação necessária**: o RDC-Arq deve buscar a informação de representação necessária junto aos produtores, desta forma, um processo de organização da informação determinará os componentes digitais que serão relacionados aos AIP's.

[4.2.5.4] **Assegurar que os requisitos da informação de representação são persistentemente associados aos objetos de dados relevantes**: o RDC-Arq terá a informação de representação suficiente para manter os objetos digitais acessíveis à comunidade designada. Para isto deverá ter acesso a ferramentas que executem tais atividades.

[4.2.6] **Ter processos documentados para aquisição de PDI, conforme os processos documentados, para sua informação de conteúdo associada**: o RDC-Arq deve assegurar a reunião de todos os componentes de PDI necessários, e manter um mecanismo padronizado para coleta destes dados.

[4.2.6.1] **Ter processos documentados para a aquisição de PDI**: o RDC-Arq definirá os procedimentos padronizados para adquirir a PDI necessária à representação da informação de conteúdo.

[4.2.6.2] **Executar processos documentados para a aquisição de PDI**: o RDC-Arq seguirá seus procedimentos de aquisição de PDI conforme definido previamente.

[4.2.6.3] **Assegurar que a PDI é persistentemente associada às informações do conteúdo relevantes**: o RDC-Arq irá registrar informações adicionais e autorizadas, capazes de corroborar com a autenticidade dos conteúdos. Este fluxo de constante associação adicionará confiabilidade aos procedimentos de aquisição de PDI.

[4.2.7] **Assegurar que as informações de conteúdo do AIP, no momento de sua criação, são compreensíveis à comunidade designada**: é essencial que o RDC-Arq crie AIP's já compreensíveis a comunidade designada. Assim, caso haja solicitações de acesso, o repositório irá dispor de toda a informação necessária que permita aos usuários interpretar corretamente a informação de conteúdo.

[4.2.7.1] **Ter um processo documentado para testar, no momento de sua criação, se a informação de conteúdo do AIP é compreensível à comunidade designada**: o RDC-Arq deve verificar logo no momento da criação do AIP, se a informação de conteúdo está acessível à comunidade designada. Assim, poderá inserir mais informações caso seja necessário para representar/interpretar as informações de conteúdo.

[4.2.7.2] **Executar um teste para cada classe de informação de conteúdo dos AIP's**: após reunir todos os componentes considerados necessários para a compreensão da informação de conteúdo pela comunidade designada é preciso executar testes para verificar cada componente do AIP.

[4.2.7.3] **Em caso de falha no teste de compreensibilidade, o repositório deve colocar as informações de conteúdo dos AIP's no nível de compreensão necessário**: caso as informações de conteúdo do AIP não sejam compreensíveis à comunidade designada, o RDC-Arq ficará

responsável por buscar informações adicionais e acrescentá-las ao pacote AIP.

[4.2.8] **Verificar a integralidade e exatidão de cada AIP no momento de sua criação**: o RDC-Arq deve manter uma descrição capaz de relacionar o AIP armazenado com o SIP submetido pelo produtor, de modo que este consiga recuperar as informações de conteúdo com integridade e precisão.

[4.2.9] **Fornecer um mecanismo independente para verificar a integridade do conjunto de conteúdos do repositório**: o RDC-Arq deverá ter um mecanismo independente para verificar a integridade do acervo, identificando cada AIP e seus componentes relacionados. Isto é relevante para garantir princípios arquivísticos como o da proveniência e da integridade dos fundos. Tal verificação auxilia para reunir toda a informação necessária para a correta interpretação/representação das informações de conteúdo pela comunidade designada.

[4.2.10] **Ter registros contemporâneos das ações e processos de administração que são relevantes à criação do AIP**: o RDC-Arq demonstra que segue uma política de criação de AIP's previamente definida. Além disso, poderá registrar ações relevantes com o uso de metadados de preservação devidamente associados a todos os componentes digitais.

[4.3] PLANEJAMENTO DA PRESERVAÇÃO

Dentre as questões relacionadas ao planejamento da preservação, ressalta-se que o repositório irá identificar e documentar as estratégias de preservação executadas. Irá notificar quando a informação de representação adquirir risco de obsolescência, alterar os planos de preservação conforme os resultados do monitoramento, e podem fornecer evidências da eficácia do planejamento de preservação.

[4.3.1] **Ter uma documentação sobre as estratégias de preservação relevantes ao acervo**: tais estratégias definidas pelo RDC-Arq em seu plano estratégico de preservação buscam solucionar riscos como a degradação dos meios de armazenamento, a obsolescência das unidades de mídia, e a obsolescência ou inadequação da informação de representação (incluindo formatos de arquivo).Desta forma, o repositório terá registrado todas as estratégias pertinentes à preservação e manutenção da autenticidade dos documentos.

[4.3.2] **Ter mecanismos para monitorar o ambiente de preservação**: através do monitoramento do ambiente de preservação o RDC-Arq poderá tomar as decisões mais adequadas para realizar a manutenção dos objetos digitais, e minimizar os efeitos da obsolescência. Assim, irá assegurar a que a comunidade designada será capaz de compreender e utilizar os materiais preservados.

> [4.3.2.1] **Ter mecanismos para monitorar e notificar quando a informação de representação está inadequada à compreensão dos dados pela comunidade designada**: o RDC-Arq deve manter mecanismos para verificar a obsolescência no que tange a base de conhecimento da comunidade designada. E desta forma, poderá atualizar ou adicionar a informação de representação necessária para garantir a correta interpretação/representação da informação de conteúdo.

[4.3.3] **Ter mecanismos para mudar o plano de preservação conforme os resultados das atividades de monitoramento**: com o monitoramento do ambiente de preservação, o RDC-Arq terá condições previstas para alterar o planejamento definido e se adequar aos imprevistos e as novas necessidades que surjam durante a execução do plano de preservação. Da mesma, forma poderá reunir informações adicionais que corroborem com a preservação e interpretação dos objetos digitais.

[4.3.3.1] **Ter mecanismos para criar, identificar ou reunir qualquer informação de representação adicional que seja necessária**: o RDC-Arq identificará a informação de representação e os formatos de arquivo potencialmente obsoletos e, por conseguinte, proceder à atualização ou adicionar maiores informações que auxiliem no processo de preservação.

[4.3.4] **Apresentar provas da eficácia das atividades de preservação**: o RDC-Arq demonstrará capacidade de preservação continuada da informação de conteúdo ao permitir auditorias (testes aleatórios) que comprovam a eficácia dos métodos, além de garantir a sua correta representação/interpretação.

[4.4] PRESERVAÇÃO DO AIP

Preservar as informações de conteúdo dos AIP's requer a implementação de estratégias de preservação documentadas por metadados adequados registrando as ações aplicadas para especificar o seu tratamento. Além disso, o RDC-Arq deve monitorar continuamente a integridade dos AIP's, e manter o registro de ações e processos administrativos pertinentes à preservação.

[4.4.1] **Ter especificações sobre a forma como os AIP's são armazenados até o nível de *bit***: o RDC-Arq poderá recuperar as informações de conteúdo do AIP devido ao conhecimento sobre os formatos, de modo que poderá extrair a informação contida no AIP em qualquer tempo.

[4.4.1.1] **Preservar as informações de conteúdo do AIP**: o RDC-Arq manterá um registro de todas as transformações realizadas sobre as informações de conteúdo recebidas. Caso sejam necessárias conversões ou informações adicionais, todos estes procedimentos estarão registrados, compondo um testemunho do histórico dos objetos digitais. Logo, este registro irá garantir a autenticidade dos conteúdos em custódia.

[4.4.1.2] **Monitorar ativamente a integridade do AIP**: O RDC-Arq manterá um processo regular de verificação da integridade para cada objeto digital admitido e adicionará informações de fixidez, as quais irão auxiliar na presunção de autenticidade, além de reparar os objetos que estão corrompidos.

[4.4.2] **Ter registros contemporâneos das ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIP's**: o RDC-Arq deverá demonstrar, através de documentação e registros de metadados, que todas as ações relevantes são realizadas. Tal procedimento agregará confiabilidade às decisões administrativas relacionadas aos AIP's.

[4.4.2.1] **Ter procedimentos definidos para todas as ações tomadas em um AIP**: o RDC-Arq deve respeitar uma variabilidade limitada, a qual é um parâmetro entre as necessidades de alterar as informações de conteúdo e de manter as propriedades significativas. Com isto, a informação de conteúdo poderá sofrer alterações desde que mantenham as propriedades significativas requeridas para manutenção da sua autenticidade. Logo, as transformações realizadas pelo repositório não devem descaracterizar os objetos digitais com relação à sua representação, para isto, deve-se considerar um conjunto de alterações aceitáveis, e registrar todas as ações de alteração.

[4.4.2.2] **Demonstrar que as medidas tomadas em um AIP estão em conformidade com as especificações dessas ações**: quaisquer ações que afetem os conteúdos armazenados no RDC-Arq devem seguir procedimentos previamente estabelecidos, além de serem registrados por metadados. Desta forma, é possível demonstrar que as ações registradas pelos metadados estão em conformidade com o que foi previamente definido como "alterações aceitáveis".

[4.5] GESTÃO DA INFORMAÇÃO

Na gestão da informação o RDC-Arq captura ou cria os metadados de descrição necessários, e os associa ao AIP, para que a comunidade designada identifique os materiais de interesse. Assim, será capaz de demonstrar que a integridade referencial é criada e mantida entre todos os AIP's e suas informações descritivas associadas.

[4.5.1] **Especificar os requisitos mínimos de informação para permitir que a comunidade designada descubra e identifique o material de interesse**: o RDC-Arq deve acrescentar informações descritivas aos objetos digitais admitidos, de modo a auxiliar no processo de busca e recuperação da informação de conteúdo desejada pela comunidade designada. Logo, ressalta-se a necessidade de definir padrões de metadados assim como um vocabulário controlado para otimizar a precisão das buscas.

[4.5.2] **Capturar ou criar informação descritiva mínima e assegurar que ela está associada ao AIP**: o RDC-Arq deverá associar a informação descritiva necessária para cada AIP, esta informação adicional não precisa, necessariamente, estar inserida no pacote de informação. No entanto, é essencial que a informação descritiva esteja relacionada com cada AIP, e poderá atuar por meio de identificadores únicos para estes. Da mesma forma, a informação descritiva poderá fornecer detalhes adicionais relacionados às responsabilidades advindas do processo de admissão de conteúdos, ressalta-se que no caso do RDC-Arq, a descrição seguira os padrões preconizados pela Arquivística.

[4.5.3] **Manter ligação bidirecional entre cada AIP e sua informação descritiva**: o RDC-Arq deve estabelecer e manter informações descritivas associadas para cada AIP. Com uma relação bidirecional, pode-se localizar a informação descritiva através do AIP, como também, pode-se localizar o AIP a partir da informação descritiva.

[4.5.3.1] **Manter associação entre o AIP e as suas informações descritivas ao longo do tempo**: o RDC-Arq deve identificar qualquer interrupção entre os dados e a informação descritiva associada, para assim, garantir que ela pode ser restaurada, e com isso, os AIP's poderão ser recuperados.

[4.6] GESTÃO DE ACESSO

Com a gestão de acesso, o repositório irá documentar e comunicar opções de acesso e entrega que estão disponíveis à comunidade designada. Todas as solicitações de acesso devem são registradas, e visam atender aos requisitos do repositório e dos produtores, além de cumprir os acordos relacionados às condições de acesso. A gestão de acesso irá definir e implementar uma política de acesso segura via sistema de gerenciamento, aos contratos de depósito. Desta forma, irá demonstrar que todas as solicitações de acesso resultam em uma resposta de aceitação ou rejeição, e assim, registrar todas as falhas de gerenciamento de acesso e analisar os casos de negação de acesso.

[4.6.1] **Cumprir políticas de acesso**: o RDC-Arq deverá demonstrar que cumpre as políticas de acesso, de modo que atende todas as solicitações da comunidade designada e mantem mecanismos de autenticação de usuários para controlar o acesso.

[4.6.1.1] **Registrar e analisar todas as falhas e anomalias de gerenciamento de acesso**: o RDC-Arq irá descobrir todas as falhas relacionadas ao acesso que afetam a sua confiabilidade. Com a identificação das anomalias e vulnerabilidades o repositório poderá concentrar esforços para solucionar estas falhas.

[4.6.2] **Seguir políticas e procedimentos que permitam a disseminação objetos de digitais os quais sejam rastreáveis aos originais, com evidência de sua autenticidade**: o RDC-Arq deverá gerar pacotes DIP's em conformidade com os AIP's dos quais são derivados. Logo, torna-se

fundamental definir procedimentos padronizados para a criação do DIP garantindo a sua fidedignidade frente ao AIP.

[4.6.2.1] **Registar e agir de acordo com relatórios de problemas sobre erros nos dados ou respostas para usuários**: O RDC-Arq deverá considerar os relatórios de erros sobre as solicitações de acesso. Sendo assim, a sua confiabilidade estará relacionada à capacidade de investigar e tomar decisões com relação a tais erros. Logo, as ações tomadas pelo repositório para solucionar problemas de acesso irão agregar confiança frente à comunidade designada.

[5] INFRAESTRUTURA E SEGURANÇA DA GESTÃO DE RISCOS

A seção de infraestrutura e segurança da gestão de riscos compreende aspectos relacionados à infraestrutura técnica do sistema, e gestão de riscos.

[5.1] GESTÃO DE RISCOS DE INFRAESTRUTURA TÉCNICA

As funções de repositório devem ser suportadas pelos principais sistemas operacionais, de modo que seja possível assegurar suporte de *hardware* e *software* adequado às funcionalidades de *backup* e suficientes aos conteúdos armazenados. Assim, é possível gerenciar as quantidades e as localizações das cópias de todos os objetos digitais, e sincronizar as cópias dos objetos digitais. Além disso, o repositório irá detectar a corrupção ou perda de *bits* por meio de mecanismos de análise de erro, e informar à administração todos estes incidentes e as medidas adotadas para reparar ou substituir os dados afetados. Os processos de atualização das mídias de armazenamento, do *hardware* e da segurança *software* devem ser definidos, e registrar a gestão de mudanças, sendo necessário um processo para testar o efeito de mudanças críticas ao sistema. Desta forma, o repositório possuirá tecnologias de *hardware* e *software* apropriadas aos serviços que presta à comunidade designada, bem como, procedimentos para monitorar e avaliar a necessidade de mudanças nas tecnologias de *hardware* e/ou *software* utilizadas.

[5.1.1] **Identificar e gerir os riscos às suas operações de preservação e os objetivos associados com a infraestrutura do sistema**: o RDC-Arq deverá preconizar uma infraestrutura confiável, para isso, irá gerir os riscos relacionados às plataformas de *hardware* e *software*, buscando minimizar a dependência do sistema. Sua infraestrutura tecnológica deve ser expansível, além de possibilitar a execução de um plano de sucessão futuro, caso seja necessário.

[5.1.1.1] **Empregar relógios de tecnologia ou outra tecnologia para sistemas de notificação de monitoramento**: o RDC-Arq deve manter um monitoramento contínuo das plataformas tecnológicas, acompanhado de avaliação para identificar potenciais vulnerabilidades nos componentes do sistema.

[5.1.1.1.1] **Ter tecnologias de *hardware* adequadas aos serviços que presta para sua comunidade designada**: o RDC-Arq deverá manter plataformas de *hardware* adequadas para os serviços que presta, e considerar o *feedback* recebido par realizar ajustes no sistema. Além disso, deve-se ressaltar que a adequação dos componentes de *hardware* irá impactar em todas as funções do repositório.

[5.1.1.1.2] **Dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças na tecnologia de *hardware***: o RDC-Arq deverá monitorar as mudanças nas plataformas de *hardware* a fim manter uma infraestrutura capaz de realizar suas funções relativas a admissão, armazenamento e acesso. O ponto fundamental deste requisito é manter a interoperabilidade entre a plataforma de *hardware* e as funções executadas pelo repositório para desenvolvê-las conforme o esperado.

[5.1.1.1.3] **Dispor de procedimentos para avaliar quando é necessário atualizar o *hardware* atual**: o RDC-Arq deverá antecipar as atualizações

de *hardware*, ao manter um constante monitoramento do sistema, verificando meios para reduzir custos e falhas.

[5.1.1.1.4] **Ter procedimentos, compromissos e financiamentos para substituir *hardware* quando a avaliação indicar tal necessidade**: o RDC-Arq deve realizar a substituição do *hardware* logo após identificar tal necessidade. Sendo assim, deve haver o compromisso da instituição, de modo que o RDC-Arq disponha de recursos financeiros suficientes, como também poderá demonstrar que o novo *hardware* será capaz de economizar recursos no decorrer de seu uso.

[5.1.1.1.5] **Ter tecnologias de *software* apropriadas para os serviços que proporciona a sua comunidade designada**: o RDC-Arq deve manter as tecnologias de *software* apropriadas para desempenhar as funções como interfaces e ferramentas para migração. Logo, é preciso considerar, em especial, o *feedback* da comunidade designada em relação aos *softwares* utilizados para a localização e recuperação/interpretação da informação de conteúdo.

[5.1.1.1.6] **Dispor de procedimentos para monitorar e receber notificações quando alterações de *software* são necessários**: o RDC-Arq deverá ter procedimentos pré-estabelecidos para verificar erros, vulnerabilidades e buscar atualizações para os *softwares* que integram o sistema de preservação digital. Além disso, é preciso atender a mudanças solicitadas pela comunidade designada para facilitar o processo de busca, recuperação e interpretação dos conteúdos. E por fim, buscar a interoperabilidade entre as plataformas de *hardware* e *software*.

[5.1.1.1.7] **Dispor de procedimentos para avaliar a necessidade de atualização do *software* atual**: o RDC-Arq deve antecipar a necessidade de atualização de *software* ao monitorar a evolução das plataformas tecnológicas. Tal ação irá minimizar riscos, evitar custos adicionais e melhorar o desempenho do sistema. Este procedimento previamente

estabelecido fundamenta-se em evitar que os *softwares* utilizados no sistema tornem-se obsoletos e comprometam as atividades desenvolvidas no âmbito do repositório.

[5.1.1.1.8] **Ter procedimentos, definir compromissos e garantir financiamentos para substituir o *software* quando a avaliação indica tal necessidade**: o RDC-Arq deverá substituir o *software* de modo a evitar falhas e consequentes perdas de dados. Assim, deve-se demonstrar a capacidade e os recursos suficientes para incorporar novas tecnologias.

[5.1.1.2] **Ter *hardware* adequado e suporte de *software* suficiente para realização do *backup* para proteger os conteúdos do repositório e acompanhar suas funções de preservação**: o RDC-Arq deve possuir plataformas de *hardware* e *software* capazes de realizar o *backup* dos objetos digitais e dos sistemas. Com o desenvolvimento de planos de *backup* será possível retomar as funções de preservação em todas as situações que ocorrerem falhas, independente do nível (objetos digitais, mídias de armazenamento, *hardwares* ou *softwares*).

[5.1.1.3] **Ter mecanismos eficazes para detectar a corrupção ou perda de *bits***: o RDC-Arq não deve tolerar perdas de dados em seus AIP e informações relacionadas. Para isto, deverá manter mecanismos que identifiquem as possíveis perdas ou corrupção de dados e executem a restauração.

[5.1.1.3.1] **Registrar e reportar à administração, todos os incidentes de corrupção ou perda de dados, e quais medidas de reparo/substituição de dados corrompidos/perdidos, deverão ser tomadas**: o RDC-Arq deve informar à administração sobre as perdas de dados e o respectivo processo de recuperação executado. Com isto, é possível identificar as fontes de falhas e reparar as vulnerabilidades em nível de *hardware*, *software*, suportes e procedimentos.

[5.1.1.4] **Ter um processo para registrar a disponibilidade de novas atualizações de segurança com base na avaliação do risco/benefício**: o RDC-Arq deve evitar as alterações e exclusões de conteúdos não autorizadas. Além disso, deve realizar atualizações de segurança em sua infraestrutura tecnológica para minimizar os riscos.

[5.1.1.5] **Deve definir processos para a mídia de armazenamento e/ou alteração de *hardware***: é fundamental que o RDC-Arq mantenha um processo de migração para as mídias de armazenamento com base nas estimativas de vida útil e análise de conservação física. Ressalta-se que no longo prazo, há maior dificuldade em se obter suporte aos componentes de *hardware*, o que aumenta a responsabilidade do RDC-Arq em buscar alternativas.

[5.1.1.6] **Identificar e documentar os processos críticos que afetam a capacidade de cumprir as responsabilidades obrigatórias**: o RDC-Arq deve ter um controle sobre todos os processos críticos que podem afetar suas responsabilidades obrigatórias, de modo seja possível compreender a necessidade destes fluxos de informação. Assim, é possível manter uma revisão buscando a melhora contínua destes procedimentos.

[5.1.1.6.1] **Ter um processo de gestão da mudança documentado, que identifica as alterações em processos críticos, os quais afetam potencialmente a capacidade do repositório para cumprir suas responsabilidades obrigatórias**: o repositório deverá ter especificações sobre os processos aplicados ao acervo relacionados às mudanças em seus processos críticos. Desta forma, é possível compreender como as mudanças foram efetuadas no sistema, e consequentemente, aprender com as mudanças. E caso seja necessário, será possível reverter ações que comprometam as atividades do RDC-Arq.

[5.1.1.6.2] **Ter um processo para testar e avaliar o efeito das mudanças em seus processos críticos**: o RDC-Arq deve avaliar as mudanças em seus processos críticos. Isto se torna essencial, pois estes processos se referem às funções primordiais que ele executa. Assim, as alterações devem ser testadas antes de sua implementação, após implementar devem ser monitoradas e caso seja necessário devem ser revertidas.

[5.1.2] **Gerir o número e a localização das cópias de todos digitais objetos**: o RDC-Arq deve ser capaz de gerir seus *backups*, de modo que consiga localizar as cópias de segurança de todos os objetos digitais custodiados. Esta localização deverá ser descrita com elevado grau de precisão, e assim considerar a localização física, o armazenamento lógico na mídia, nos sistemas e nos subsistemas.

[5.1.2.1] **Ter mecanismos para garantir que todas as cópias dos objetos digitais são sincronizadas**: o RDC-Arq deve garantir que possui cópias sincronizadas de todos os objetos digitais, para os casos em que seja necessário executar o plano para recuperação de desastres. Isto é fundamental para garantir a proteção do acervo contra sinistros e corrupções de dados, da mesma forma, o repositório deve identificar e reparar os dados corrompidos para que estes não sejam indevidamente sincronizados na forma de cópias de *backup*.

[5.2] GESTÃO DO RISCO DE SEGURANÇA

A gestão do risco de segurança auxilia o repositório a manter uma análise sistemática em relação a dados, sistemas, pessoal, planta física e segurança. O repositório determina funções, responsabilidades e autorizações relacionadas à implementação de mudanças no sistema, além de ter um plano de preparo e recuperação de desastres.

[5.2.1] **Manter uma análise sistemática dos fatores de risco da segurança associada a dados, sistemas, pessoal e instalações físicas**: o RDC-Arq deve manter uma análise contínua dos riscos relacionados ao ambiente de preservação como um todo. Isto compreende a segurança física e lógica dos dados, e sua relação com sistemas, pessoal e instalações físicas.

[5.2.2] **Implementar controles para tratar adequadamente cada um dos riscos de segurança definidos**: o RDC-Arq deve tratar cada um dos riscos identificados, para isto, pode usar normas como a ISO/IEC 27000:2018 e a ISO/IEC 17799:2005. Da mesma forma, pode-se manter um registro de problemas relacionados a ataques para prevenir sua recorrência e revisar constantemente os planos de emergência.

[5.2.3] **Definir papéis, responsabilidades e autorizações relacionadas com a implementação de mudanças no sistema**: o RDC-Arq deve atribuir as responsabilidades e recursos para implementar mudanças no ambiente. Neste sentido, as normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir, respectivamente, na atribuição de responsabilidades e posterior certificação.

[5.2.4] **Ter uma preparação adequada para desastres e um plano de recuperação documentado, incluindo pelo menos um *backup off-site* de todas as informações preservadas, juntamente com uma cópia fora do local do plano de recuperação**: o RDC-Arq deve manter o *backup* e uma cópia do plano de recuperação em um local seguro e separado do acervo, de modo a garantir a continuidade dos serviços do repositório. As normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir para minimizar os riscos do ambiente de preservação. Além disso, o repositório deve definir claramente o seu plano de desastres, considerando todos os riscos aos quais está sujeito. Desta forma, o plano de recuperação se tornará mais eficaz, caso seja necessário executá-lo.

5. CONCLUSÃO

Este manual realizou uma complementação dos requisitos do ACTDR de modo a acrescentar uma visão arquivística aos requisitos utilizados para auditoria de repositórios digitais. Sendo assim, o ACTDR é contextualizado para ser aplicado aos RDC-Arq's, considerando que este está em conformidade com o modelo OAIS e envolvido em uma cadeia de custódia confiável.

Inicialmente, o modelo OAIS foi abordado para destacar as suas responsabilidades obrigatórias, assim como, apresentar uma breve descrição dos fluxos de informação realizados pelas entidades funcionais. Posteriormente, ao abordar a cadeia de custódia documental, destacaram-se os principais requisitos e padrões arquivísticos a serem considerados na implementação de um sistema de gestão documental.

Após relacionar o RDC-Arq frente ao modelo OAIS e a cadeia de custódia documental, prosseguiu-se com a contextualização dos requisitos do ACTDR no âmbito da Arquivística. Assim, o manual fornece uma base para que arquivistas compreendam os critérios do ACTDR, no entanto, não substitui a leitura e compreensão do OAIS e do ACTDR. Desta forma, a após a contextualização de cada critério do ACTDR tem-se uma base auxiliar para que os arquivistas dialoguem com os demais profissionais envolvidos no planejamento e implementação de um RDC-Arq.

Dessa forma, estima-se incentivar o diálogo em torno dos RDC-Arq's, visto que a literatura sobre repositórios digitais, no sentido genérico do termo, está bem avançada; ao passo que a caracterização "repositório arquivístico" ainda carece de literatura própria. Por fim, este manual consiste em uma aproximação entre RDC-Arq, OAIS, ACTDR e cadeia de custódia documental; logo, objetiva incentivar a reflexão a auxiliar nos processos de planejamento e implementação de RDC-Arq's.

6. REFERÊNCIAS

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

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara técnica de normalização da descrição arquivística. **Norma brasileira de descrição arquivística (Nobrade)**. Rio de Janeiro: Arquivo Nacional, 2006.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. **Resolução nº 28, de 17 de fevereiro de 2009**. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from_info_index=21&infoid=273&sid=46>. Acesso em: 22 abr. 2018.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Reference Model for an Open Archival Information System (OAIS)**. Magenta Book. Washington, Jun. 2012. Disponível em: <http://public.ccsds.org/publications/archive/650x0m2.pdf>. Acesso em: 13 mai. 2014.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. Cadeia de custódia para documentos arquivísticos digitais. **Acervo**, Rio de Janeiro, v. 29, n. 2, p. 117-132, nov. 2016. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717>. Acesso em: 09 mai. 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721:2012**. Space data and information transfer systems: Open archival information system – Reference model.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 17799:2005**. Information technology: security techniques – Code of practice for information security management.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000:2018**. Information technology: security techniques – Information security management systems: overview and vocabulary.

SOBRE O AUTOR

Henrique Machado dos Santos, bacharel em Arquivologia e mestre em Patrimônio Cultural pela Universidade Federal de Santa Maria (UFSM). Atualmente é arquivista da Universidade Federal do Rio Grande (FURG), membro dos grupos de pesquisa: Gestão Eletrônica de Documentos Arquivísticos (GED/A) e Patrimônio Documental Arquivístico (PDA). Dedica-se à pesquisa de documentos digitais desde 2012, tendo publicado mais de 25 artigos em revistas científicas no Brasil e no exterior. Os principais temas abordados são: preservação de documentos arquivísticos digitais, diplomática contemporânea e gestão do conhecimento. Dentre seus principais trabalhos destacam-se:

- Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo[4];
- Políticas de preservação digital para documentos arquivísticos[5];
- Preservação de documentos arquivísticos digitais: reflexões sobre o uso de padrões abertos nos acervos[6];
- As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital[7];
- Novos rumos da preservação digital: das estratégias aos sistemas informatizados[8];
- Estratégias de preservação digital para documentos arquivísticos: uma breve reflexão[9];
- Cadeia de custódia para documentos arquivísticos digitais[10];
- Os impactos da obsolescência tecnológica frente à preservação de documentos digitais[11];

[4] www.portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2341

[5] www.portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2542

[6] dx.doi.org/10.22201/iibi.24488321xe.2018.74.57905

[7] www.biblios.pitt.edu/ojs/index.php/biblios/article/view/215

[8] dx.doi.org/10.5195/biblios.2018.326

[9] www.bad.pt/publicacoes/index.php/cadernos/article/view/1225

[10] www.revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717

- Um diálogo entre arquivo, conhecimento e tecnologia[12];
- Da preservação digital ao acesso à informação: uma breve revisão[13];
- Os fundamentos da diplomática contemporânea na preservação de documentos arquivísticos digitais[14];
- O documento arquivístico digital enquanto fonte de pesquisa[15];
- O documento digital no contexto das funções arquivísticas[16];
- Documentos digitais: o desafio da preservação[17].

Contato

E-mail: henrique.hms.br@gmail.com

Academia.com: furg.academia.edu/HenriqueMachadodosSantos

Google Scholar: scholar.google.com.br/citations?user=0VLAu8sAAAAJ&hl=pt-BR

Orcid: orcid.org/0000-0002-2497-7321

Lattes: lattes.cnpq.br/2224553749651399

ResearchGate: www.researchgate.net/profile/Henrique_Santos17

Redalyc: www.redalyc.org/autor.oa?id=539

Researcherid: www.researcherid.com/rid/B-2053-2016

Scopus: www.scopus.com/authid/detail.uri?authorId=56717359300

Blog: gestaodedocumentoseinformacoes.blogspot.com.br/

[11] www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5550

[12] www.biblios.pitt.edu/ojs/index.php/biblios/article/view/231

[13] www.ojs.letras.up.pt/index.php/paginasaeb/article/view/2836

[14] www.seer.furg.br/biblos/article/view/4825

[15] www.portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2688

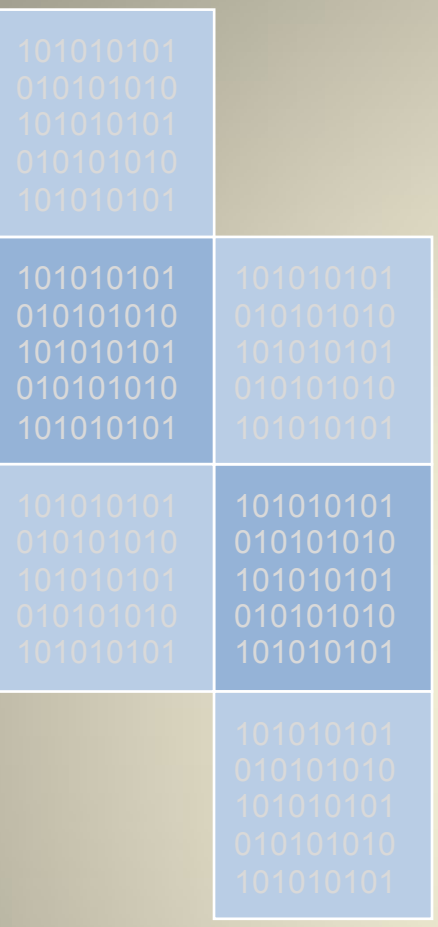
[16] www.ojs.letras.up.pt/index.php/paginasaeb/article/view/1477

[17] www.assinaturadigital.cienciahoje.org.br/revistas/reduzidas/330/?revista=330#20

Manual para Auditoria de Repositórios Arquivísticos Digitais Confiáveis

Henrique Machado dos Santos

Bacharel em Arquivologia e mestre em Patrimônio Cultural pela Universidade Federal de Santa Maria. Atualmente é arquivista da Universidade Federal do Rio Grande, membro dos grupos de pesquisa: Gestão Eletrônica de Documentos Arquivísticos e Patrimônio Documental Arquivístico. Dedica-se à pesquisa de documentos digitais desde 2012, tendo publicado mais de 25 artigos em revistas científicas no Brasil e no exterior. Os principais temas abordados são: preservação de documentos arquivísticos digitais, diplomática contemporânea e gestão do conhecimento.



O presente manual tem por objetivo fornecer subsídios teóricos para compreensão do modelo OAIS e do padrão ACTDR, com ênfase nos requisitos para auditoria de RDC-Arq's. Da mesma forma, busca-se esclarecer os requisitos arquivísticos que estão subentendidos no RDC-Arq, realçando sua pertinência durante o processo de auditoria.