

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”  
FACULDADE DE FILOSOFIA E CIÊNCIAS  
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO**

**PAULA REGINA VENTURA AMORIM GONÇALEZ**

**REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS: IDENTIFICAÇÃO DE  
REQUISITOS COM ÊNFASE NO ACESSO À INFORMAÇÃO**

**Marília - SP  
2017**

**PAULA REGINA VENTURA AMORIM GONÇALEZ**

**REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS: IDENTIFICAÇÃO DE REQUISITOS COM ÊNFASE NO ACESSO À INFORMAÇÃO**

Tese apresentada ao Programa de Pós-graduação em Ciência da Informação da Universidade Estadual Paulista - Campus de Marília, para obtenção do título de Doutor em Ciência da Informação.

**Área de Concentração:** Informação, Tecnologia e Conhecimento.

**Linha de Pesquisa:** Informação e Tecnologia

Financiamento: CAPES

Orientadora: Prof.<sup>a</sup> Dr.<sup>a</sup> Maria José Vicentini Jorente

**Marília - SP  
2017**

Ficha catalográfica elaborada pela Seção Técnica de Aquisição e Tratamento da Informação  
Faculdade de Filosofia e Ciências (FFC/UNESP - Marília)

Gonçalez, Paula Regina Ventura Amorim.

G635r Repositórios arquivísticos digitais confiáveis: identificação de requisitos com ênfase no acesso à informação / Paula Regina Ventura Amorim Gonçalez. – Marília, 2017.  
165 f. ; 30 cm.

Orientador: Maria José Vicentini Jorente.

Tese (Doutorado em Ciência da Informação) – Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, 2017.

*Bibliografia: f. 151-162*

1. Repositórios institucionais. 2. Arquivos e arquivamento (Documentos) – Certificados e licenças. 3. Conselho Nacional de Arquivos (Brasil). 4. Arquivos e arquivamento (Documentos) – Normas. 5. Organização Internacional de Normalização. 6. Informação arquivística. I. Título.

**CDD 025.171**

**PAULA REGINA VENTURA AMORIM GONÇALEZ**

**REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS: IDENTIFICAÇÃO DE REQUISITOS COM ÊNFASE NO ACESSO À INFORMAÇÃO**

Tese apresentada ao Programa de Pós-graduação em Ciência da Informação da Universidade Estadual Paulista - Campus de Marília, para obtenção do título de Doutor em Ciência da Informação.

**Área de Concentração:** Informação, Tecnologia e Conhecimento.

**Linha de Pesquisa:** Informação e Tecnologia

**Aprovada em 06 de março de 2017**

**BANCA EXAMINADORA**

---

**Dr.<sup>a</sup> Maria José Vicentini Jorente** - *Orientadora*  
Universidade Estadual Paulista (UNESP – Campus Marília)

---

**Dr.<sup>a</sup> Ana Cristina Albuquerque**  
Universidade Estadual de Londrina (UEL)

---

**Dr.<sup>a</sup> Brígida Maria Nogueira Cervantes**  
Universidade Estadual de Londrina (UEL)

---

**Dr.<sup>a</sup> Silvana Aparecida Borsetti Gregório Vidotti**  
Universidade Estadual Paulista (UNESP – Campus Marília)

---

**Dr. Ricardo César Gonçalves Sant'Ana**  
Universidade Estadual Paulista (UNESP – Campus Marília)

Dedico este trabalho ao Senhor Jesus, pela força e amparo em todos os momentos.  
A Ele toda Honra e toda Glória.  
Ao Jorge, pelo apoio incondicional e  
À minha família, sempre presente, me apoiando e me incentivando. Eu os amo muito!

## AGRADECIMENTOS

A Deus, por permitir a conquista de mais um sonho, por colocar pessoas tão especiais as quais sem vocês essa realização seria impossível.

Aos meus pais Rubens e Ana que apesar de não estarem mais aqui, passaram a vida demonstrando que todo esforço para o conhecimento valem a pena.

Ao meu esposo Jorge, companheiro de todos os momentos, que fez-se presente e incentivou-me mesmo a quilômetros de distância. Sem o seu carinho e compreensão, esse sonho não seria possível.

À orientadora: Prof.<sup>a</sup> Dr.<sup>a</sup> Maria José Vicentini Jorente, pela confiança e incentivo ao meu trabalho.

À Prof.<sup>a</sup> Dr.<sup>a</sup> Brígida Maria Nogueira Cervantes, pelo profissionalismo impecável, pela mansidão e sabedoria de suas palavras e pela amizade.

À Prof.<sup>a</sup> Dr.<sup>a</sup> Ana Cristina Albuquerque, por compartilhar sua amizade e conhecimento em todos os momentos em que é possível estarmos juntas.

A Prof.<sup>a</sup> Dr.<sup>a</sup> Silvana Aparecida Borsetti Gregório Vidotti, pela amizade, por sempre me atender prontamente, pela gentileza de participar da minha banca de mestrado e de doutorado e pela ISO...

Ao Prof. Dr. Ricardo Cezar Sant'Ana, pelo acolhimento e confiança desde o mestrado, pelo sorriso, pela palavra amiga e pelas reflexões.

A Prof.<sup>a</sup> Dr.<sup>a</sup> Plácida Leopoldina Ventura Amorim da Costa Santos, minha irmã, exemplo de professora e pesquisadora, pelo incentivo e apoio incondicional em todos os momentos.

Aos professores do curso de Pós-Graduação em Ciência da Informação pelos valiosos ensinamentos.

Ao Edevaldo Donizeti dos Santos pela diagramação do texto, disponibilidade e gentileza.

Aos meus filhos Giovanna, Isabella e Guilherme, pela compreensão com a minha ausência mesmo estando no mesmo espaço físico.

Aos meus queridos amigos: Caio, Felipe, Karu, Angela, Janice, Ana Maria, Ana Paula, Fábio, Sandra, Rachel, pelos artigos, pelos momentos compartilhados, pelo apoio, pelas risadas, pelos cafezinhos, pelas alegrias, pelos desabafos...

Aos professores e funcionários do Departamento de Ciência da Informação da Universidade Estadual de Londrina pelo acolhimento e carinho.

Muito obrigada!!!

GONÇALEZ, Paula Regina Ventura Amorim. **Repositórios arquivísticos digitais confiáveis**: identificação de requisitos com ênfase no acesso à informação. 2017. 166 f. Tese (Doutorado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2017.

## RESUMO

As Instituições Arquivísticas são desafiadas a constante atualização no uso das Tecnologias de Informação e Comunicação (TIC) para organizar, preservar e disponibilizar de maneira confiável seu acervo documental que é gerado em grandes quantidades e em diferentes suportes. Na atualidade, os acervos arquivísticos são híbridos, isto é, são compostos por documentos nascidos digitais, digitais e analógicos. Isso exige das instituições a otimização de seus serviços, ainda mais no que se refere ao atendimento ao usuário que almeja ter satisfeitas suas necessidades informacionais de maneira fácil, rápida e segura. Nesse cenário, o objetivo deste trabalho é analisar o conjunto de atributos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) e a vinculação do arquivista como membro integrante de uma equipe de trabalho na orientação dos requisitos com ênfase ao acesso à informação. Optou-se como procedimento metodológico pelo estudo teórico fundamentado nos princípios da Arquivologia. A etapa exploratória é realizada a partir da análise da Resolução 39 do CONARQ (Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq) e da ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*) que fazem recomendações técnicas para serem utilizadas como base para que repositórios digitais sejam certificados confiáveis ou que possibilitem a medição da confiabilidade do repositório. Os resultados apresentam as ações do arquivista para o acesso a documentos e informações arquivísticas e o cotejamento entre a Norma ISO 16363:2012 e a Recomendação 39 do CONARQ. Assim, o estudo resultou em um conjunto de recomendações para a certificação de Repositórios Arquivísticos Digitais com um recorte focado na identificação de requisitos com ênfase no acesso à informação. Por fim, é apresentado um conjunto de informações para que o arquivista possa fazer a medição da certificação de confiabilidade de um repositório digital ou para pedir sua certificação de confiabilidade.

**Palavras chave:** Instituições Arquivísticas. Repositórios Arquivísticos Digitais. Resolução 39 CONARQ. Norma ISO 16363:2012. Repositórios Confiáveis.

GONÇALEZ, Paula Regina Ventura Amorim. **Trusted digital archive repositories: Identification of requirements with emphasis on access to information.** 2017. 166 f. Tese (Doutorado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2017.

### **ABSTRACT**

Archival institutions are constantly challenged to update the use of Information and Communication Technologies (ICT) to reliably organize, preserve and provide their document collections that are generated in large quantity and in different media. Currently, the archival collections are hybrids, ie they are composed of documents that were originally digital, converted to digital, and analog. This requires that the institutions optimize their services, especially as regards to service to the user who aims to have his / her information needs satisfied easily, quickly and safely. In this scenario, the objective of this study is to analyze the set of essential attributes for the deployment of Trusted Digital Archival Repositories (TDARs) and the linking of the archivist as a member of a work team in guiding the requirements with emphasis on access to information. The methodological procedure was chosen by theoretical study grounded on the principles of Archivology. The exploratory stage is carried out from the analysis of Resolution 39 of CONARQ (Guidelines for the implementation of Trusted Digital Archival Repositories TDARs) and ISO 16363: 2012 (*Space data and information transfer systems - Audit and certification of trustworthy digital repositories*) that make technical recommendations used as a basis for digital repositories being certified as reliable or allow the measurement of repository reliability. The results present the archivist's actions for access to archival documents and information and the comparison between ISO 16363: 2012 and Recommendation 39 of CONARQ. Thus, the study resulted in a set of recommendations for certification of Digital Archival Repositories with a focus on identifying requirements with an emphasis on access to information. Finally, a set of information is presented so that the archivist can measure reliability of the certification of a digital repository or ask for its reliability certification.

**Keywords:** Digital Archival Repositories. Recommendation 39 of CONARQ. ISO 16363:2012. Trusted Repositories.

## LISTA DE FIGURAS

<b>Figura 1</b> - Ciclo de vida da Curadoria Digital.....	53
<b>Figura 2</b> - Ações para todo ciclo de vida da Curadoria Digital .....	54
<b>Figura 3</b> - Ações sequenciais do ciclo de vida da Curadoria Digital .....	56
<b>Figura 4</b> - Ações ocasionais do ciclo de vida da Curadoria Digital .....	58
<b>Figura 5</b> - Fases do ciclo de vida da Curadoria Digital.....	59
<b>Figura 6</b> - Modelo de ambiente de uma OAIS.....	85
<b>Figura 7</b> - Entidades funcionais OAIS .....	86
<b>Figura 8</b> - Modelo Cornell para atributos de repositório digital confiável .....	88
<b>Figura 9</b> - Categorização do termo acesso: ISO 16363:2012 e Resolução 39 do CONARQ.....	104

## LISTA DE QUADROS

<b>Quadro 1</b> - Países que adotaram Leis de Acesso à Informação .....	63
<b>Quadro 2</b> - Ações do arquivista para o acesso a documentos e informações.....	74
<b>Quadro 3</b> - Categorização de termos em relação aos requisitos para RDC-Arq: ISO 16363:2012 e Resolução 39 do CONARQ .....	104
<b>Quadro 4</b> - Análise demonstrativa, itens compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 3 - Organização e Infraestrutura .....	113
<b>Quadro 5</b> - Análise demonstrativa, itens não compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 3 - Organização e Infraestrutura .....	115
<b>Quadro 6</b> - Análise demonstrativa, itens compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 4 - Gerenciamento do Objeto Digital.....	117
<b>Quadro 7</b> - Nomenclaturas utilizadas na Seção 4 - Gerenciamento do Objeto Digital .....	122
<b>Quadro 8</b> - Análise demonstrativa, itens não compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 4 - Gerenciamento do Objeto Digital.....	123
<b>Quadro 9</b> - Análise demonstrativa, itens compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 5 - Infraestrutura e Segurança na Gestão de Riscos .....	125
<b>Quadro 10</b> - Análise demonstrativa, itens não compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 5 - Infraestrutura e Segurança na Gestão de Riscos .....	127
<b>Quadro 11</b> - Recomendações de <i>checklist</i> para medição e/ou certificação de confiabilidade para RDC-Arq com ênfase no Acesso à Informação .....	131

## LISTA DE ABREVIATURAS E SIGLAS

AIP	<i>Archival Information Package</i>
CCSDS	<i>Consultative Committee for Space Data Systems</i>
CONARQ	Conselho Nacional de Arquivos
CPA	<i>Commission on Preservation and Access</i>
CTDE	Câmara Técnica de Documentos Eletrônicos
DCC	<i>Digital Curation Centre</i>
DUDH	Declaração Universal dos Direitos Humanos
DIBRATE	Dicionário Brasileiro de Terminologia Arquivística
DigCCurr	<i>Digital Curation Curriculum</i>
DIP	<i>Dissemination Information Package</i>
EAD	<i>Encoded Archival Description</i>
EUA	Estados Unidos da América
ICA	<i>International Council of Archives</i>
ICPSR	<i>Inter-University Consortium for Political and Social Research</i>
IFLA	<i>International Federation of Library Associations and Institutions</i>
IBICT	Instituto Brasileiro de Informação em Ciência e Tecnologia
IIB	Instituto Internacional de Bibliografia
IPHAN	Instituto do Patrimônio Histórico e Artístico Nacional
ISAAR -CPF	Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias
ISAD(G)	Norma Geral Internacional de Descrição Arquivística
ISDF	Norma Internacional para Descrição de Funções
ISDIAH	Norma Internacional para Descrição de Instituições com Acervo Arquivístico
ISO	Organização Internacional para Normalização
JISC	<i>Joint Information Systems Committee</i>
METS	<i>Metadata Encoding and Transmission Standard</i>
MIT	<i>Massachusetts Institute of Technology</i>
NARA	<i>National Archives and Records Administration</i>
NOBRADE	Norma Brasileira de Descrição Arquivística
OAI-PMH	<i>Open Archives Initiative - Protocol for Metadata Harvesting</i>

OAIS	<i>Open Archival Information System</i>
OCLC	<i>Online Computer Library Center</i>
PREMIS	<i>Preservation Metadata: Implementation Strategies</i>
RDC-Arq	Repositórios Arquivísticos Digitais Confiáveis
RDs	Repositórios Digitais
RLG	<i>Research Libraries Group</i>
SAAI	Sistema Aberto de Arquivamento de Informação
SINAR	Sistema Nacional de Arquivos
SIP	<i>Submission Information Package</i>
TIC	Tecnologias de Informação e Comunicação
TRAC	<i>Trustworthy Repository Audit Certification: Criteria and Checklist</i>
UNESCO	Organizações das Nações Unidas para Educação, Ciência e Cultura
XML	<i>eXtensible Markup Language</i>

## SUMÁRIO

1	INTRODUÇÃO .....	13
1.1	Problema.....	19
1.2	Dos objetivos.....	19
1.2.1	Objetivo geral .....	19
1.2.2	Objetivos específicos .....	19
1.3	Motivação e justificativa da pesquisa.....	20
1.4	Tese .....	22
1.5	Hipótese .....	22
1.6	Proposição .....	22
1.7	Metodologia.....	22
1.8	Estrutura do texto.....	24
2	PATRIMÔNIO CULTURAL .....	26
2.1	Patrimônio documental .....	30
2.2	Documento .....	35
2.3	Documento arquivístico.....	38
2.4	Documento digital .....	42
2.5	Curadoria Digital .....	44
2.6	Ciclo de vida da Curadoria Digital.....	52
3	ACESSO À INFORMAÇÃO E O ARQUIVISTA .....	61
3.1	Lei de Acesso à Informação - LAI.....	61
3.1.1	O direito do acesso à informação no Brasil .....	66
3.2	Saberes e fazeres do arquivista .....	71
4	CONFIABILIDADE EM ARQUIVOS DIGITAIS: UM CAMINHO PARA REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS .....	77
4.1	Repositórios digitais .....	77
4.2	Repositórios digitais confiáveis .....	82
4.3	Repositórios arquivísticos digitais confiáveis.....	91
5	DIRETRIZES NACIONAIS PARA REPOSITÓRIOS DIGITAIS CONFIÁVEIS .....	94
5.1	Resolução 39 do CONARQ .....	94
5.2	<i>Space data and information transfer systems -- Audit and certification of trustworthy digital - ISO 16363:2012.....</i>	99
5.3	Categorização do termo acesso na norma ISO 16363 e na Resolução 39 do CONARQ .....	102
5.4	Requisitos da ISO 16363:2012 e da Resolução 39 do CONARQ.....	111
6	RECOMENDAÇÕES PARA A CONSTRUÇÃO DE RDC-ARQ CONSIDERANDO AS DIRETRIZES DA NORMA ISO 16363:2012 E A RESOLUÇÃO 39 DO CONARQ BASEADAS NO ACESSO À INFORMAÇÃO .....	129
7	CONSIDERAÇÕES FINAIS .....	146
	REFERÊNCIAS.....	152
	APÊNDICE A .....	164

## 1 INTRODUÇÃO

As mudanças proporcionadas pela sociedade da informação desafiaram os cidadãos, a partir do século XX, a importantes alterações de hábitos no que tange ao uso da informação, seja na vida pessoal ou no desenvolvimento de sua profissão. Esse novo cenário imprimiu um novo ritmo no processo de modernização das estruturas e agilidade na prestação de serviços em todas as áreas da sociedade.

As Instituições arquivísticas, desde seus primórdios, buscam organizar, preservar e disponibilizar os documentos criados pela humanidade, visto que no decorrer de sua história, tais instituições fazem o registro de suas atividades para que esse sirva como evidência ou prova de algum fato ocorrido. Assim, não somente dão aderência para fundamentação das ações, como também explicam os fatos ocorridos.

Segundo Vivas Moreno (2004, p. 77, tradução nossa), “[...] não se trata apenas da história dos arquivos ou das teorias fundamentadas por ele, mas da *práxis* política dos diferentes métodos administrativos [...]”, afirmando, também, que o fator predominante para a existência dos arquivos foi o surgimento da escrita, pois, a partir daquele momento, o homem registrou, conservou e comunicou por escrito suas relações como ser social, sendo que tal registro poderia ter ainda uma posterior utilização.

O que nos leva a concluir que o arquivo surgiu para que houvesse um controle do fluxo informacional e conseqüentemente do poder. Ainda que seja bastante radical, essa afirmação também é partilhada por Derrida (2001, p. 12), quando ele nos apresenta o significado da palavra Arquivo, apontando que ela vem do grego *Arkhêion*, o que:

[...] inicialmente era uma casa, um domicílio, um endereço, a residência dos magistrados superiores, os arcontes, aqueles que comandavam. Aos cidadãos que detinham e assim denotavam o poder político, reconheciam-se no direito de fazer ou de representar a lei. Levada em conta sua autoridade publicamente reconhecida, era seu lar, nesse lugar que era a casa deles (casa particular, casa de família ou casa funcional) que se depositavam então os documentos oficiais.

Os arcontes foram os primeiros guardiões dos documentos oficiais e como magistrados tinham o poder da interpretação dos arquivos, além da segurança física, da custódia e do suporte; assim, detinham o poder da guarda e de interpretação dos documentos que evocam e convocam à lei. Nesse contexto, nessa domicialização, surgiram os arquivos, na passagem do institucional para o público (DERRIDA, 2001)

Para Sargentini (2008, p. 110), ao reunir, organizar e selecionar, “[...] já estabelece, impondo sua ótica os recortes que comporão o arquivo”. Dessa maneira, desde seus primórdios, os arquivos se destacam como casas de memória, documentos e poder. Ao determinarem quais informações/documentos serão expostos e quem terá o acesso, interferindo, diretamente na vida dos sujeitos.

Chagas (2002, p. 146) aponta que o papel dos arquivos “[...] não é apenas o de guarda, e que, portanto, podem trabalhar a favor da democratização da produção de novos conjuntos de bens culturais, de novos saberes até então não cogitadas”.

Refletimos então sobre os usuários dos arquivos, visto que, o acesso às informações e aos documentos é a última etapa da função dos arquivos, pois, no que concerne ao acesso à informação Barros e Neves (2009, p. 5) também concordam que a função dos arquivos é tornar público e disponíveis as informações, e pontuam: o arquivo é “[...] um lugar para a construção do saber, [...] permite o acesso do pesquisador ao objeto de pesquisa”.

Nesse contexto, os arquivos são locais que abrigam a memória e o patrimônio cultural de uma sociedade, portanto precisam ser disponibilizados de maneira rápida, fácil e acessível a toda comunidade, contribuindo, dessa forma, para que a história possa ser conhecida, a memória construída e os arquivos se tornem referência para o empoderamento dos sujeitos.

Segundo Bellotto (2004, p. 23), “No universo da administração e da história reside a própria razão de ser dos arquivos públicos na sua característica dinâmica: a do ciclo vital dos documentos”. Assim, arquivos administrativos custodiam documentos produzidos e recebidos por uma instituição. Durante o exercício de suas funções, os documentos são organizados de maneira orgânica e cumulativa, conforme vão sendo cumpridas as finalidades para as quais foram criados. Tais documentos futuramente serão os mesmos que suprirão as necessidades informacionais de historiadores, de

pesquisadores e da comunidade em geral, visto que são elementos de comprovação de eventos ou fatos ocorridos. Nessa fase, os documentos estarão custodiados nos arquivos permanentes.

Os documentos administrativos podem passar por três ciclos, que são denominados de ciclo vital dos documentos, pois são compreendidos por três idades:

- Primeira idade - denominada de arquivos correntes, encontram-se os documentos que estão em uso funcional, administrativo, jurídico; sua utilização está relacionada à sua criação e à sua tramitação legal. A permanência do documento nesse tipo de arquivo dependerá de sua tipologia/função e de sua vigência. Geralmente a permanência dos documentos nesse arquivo é de um ano e situa-se junto ao seu produtor/administrador, devido ao seu uso.
- Segunda idade - denominada de arquivos intermediários, os documentos já excederam seu prazo jurídico-administrativo, porém podem ser utilizados pelo produtor. Nessa fase, os documentos poderão estar organizados junto com documentos de outros setores em outro local, como um arquivo central, e serão submetidos à avaliação. Para tanto, o arquivista contará com a assessoria de administradores, juristas e historiadores que fixarão critérios para a eliminação dos documentos sem valor ao órgão de origem e sem interesse à pesquisa histórica. Os documentos que forem contemplados, isto é, que não forem eliminados, são os documentos de valor permanente, chamados documentos históricos.
- Terceira idade - denominada de arquivos permanentes, encontram-se os documentos custodiados definitivamente, assim, tem-se início o uso científico, social e cultural dos documentos. Para que cumpram seu papel, os documentos e informações devem estar disponibilizados em locais de fácil acesso para que seus usuários satisfaçam suas necessidades informacionais.

Silva (2002) afirma que os arquivos podem ser tratados no panorama da interdisciplinaridade, no contexto das Ciências Sociais Aplicadas. Ressalta que as

tecnologias presentes a partir da segunda metade do século XIX, e o fortalecimento dessas a partir dos anos 90 do século XX, influem sobre o tratamento das informações contidas nos documentos de forma a permitir seu uso e reuso.

As mudanças relacionadas em nossos dias, como a ampliação do fluxo de informações, de produção e difusão do conhecimento e, com as possibilidades de acesso proporcionadas pelas Tecnologias de Informação e Comunicação (TIC), fizeram com que os Arquivos em todo mundo ampliassem sua forma de atuação. Assim eles passaram a disponibilizar informações e documentos arquivísticos no ambiente Web.

Adequando-se a essa nova realidade, disseminam as informações por eles custodiadas ao tornarem acessível a busca, a consulta, o uso e o reuso da informação, visto que ambientes digitais possibilitam que os visitantes/usuários acessem os documentos e informações arquivísticas para satisfazer suas necessidades informacionais de forma rápida, simples e dinâmica.

Segundo Castells (2006, p. 225), “A era da informação é a nossa era. É um período histórico caracterizado por uma revolução tecnológica centrada nas tecnologias digitais de informação e comunicação [...]” que está alicerçada na estrutura social dos computadores em rede, a Internet, caracterizada como espaços e lugares que ligam e interligam as atividades humana e que, apesar de ser um instrumento relacionado à atividade econômica, o maior fluxo de informação se concentra no uso social e pessoal e não no comercial.

A informação é o insumo para a viabilização de atividades em processos culturais, de ensino e aprendizagem, de aquisição e construção de conhecimento para pesquisa científica e tecnológica e em outros setores ou atividades onde o conhecimento humano se faz necessário (MARCONDES, 2001). O que chancela que a forma de disponibilização da informação que se faz extremamente importante para a construção de novos conhecimentos por parte do usuário, principalmente quando nos valemos de recursos digitais tão presentes em nossas vidas e conscientes de que a Internet, bem como os dispositivos usados para o seu acesso, integra-se de maneira inequívoca na vida diária dos cidadãos.

Nesse contexto, podemos afirmar que a relação mais evidente entre a Ciência da Informação e a disponibilização da Informação nos ambientes da Sociedade em Rede

está na proposta voltada para as tarefas dos usuários, que são desempenhadas por esses quando estão buscando ou fazendo uso de instrumentos de representação da informação em ambientes informacionais (INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS, 1998): encontrar, identificar, selecionar, adquirir/obter informações e navegar em ambientes informacionais (SVENONIUS, 2000).

Borko (1968) nos aponta que a Ciência da Informação é considerada como ciência interdisciplinar que estuda as propriedades e o comportamento da informação, as forças que dirigem seu fluxo, o uso da informação e as técnicas manuais e/ou mecânicas para seu processamento, objetivando a armazenagem, a recuperação e a disseminação da informação.

A Ciência da Informação é a disciplina que investiga as propriedades e comportamento da informação, as forças que governam o fluxo de informação, e os meios de processamento da informação, para otimizar a acessibilidade [o acesso] e a usabilidade. [...] Têm ambos, componentes de ciência pura, visto que investiga seu objeto sem considerar sua aplicação, e componentes de ciência aplicada, visto que desenvolve serviços e produtos (BORKO, 1968, p. 3).

Para Saracevic (1997), a Ciência da Informação é uma ciência interdisciplinar relacionada com a Tecnologia da Informação e Comunicação, tendo grande alcance social e humano. Igualmente, o autor pontua a importância do diálogo com a recuperação da informação multimídia e multilíngue, os arquivos virtuais, as buscas na Internet e os estudos de interação.

Para Wersig e Nevelling (1995 apud SARACEVIC, 1997), é responsabilidade social a transmissão do conhecimento para aqueles que dele necessitam. Desse modo, questões relacionadas à informação e sua transmissão podem ser consideradas como o fundamento da Ciência da Informação.

Santos e Vidotti (2009, p. 6), ao discorrerem sobre as Tecnologias de Informação e Comunicação e a Ciência da Informação, fazem a seguinte alegação:

A ciência da Informação deveria ter ou criar mais espaços de investigação que permitam a compreensão das Tecnologias de Informação e Comunicação (TIC) para a potencialização de

competências informacionais e computacionais mais inclusivas, para a conceituação de usos da informação em ambientes informacionais digitais, para a aprendizagem de metalinguagens e para a representação da informação.

Diante do exposto, as mudanças tecnológicas proporcionadas e facilitadas pelo avanço das Tecnologias de Informação e Comunicação foram absorvidas e incorporadas pela atual estrutura social. Nesse cenário, os arquivos permanentes devem ser reconhecidos como instituições que custodiam, preservam e disseminam informações pertinentes a todo tipo de comunidade. Norteada pelo direito ao acesso às informações e aos documentos hoje garantidos por lei a todos os cidadãos brasileiros, há uma urgência de se considerar o uso das TIC a partir de reflexões sobre o caminho que os ambientes informacionais, como ambientes digitais arquivísticos estão seguindo, bem como observar como está sendo a interação desses ambientes com os usuários especialistas ou não.

A Internet propicia a interação do usuário com os ambientes arquivísticos como resultado das mudanças que ocorreram na forma de difusão e aquisição da informação. Com isso, há uma ampliação no paradigma de custódia e acesso aos conteúdos documentais, ou seja, o acesso à informação por meio de mídias disponíveis e acessíveis. Diante disso, a facilidade e rapidez (no acesso, uso e reuso da informação) constituem-se como primeiros objetivos dos serviços de informação.

Nesse contexto, os arquivos digitais, podem contribuir para o ensino e a pesquisa e atender às necessidades informacionais da sociedade, oferecendo serviços com foco no atendimento dos diferentes grupos de usuários. Assim, os serviços gerados por Repositórios Arquivísticos Digitais dos Arquivos Permanentes, motivados pelas tecnologias, podem ter suas rotinas racionalizadas ao se utilizarem de sistemas de automação que agilizem o processo de recuperação e transmissão da informação, tornando-os acessíveis a todo cidadão.

Para tanto, os arquivistas devem assumir condutas e práticas profissionais que estejam em consonância com a perspectiva teórica da área e com o Conselho Nacional de Arquivos (CONARQ) no que diz respeito à incorporação das tecnologias de comunicação e informação e, desta maneira tornar a informação ágil, precisa e globalizada.

## 1.1 Problema

Os arquivos públicos brasileiros se utilizam dos ambientes digitais para cumprir as exigências da Resolução 39 do CONARQ, que estabelece diretrizes para implementação e implantação de repositórios arquivísticos, para o arquivamento e a manutenção de documentos.

Considerando as condições atuais de desenvolvimento tecnológico e a presença dos arquivos públicos brasileiros nos ambientes digitais de informação, apresentam-se as seguintes questões de investigação:

Tendo como diretrizes as orientações da Resolução 39 e da Norma ISO 16363:2012, quais são as características de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq)?

Qual deve ser o papel do arquivista como membro integrante de uma equipe no trabalho para a construção de RDC-Arq.?

## 1.2 Dos objetivos

Tendo como diretrizes as orientações da Resolução 39 do CONARQ e da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*).

### 1.2.1 Objetivo geral

Analisar o conjunto de atributos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) a partir das diretrizes da Norma ISO 16363:2012 e da Resolução 39 do CONARQ para criação de um conjunto de recomendações para a certificação de Repositórios Arquivísticos Confiáveis.

### 1.2.2 Objetivos específicos

- Descrever o papel do arquivista como usuário-chave, na construção de um Repositório Arquivístico Digital Confiável (RDC-Arq).

- Identificar as diretrizes da Resolução 39, “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq” e da norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*), com foco na certificação de RDC-Arq.
- Categorizar as diretrizes da Resolução 39, “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq” e a norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*), com foco na certificação de RDC-Arq.
- Compatibilizar/Cotejar os requisitos indicados pela Norma ISO e pela Resolução do CONARQ.
- Sistematizar convergências para identificação dos requisitos com ênfase no acesso à informação em Repositórios Arquivísticos Digitais Confiáveis.

### **1.3 Motivação e justificativa da pesquisa**

O tema acesso à Informação é uma preocupação que vem da minha experiência como profissional da informação, trabalhando com arquivos permanentes. Assim, pude perceber o quão importante é que o arquivista se configure como usuário chave (*key user*) no ambiente arquivístico. Como parte de uma equipe multidisciplinar ele é conhecedor das melhores práticas para que o arquivo atenda as necessidades informacionais de seu público alvo, agora também no ambiente digital. Dessa feita, é imprescindível seu diálogo com profissionais da tecnologia para que transmita seu conhecimento ao solicitar produtos e serviços que resultarão em melhores práticas na prestação de serviços do arquivo que facilitem, otimizem e ampliem o acesso aos documentos e às informações arquivísticas, ou seja, a construção de arquivos digitais confiáveis que ofereçam o acesso como pontes entre a informação e o documento arquivístico solicitado.

O tema também foi abordado em minha dissertação em que foi tratada a temática: “Disseminação da Informação nos Websites dos Arquivos Permanentes” que

teve como foco analisar quais os arquivos públicos dos estados brasileiros se encontravam na ambiência digital e como era feita a disponibilização de seus documentos e informações nesse ambiente. Como resultado foi constatado que 59% dos arquivos públicos estaduais brasileiros que se encontravam na *Web*, utilizavam-na como meio divulgador e não como meio disseminador da informação. Dessa maneira, não se proporcionava o acesso às informações e aos documentos (GONÇALEZ, 2013) o que nos encaminhou para esta pesquisa, sobre RDC-Arq e papel do arquivista frente a essa realidade. Destaque-se que o acesso às informações arquivísticas sempre foi nossa preocupação.

A pesquisa tem relevância no âmbito científico e acadêmico contribuindo com subsídios teóricos para a Ciência da Informação e oferecendo orientações de aplicação para as comunidades de prática. No âmbito social, a relevância pode ser percebida na contribuição para estruturação dos repositórios arquivísticos digitais confiáveis.

No cenário arquivístico, estamos vivenciando diferentes formas de acesso às informações. A ausência do tema na literatura brasileira e sua escassez na internacional são motivações para um olhar científico sobre a temática.

Portanto, justifica-se a pesquisa em curso, dada sua relevância científica e acadêmica no desenvolvimento de um estudo sistemático sobre a temática em tela, sua relevância social no encaminhamento de recomendações para o desenvolvimento de RDC-Arq.

Cabe destacar que a investigação está pautada na análise e na categorização de uma normalização de caráter internacional, a ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*), que “define uma prática recomendada para avaliar a confiabilidade de repositórios digitais e é aplicável a toda a gama de repositórios digitais e pode ser utilizada como uma base para a certificação” das diretrizes nacionais propostas pelo CONARQ por meio da Resolução 39, para o desenvolvimento de recomendações para construção de RDC-Arq para o desenvolvimento de melhores práticas e recomendações de trabalho.

A originalidade da pesquisa está em relacionar a Norma ISO 16363:2012 e a Resolução 39 do Conarq para propor recomendações para certificação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq).

## **1.4 Tese**

Os requisitos que compõem a Norma ISO e a Resolução 39 do Conarq são elementos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) no que diz respeito ao uso e ao acesso à informação por conectar serviços e coleções visando às comunidades alvo.

## **1.5 Hipótese**

Comprovar se a análise das normas ISO 16363:2012 e Resolução 39 do CONARQ são fundamentais para a identificação dos requisitos essenciais para a implantação de um Repositório Arquivístico Digital Confiável.

## **1.6 Proposição**

Estudo teórico dos Repositórios Arquivísticos Digitais (RDC-Arq) considerando a resolução 39 do Conarq para a implantação de Repositórios Arquivísticos Digitais Confiáveis e as boas práticas recomendadas pela norma ISO 16363:2012, Repositórios Digitais Confiáveis, tendo como foco o acesso à informação.

## **1.7 Metodologia**

O desenvolvimento da pesquisa consistiu-se em um estudo teórico, exploratório, descritivo e documental, visto que seu desenvolvimento se embasou no material publicado sobre o tema estudado (LAKATOS; MARCONI, 2001). A pesquisa exploratória e descritiva da literatura permitiu a análise do tema e a construção de um conhecimento teórico que muito auxiliou na compreensão do problema proposto e na construção dos resultados esperados.

Segundo Köche (2003, p. 126), os estudos exploratórios desencadeiam “[...] um processo de investigação que identifica a natureza do fenômeno e apontam características essenciais das variáveis que se quer estudar”. O caráter descritivo da

pesquisa permitirá apresentar as características do objeto de estudo em questão, conforme a proposição e os objetivos (COSTA; COSTA, 2001). Já o caráter documental, segundo Gil (2002) apesar da semelhança à pesquisa bibliográfica possui diferença no que diz respeito à natureza das fontes. Ainda segundo o autor, dentre as vantagens da pesquisa de caráter documental esta considera que os documentos constituem fonte rica e estável de dados. Nessa pesquisa, os documentos utilizados foram: a Norma ISO 16363:2012 e a Resolução 39 do CONARQ.

Pela perspectiva da abordagem do problema, a presente pesquisa é quali-quantitativa, visto que os dados foram coletados, tabulados a partir das recomendações nacionais e normas internacionais, e pelo fato de a análise nela proposta estar pautada na análise e interpretação de seus conteúdos. Para a realização de procedimentos metodológicos, as atividades foram planejadas e divididas em etapas conforme se pode ver abaixo.

### **1ª Etapa – Levantamento bibliográfico e seleção do material**

Recorte de informações pertinentes ao tema para a construção do embasamento teórico da pesquisa em andamento.

O levantamento bibliográfico foi efetuado em nível nacional e internacional. As fontes bibliográficas da área de estudo foram divididas em fontes primárias, secundárias e terciárias. A seleção das fontes de informação foi realizada a partir dos critérios:

1. Pertinência do tema investigado;
2. Idioma dos documentos (português, inglês e espanhol);
3. Atualidade dos documentos.

### **2ª Etapa – Leitura e interpretação, análise e sistematização da documentação selecionada**

Construção da base teórica para a discussão dos diferentes pontos de vista identificados na literatura sobre o tema em análise para a criação de subsídios e alcance dos objetivos propostos na pesquisa.

### **3ª Etapa - Análise e estabelecimento de características fundamentais sobre os termos utilizados para expressar os arquivos digitais, os repositórios arquivísticos**

Foi realizada a análise das características encontradas na literatura, para elucidação dos termos utilizados na pesquisa, criando assim a base teórica para a sua redação.

### **4ª Etapa – Sistematização do estudo exploratório**

Foi feita a identificação e análise das relações existentes sobre a disponibilização da informação, acesso ao documento arquivístico em meios digitais, preservação dos documentos arquivísticos em repositórios arquivísticos digitais confiáveis, conforme orientações das normas ISO 16363:2012 e a Resolução 39 do CONARQ e de ações do arquivista que possibilitam/facilitam o acesso a documentos e informações arquivísticas, objetivando a identificação dos requisitos essenciais para a implantação de um Repositório Arquivístico Digital Confiável como ponto original e inovador de uma tese de doutorado.

### **5ª Etapa – Elaboração e redação para o exame de qualificação**

Apresentação à banca examinadora, considerações preliminares sobre o estudo proposto.

### **6ª Etapa – Elaboração e redação final da pesquisa**

Após a orientação e sugestões da banca de qualificação, foi realizado o desenvolvimento das propostas finais de pesquisa com o intuito de divulgar à comunidade científica os resultados obtidos com o desenvolvimento do estudo em questão.

## **1.8 Estrutura do texto**

Esta tese estrutura-se em sete capítulos.

**Capítulo 1** - Introdução. Aborda os pressupostos iniciais como o problema de pesquisa, tese, hipótese, justificativa, objetivos e metodologia. Apresentam-se também os seguintes.

**Capítulo 2** - Patrimônio Cultural, Documento Arquivístico Digital e Curadoria. O capítulo conceitua os termos: Documento; Documentos Arquivísticos; Documentos Digitais; Curadoria e Ciclo de Vida da Curadoria Digital.

**Capítulo 3** - Acesso à Informação e o arquivista. Apresenta, no âmbito nacional e internacional, a Lei de Acesso à Informação, as principais propriedades da LAI no Brasil, os fazeres e saberes do arquivista e ações desse profissional que possibilitam e facilitam o acesso a documentos e informações arquivísticas.

**Capítulo 4** - Confiabilidade em arquivos digitais: um caminho para repositórios arquivísticos digitais. Conceitua os termos utilizados na literatura para a construção de RDC-Arq: Repositórios digitais; Repositórios Digitais Confiáveis e Repositórios Arquivísticos Digitais Confiáveis.

**Capítulo 5** - Apresenta as Diretrizes Nacionais e Internacionais para repositórios Digitais confiáveis, bem como identifica e categoriza o termo acesso no texto da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*) e no texto da Resolução 39 do CONARQ para certificação de RDC-Arq. Analisa os Requisitos indicados nacional e internacionalmente para a construção de repositórios arquivísticos digitais que garantam as características necessárias para o tratamento arquivístico dos documentos e que sejam repositórios confiáveis, como especifica a resolução e como certifica a norma.

**Capítulo 6** - Sugere Recomendações para construção de RDC-Arq, considerando as diretrizes da Norma ISO 16363:2012, a Resolução 39 do CONARQ baseados no acesso à informação e apresenta um *Checklist* para que o Arquivista possa mensurar o nível de confiabilidade de um Repositório e adequá-lo para certificação.

**Capítulo 7** - Considerações finais. São apresentadas as considerações desta pesquisa, pontuando os resultados obtidos e vislumbrando possíveis desdobramentos futuros desse estudo.

**Referências**

## 2 PATRIMÔNIO CULTURAL

Este capítulo tem como proposta apresentar uma abordagem sobre a noção de patrimônio cultural (material e imaterial) no âmbito nacional e internacional e conceituar os termos: documento, documento arquivístico, documento arquivístico digital, Curadoria Digital e Ciclo de Vida do Documento Digital. Essa abordagem subsidiará as discussões dos próximos capítulos que se pautarão na temática dos fazeres e saberes do arquivista na construção, na certificação ou na medição de confiabilidade de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq).

A palavra patrimônio, em sua acepção mais primitiva, é originada do termo grego *pater*, cujo significado é pai ou paterno, relacionando-se historicamente ao sagrado, à herança e aos bens familiares que são deixados pelo pai e assim transmitidos para seus filhos.

Segundo Zanirato e Ribeiro (2006, p. 253), a palavra provém do termo latino *patrimonium* e refere-se à “[...] propriedade herdada do pai ou antepassados, uma herança”, confirmando que patrimônio é aquilo recebido das pessoas que viveram no passado. Num âmbito mais geral, Garbinatto (2000) aponta que patrimônio se constitui como uma construção coletiva, pertencente a todos cidadãos e, assim, todos têm o direito e o dever de preservá-lo, possibilitando, dessa maneira, o resgate de sua identidade social e individual.

Quando pensamos em uma sociedade, uma instituição familiar ou privada, devemos pensar que o patrimônio, tanto material quanto imaterial, faz parte da história e constitui a memória dos agrupamentos sociais. Como patrimônio material, podemos apontar os bens materiais, isto é, os bens tangíveis, os bens imóveis que são constituídos de edifícios, sítios arqueológicos, propriedades, monumentos, enfim, tudo o que é composto de elementos naturais, como os acervos documentais, arquivísticos, museológicos e bibliográficos, videográficos, fotográficos e cinematográficos (INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL, 2014). Já os bens de natureza imaterial são constituídos pelos elementos intangíveis, os que dizem respeito às práticas e domínios da vida social manifestados nos saberes, nos ofícios e nos modos de fazer.

No final do século XVII, com o entendimento moderno de história e de cidades, começa a tomar forma a ideia de que o patrimônio deve ser comum a uma sociedade, pois ele lhe dará identidade e auxiliará na identificação ou na construção da memória e da história do grupo. Porém, somente os bens que estavam relacionados à cultura ou ao passado de uma coletividade foram contemplados, pois se julgava que esses eram merecedores de proteção (SANTOS, 2001).

À medida que a ideia de que o patrimônio cultural era um bem comum foi se fortalecendo, fez-se necessário estabelecer limites físicos e conceituais. Assim sendo, foram criadas leis e regras para que isso acontecesse.

Para Fonseca (1997, p. 54-59):

[...] foi a idéia de nação que veio garantir o estatuto ideológico (do patrimônio), e foi o Estado nacional que veio assegurar, através de práticas específicas a sua preservação. (...) A noção de patrimônio se inseriu num projeto mais amplo de construção de uma identidade nacional, e passou a servir ao processo de consolidação dos estados-nação moderno.

Com o advento da Revolução Francesa (1789-1799), quando é salientada a necessidade de se eleger monumentos, as escolhas materiais não poderiam se contrapor ao esquecimento, ao passado. Desse modo, os monumentos tinham que expressar fatos de natureza singular e grandiosa, devido às noções historiográficas da época. Assim se preservaria o passado e ainda haveria aderência ao pensamento de melhoria, evolução e progresso.

Segundo Gonçalves (2002, p. 121-122),

Os patrimônios culturais são estratégias por meio das quais grupos sociais e indivíduos narram sua memória e sua identidade, buscando para elas um lugar público, de reconhecimento, na medida mesmo em que se transformam em “patrimônio”. Transformar objetos, estruturas arquitetônicas e estruturas urbanísticas em patrimônios culturais significa atribuir-lhes uma função de “representação”, que funda a memória e a identidade (...). Os patrimônios são assim, instrumentos de constituição de subjetividade individual e coletiva, um recurso à disposição de grupos sociais e seus representantes em sua luta de reconhecimento social e político no espaço público.

A ampliação do patrimônio cultural, no Brasil, foi reconhecida pela Constituição Federal no ano de 1988, quando - em seus artigos 215 e 216 - reconhece a existência de bens culturais de natureza material e imaterial.

**Art. 215.** O Estado garantirá a todos o pleno exercício dos direitos culturais e acesso às fontes da cultura nacional e apoiará e incentivará a valorização e a difusão das manifestações culturais.

**Art. 216.** Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial tomados individualmente ou em conjunto, portadores de referência à identidade, à nação, 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.

§ 1º - O poder público, com a colaboração da comunidade, promoverá e protegerá o patrimônio cultural brasileiro, por meio de inventários, registros, vigilância, tombamento e desapropriação, e de outras formas de acautelamento e preservação.

§ 2º - Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

§ 5º - Ficam tombados todos os documentos e os sítios detentores de reminiscências históricas dos antigos quilombos (BRASIL, 1988).

Fontal Merillas (2003) nos aponta que o conceito de patrimônio cultural é sempre atribuído a manifestações e testemunhos significativos da civilização humana. Afirma ainda que esse conceito é múltiplo, visto que as interpretações diferenciam-se em suas concepções em cada unidade de patrimônio e cultura e quando em conjunto de patrimônio cultural.

De acordo com Santos (2006, p. 8), “[...] cultura diz respeito à humanidade e ao mesmo tempo a cada um dos povos, nações, sociedade e grupos humanos”. O autor afirma que, apesar das várias maneiras de entender o que é cultura, elas derivam de duas concepções básicas:

A primeira dessas concepções preocupa-se com todos os aspectos de uma realidade social. Assim a cultura diz respeito a tudo aquilo que caracteriza a existência social de um “povo ou nação” ou então de grupos no interior de uma sociedade (SANTOS, 2006, p. 23).

Quanto à segunda concepção, essa ocorre “[...] quando falamos em cultura e estamos nos referindo mais especificamente ao conhecimento, às ideias e crenças, assim como às maneiras como eles existem na vida social.” (SANTOS, 2006, p. 24).

Nesse contexto, para Coelho (1999, p. 103), a cultura “[...] remete à ideia de uma forma que caracteriza o modo de vida de uma comunidade em seu aspecto global e totalizante”.

Deve-se ressaltar que memória é a alegoria dos tempos passados ou presentes, e que os bens materiais ou imateriais, que formam o patrimônio de uma pessoa, da sociedade ou da instituição. São emblemas repositórios da memória que permitirão o diálogo entre o passado e o presente, assim, possibilitando a transmissão do conhecimento e a formação da identidade dos cidadãos.

Segundo Castillo Ruíz (1996), patrimônio pode compreender elementos materiais e imateriais, naturais e culturais, herdados no passado ou criados no presente, em que um grupo de indivíduos reconhece sinais de sua identidade.

Como percebemos, o conceito de patrimônio segue por diferentes vertentes, pois é polissêmico. Neste estudo, abordaremos o patrimônio cultural enquanto representação da memória individual e coletiva, dando enfoque às criações documentais que são compostas de legislações, tratados, cartas, registros cartoriais, livros de batismo, óbitos, casamentos entre outros, os quais compõem o acervo documental arquivístico público ou privado.

Segundo Bellotto (2000, p. 153), o patrimônio documental que constitui os acervos dos arquivos permanentes faz parte do patrimônio histórico e pontua que esse documento é “[...] como algo inerente à sociedade que produz/usa/consome o documento do arquivo, seja ele normativo, testemunhal ou informativo, não deixa de ser elemento integrante do patrimônio cultural” e complementa que os documentos que constituem o patrimônio documental:

Já cumpriram sua função mediata, ligada à razão pela qual foram gerados; não tramitam mais; passaram pelo arquivo corrente; foram avaliados como de valor permanente, pela densidade de seu valor informativo, tanto para instituição que o produziu, como para a sociedade, em cujo contexto atuou a instituição (BELLOTTO, 2000, p. 154).

Desta maneira, os documentos que estão custodiados nos arquivos permanentes constituem um patrimônio documental institucional, municipal, estadual ou nacional.

## 2.1 Patrimônio documental

O termo “patrimônio documental” é utilizado por instituições culturais ou instituições de memória que se dedicam ao recolhimento, tratamento e preservação de uma determinada documentação. Entende-se por patrimônio documental registros que retratam ou representam os fatos, as atividades e informações onde estão envolvidas entidades públicas ou privadas, pessoas ou famílias.

O patrimônio documental nos remete à memória de um grupo detentor e os documentos tanto têm a função de informativos quanto de instrutivos. Segundo Lage (2002, p. 15),

O conceito de Patrimônio Documental liga-se intrinsecamente ao conceito de documento em seu duplo sentido – de recurso, logo funcional, e de significado, logo cultural – sendo no entanto mais complexo que os conceitos já de si complexos de Documento (unidade de informação), Informação (dados do conhecimento registrado) ou Fonte Histórica (todo o dado precedente do passado, do recente, que tem uma realidade material e objectiva, relacionado com a actividade científica e social e historicamente produzido); testemunho original, não re-elaborado, do conhecimento do passado.

Com esses apontamentos, Lage (2002) nos fornece elementos para a aproximação entre patrimônio documental e arquivos permanentes, visto que pondera a relação do patrimônio documental com os demais patrimônios e com os demais documentos, como também temos a compreensão do documento como recurso ou sua função, isto é, o porquê ele existe, o seu papel no contexto em que se integra e também como significado, como informação documental a partir das interpretações desse documento.

Lage (2002) ainda nos aponta duas maneiras pelas quais o patrimônio documental poderá ser apresentado, destacando-os em “categorias” que são: o conjunto de patrimônio bibliográfico e o conjunto de patrimônio arquivístico. Assim, utilizam o documento quanto à sua natureza que pode ser bibliográfico ou arquivístico.

Nessa linha de pensamento, a autora compreende que esses materiais são parte integrante, ou relacionada a um conjunto maior, denominado por ela de patrimônio documental. O primeiro conjunto a autora entende da seguinte maneira:

Patrimônio Bibliográfico – patrimônio intelectual da humanidade, do saber humano produzido sob qualquer modalidade e gravado/inscrito em qualquer tecnologia e/ou suporte, depositado em bibliotecas e constituído referência básica do ensino/investigação/produção do conhecimento (LAGE, 2002, p. 15).

Como descrito acima, os documentos dessa categoria estão voltados aos produtos bibliográficos, isto é, aos materiais que têm características de um documento que faz parte do acervo de bibliotecas.

Para a segunda categoria, denominada pela autora de patrimônio arquivístico, ela os descreve como:

Patrimônio Arquivístico – fontes documentais e patrimônio intelectual funcional de entidades públicas e privadas, coletivas e individuais, integradas em sistemas semi-fechados de informação social com determinada estrutura (natureza orgânica) e fundos ou núcleos (conjuntos orgânicos de documentos de uma única proveniência); séries (docs. Provenientes correspondentes ao exercício de uma mesma atividade) e distintas unidades arquivísticas (docs. relativos a ação administrativa/judicial), coleções (docs. org. para referência) registro (docs. para controle/descrição de docs. recebidos, produzidos) organizados em diferentes unidades de instalação (LAGE, 2002, p. 15).

Nessa categoria, estão os conjuntos de documentos custodiados que fazem parte do acervo dos arquivos. Na direção dos apontamentos feitos pela autora, o patrimônio documental é o conjunto composto pelos documentos bibliográficos e arquivísticos que estão vinculados em seu sentido social, interagindo com o seu meio.

Podemos então recorrer aos apontamentos de Chagas (2002) o qual observa que cada uma dessas instituições se diferencia por suas importantes especificações e, portanto, essas características de individualidade não devem ser desprezadas; todas têm um ponto de ligação entre o tratamento informacional e a preservação da memória como um campo de pertencimento comum, ao pensarmos que a ideia de cultura,

patrimônio e memória estão presentes e inteiramente relacionadas entre si (CHAGAS, 2002).

Em contraponto, García Belsunce (1986, p. 30), sobre o patrimônio documental, faz a seguinte afirmação:

Pode haver – já quase não existe- alguma hesitação quanto aos vários tipos documentais que o integram: mas é indubitável que, definindo-se o documento como aquilo que tem como finalidade imediata provar, testemunhar ou descrever algo e se reconhecendo que o valor permanente de um documento reside na qualidade informativa, não há qualquer dificuldade em se afirmar que o patrimônio documental é o conjunto de documentos de valor informativo produzido pelas pessoas públicas e privadas, físicas ou morais de uma determinada jurisdição.

Para o autor, os documentos de arquivos estão relacionados ao conceito de patrimônio documental e, apesar de isso parecer muito claro, ele abre uma brecha ao citar a existência de “vários tipos de documentos” que compõem o patrimônio documental.

Segundo Edmondson (2002, p. 9), nas diretrizes para salvaguarda do patrimônio documental, para o Programa Memória do Mundo das Organizações das Nações Unidas para Educação, Ciência e Cultura (UNESCO), “A Memória do mundo é a memória coletiva e documentada dos povos do mundo – seu patrimônio documental”. O autor aponta que a definição de patrimônio documental compreende elementos que são: móveis; consistentes em simbologia/códigos, sons e/ou imagens; conserváveis; reproduzíveis e transladáveis e é fruto de um processo de documentação deliberado (EDMONDSON, 2002, p. 15). Ele também considera que: “um documento consta de dois componentes: o conteúdo informacional e o suporte no qual se consigna”.

Também para o Arquivo Nacional (2005, p. 73), os documentos configuram-se na “[...] unidade de registro de informações, qualquer que seja o suporte ou o formato”. Porém, os documentos devem estar preservados, organizados e acessíveis, para que possam cumprir sua função social, administrativa, técnica, cultural e histórica (TESSITORE, 2003).

Para que as informações contidas nos documentos arquivísticos cumpram seu propósito de ser patrimônio documental da sociedade, essas informações precisam ser

tratadas, preservadas e estarem disponibilizadas e acessíveis a todos os cidadãos independente da forma como será acessado.

O *International Council of Archives* (ICA), em sua declaração sobre os arquivos, faz o seguinte apontamento:

Os arquivos registram decisões, ações e memórias. Arquivos são um patrimônio único e insubstituível transmitido de uma geração a outra. Documentos de arquivos são geridos desde a criação para preservar seu valor e significado. Arquivos são fontes confiáveis de informação para ações administrativas responsáveis e transparentes. Desempenham um papel essencial no desenvolvimento das sociedades ao contribuir para as constituições e salvaguarda da memória individual ou coletiva. O livre acesso aos arquivos enriquece o conhecimento sobre a sociedade humana, promove a democracia, protege os direitos dos cidadãos e aumenta a qualidade de vida (INTERNATIONAL COUNCIL OF ARCHIVES, 2010, p. 1).

Para que os arquivos cumpram as premissas de livre acesso aos documentos e aos conteúdos documentais, muitos arquivos, seguindo a tendência mundial, fazem-se presentes na ambiência digital, pois precisam disponibilizar suas informações arquivísticas a toda uma sociedade que está presente na Web e deseja ter suas necessidades informacionais de forma rápida, fácil e segura, para que possa fazer uso e reuso da informação.

A preservação das informações a longo prazo tornou-se imprescindível, pois o indivíduo é parte de um todo e todos constroem a história da sociedade, deixando como legado às gerações futuras: criações, intervenções no ambiente e registros. Tais informações propiciarão a compreensão da história humana. Caso contrário, a perda, a destruição dessas representações, desse patrimônio herdado das gerações passadas, conduzirá ao rompimento do conhecimento.

Nesse contexto é que a preservação alcança novo foco, frente à consciência do armazenamento, do acesso, da comunicação, da disseminação, do uso e reuso da informação arquivística e, por conseguinte, dos documentos que, no presente e no futuro, sejam capazes de contribuir para a identidade cultural da sociedade que os produziu.

Na contemporaneidade, o advento das Tecnologias de Informação e Comunicação (TIC) e os meios institucionais, dentre eles as Instituições Arquivísticas,

nosso objeto de pesquisa, foram impactados sobremaneira com as formas de materialização da informação, visto que atualmente grande parte de sua gênese se encontra em ambientes informacionais digitais, tornando um desafio a arquivistas a preservação digital de longa duração.

Percebe-se, nos repositórios digitais/arquivos digitais, a possibilidade de ambientes estratégicos para a preservação digital de longa duração, uma vez que é constatado que arquivos digitais crescem de maneira contínua e acelerada. Segundo Lyman (2002), mais de 90% (noventa por cento) dos objetos digitais são produzidos nos ambientes informacionais digitais, ou seja, são natos digitais, o que os torna suscetíveis a alterações, podendo ser corrompidos devido à sua fragilidade ou ainda devido à dependência tecnológica, pois se tornam vulneráveis à rápida obsolescência a que a tecnologia está sujeita.

Os arquivos digitais apresentam um conjunto de propriedades que problematizam as bases dos conceitos da arquivologia como a originalidade, a autenticidade, a identidade, a integridade e o contexto da gênese documental.

Segundo Bellotto (2002, p. 23), dentre as peculiaridades dos documentos arquivísticos na organicidade as:

[...] relações administrativas dos documentos refletem-se no interior dos conjuntos documentais. [...] é a “qualidade segundo a qual os arquivos refletem a estrutura, funções e atividades da entidade produtora/acumuladora nas relações internas e externas”.

O Conselho Nacional de Arquivos (2012, p. 2) nos dá a seguinte definição quanto aos conceitos de autenticidade e identidade e integridade:

Autenticidade: qualidade de um documento ser exatamente o que foi produzido, não tendo sofrido alterações, corrompimento e adulteração. A identidade é composta de identidade e integridade. Identidade é o conjunto dos atributos de um documento arquivístico que o caracteriza como único e o diferenciam de outros documentos arquivísticos (ex.: data, autor, destinatário, assunto, número identificador, número de protocolo). Integridade é a capacidade de um documento arquivístico transmitir exatamente a mensagem que o levou à sua produção (sem sofrer alterações de forma ou de conteúdo) de maneira a atingir seus objetivos.

Identidade e integridade são constatadas à luz do contexto jurídico administrativo, de proveniência, de procedimentos, documental e

tecnológico no qual o documento arquivístico foi produzido e usado ao longo tempo.

Cruz (2013, p. 14) ao discorrer sobre a característica originalidade dos documentos, observa que “[...] o documento de arquivo é único, não havendo exemplares que possam substituí-los em caso de extravio ou destruição”.

Diante do exposto, faz-se necessária a preservação da autenticidade, da originalidade e da integridade dos arquivos digitais em repositórios digitais, que hoje é possibilitada pela Curadoria Digital, sobre a qual discorreremos como tema no subitem 2.5.

## 2.2 Documento

Desde a antiguidade, os homens procuram uma forma de registrar seu pensamento. Assim, valeram-se de traços, desenhos, alfabetos e números, em diferentes formatos como livros, fotografias, esculturas, nos mais diferentes tipos de suporte: pedra, barro, tecido, couro, papel, plástico entre outros. Dessa forma, comunicavam sua vivência, gosto, fatos, descobertas para seus pares e para as gerações vindouras.

Todos esses registros, ainda que em diferentes suportes, podem ser compreendidos como documentos e informações.

Segundo Lopez Yepes (1977, p. 91 apud SAGREDO FERNÁNDEZ; IZQUIERDO ARROYO, 1982, p. 171), a palavra documento vem do latim *documentum* que tem “[...] a mesma raiz de docere, ensinar, o que outorga ao documento o significado de ensino”.

No âmbito da Ciência da Informação, Paul Otlet apresentou seu conceito de documento juntamente com Henri La Fontaine ao criarem o Instituto Internacional de Bibliografia (IIB) em 1908.

[...] tudo aquilo que representa ou expressa, por meio de sinais gráficos (escrita, pintura, diagramas, mapas, imagens, símbolos) um objeto, um feito, uma ideia, ou uma impressão. Textos impressos (livros, revistas, jornais) hoje constituem a mais numerosa categoria deles (ADI apud SHERA; CLEVELAND 1977, p. 251).

Segundo o Dicionário Houaiss da Língua Portuguesa, documento é:

[...] qualquer escrito usado para esclarecer determinada coisa; qualquer objeto de valor documental (fotografias, peças, papéis, filmes, construções etc.) que elucide, instrua, prove ou comprove cientificamente algum fato, acontecimento, dito etc. (HOUAISS, 2001, p. 1069).

Schellenberg (2004, p. 14), no campo da Arquivologia define que os documentos “*records*” são:

Todos os livros, papéis, mapas, fotografias ou outras espécies documentárias, independentemente de sua apresentação física ou características, expedidos ou recebidos por qualquer entidade pública ou privada no exercício de seus encargos legais ou em funções de suas atividades e preservados ou depositados para preservação por aquela entidade ou por seus legítimos sucessores como prova de suas funções, sua política, decisões, métodos, operações ou outras atividades, ou em virtude do valor informativo dos dados neles contidos.

Em dias atuais, frente à tecnologia digital, o documento, como objeto físico, foi substituído por dígitos binários, fixados em bases óticas e magnéticas e não mais visíveis ao olho humano: precisam não mais de suportes físicos, mas passam a estar vinculados a *hardware* e *software*.

Assim, a tecnologia digital passou a ocupar, hoje, um espaço importante na produção documental na sociedade, promovendo o crescimento de diferentes tipos de mecanismos e registros para produzir, armazenar, acumular e disseminar informações.

Segundo Sayão (2007, p. 183):

A urgência da sociedade contemporânea em transformar tudo, textos, imagens, vídeos, músicas, tudo para formatos digitais é justificada pela enorme economia de espaço físico de armazenamento, sobretudo pelos extraordinários ganhos de produtividade e eficiência proporcionados pela otimização dos fluxos de trabalho e a facilidade de manipulação. Isto sem falar das facilidades de acesso aos estoques informacionais, públicos e privados que, por si só, são um fenômeno novo e sem precedentes, como também é a outra face: a facilidade de produção, edição, publicação, integração e distribuição de informação em formatos digitais pelos meandros das redes de computadores mundiais.

Como formato digital compreendem-se as “[...] codificações com dígitos binários serializados conforme um modelo de informação” (INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS, 2007). A composição dos dígitos binários é formada por zero (0) e um (1) e constituem um conjunto chamado *bits* que codificam a informação digital materialmente registrada no suporte.

Sayão (2007, p. 186) expõe que:

A natureza digital de uma informação é dada pela forma como ela é armazenada: sequências de zero (0)s e um (1)s, isto é, cadeias de bits (*bitstream*). A forma mais básica de preservar a integridade de um objeto informacional é preservar a configuração de bits que o definem como um objeto único.

Para Ferreira (2006, p. 21), os dígitos binários que compõem o chamado “objeto digital” podem ser definidos como:

[...] todo e qualquer objeto de informação que possa ser representado através de uma sequência de dígitos binários... documentos de texto, fotografias digitais, diagramas vetoriais, bases de dados, sequências de vídeo e áudio, modelos de realidade virtual, páginas *Web* e aplicações de software são apenas alguns exemplos do que podemos considerar um objeto digital.

O Conselho Nacional de Arquivos (2014a, p. 13) pontua que o documento digital é “[...] a informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional”.

Podemos concluir que os documentos digitais são combinações binárias que somente serão legíveis para os humanos quando intermediados por uma máquina e um *software*. Quando essas ferramentas de acesso se tornam obsoletas, perde-se o documento, pois seu acesso é impossibilitado.

Segundo Sayão (2007, p. 187) está claro que:

[...] o objetivo da preservação digital não é preservar os objetos digitais tão somente como artefatos físicos, independentemente da sua usabilidade, posto que para tal bastaria a guarda em ambiente controlado das mídias que dão suportes a esses objetos. A preservação no universo digital tem pouca relação com a longevidade dos discos óticos, fitas magnéticas e outros meios de armazenagem (bem

guardado, o meu CD de música pode durar 100 anos, mas daqui a 25 anos haverá aparato para tocá-lo?). Hoje não há dúvida de que o santo graal da preservação digital é a preservação do acesso contínuo ao conteúdo intelectual dos documentos digitais... e que visibilidade depende fortemente da expectativa de vida dos sistemas de acesso.

No ano de 2013, Siebra et al. nos apontam que a fragilidade digital, frente à evolução tecnológica nos impoe o desafio de preservá-la e torná-la acessível para as futuras gerações. O que se vislumbra resolver com o surgimento da Curadoria Digital, a qual é vista como um processo mais completo que trata do planejamento, da avaliação e da reavaliação das ações em prol da curadoria do objeto digital que engloba a preservação digital como parte do seu ciclo (SIEBRA et al., 2013).

### **2.3 Documento arquivístico**

Ao ser procurada a expressão “documento de arquivo” no Dicionário de Terminologia Arquivística, a busca é remetida ao termo “arquivo”. Já o *Diccionario de Terminologia Archivística* (apud CRUZ MUNDET, 1994, p. 99, tradução nossa), o documento arquivístico é “[...] a combinação de um suporte e a informação registrada nele, que pode ser utilizada como prova ou para consulta”.

Na literatura arquivística, as definições de documentos seguem uma mesma linha ao afirmarem que tais documentos são gerados de maneira seriada e orgânica.

Para Gutiérrez Muñoz (1982, p. 20, tradução nossa), os documentos de arquivo são “[...] aqueles que foram produzidos ou reunidos por indivíduos ou por instituições em razão das suas funções e atividades que eles registram para atingir determinados objetivos”.

Para Heredia Herrera (1993), os documentos de arquivo são aqueles produzidos ou recebidos por uma instituição enquanto realizam suas atividades e são conservados para que possam provar algum fato ou evento ocorrido ou como fonte de informações.

O documento de arquivo possui características peculiares que o distinguem de qualquer outro, contém uma informação seja qual for a data, forma ou suporte material, produzidos e recebidos por qualquer serviço ou organismo público ou privado, no exercício de sua atividade (ROUSSEAU; COUTURE, 1994, p. 137).

Segundo o Dicionário de Terminologia Arquivística (ALVES et al.,1993, p. 38), documento de arquivo é “[...] um documento a fim de provar e/ou informar um procedimento administrativo ou judicial”.

O Arquivo Nacional (2005, p. 73) pontua que os documentos configuram-se como uma “[...] unidade de informação, qualquer que seja o suporte ou o formato”.

Para o Instituto Português de Qualidade (2005, p. 9), o documento de arquivo “[...] é produzido, recebido e mantido a título probatório e informativo por uma organização ou pessoa, no cumprimento de suas obrigações legais ou na condução de suas atividades”.

Bellotto (2014, p. 329) ao apontar as duas características do documento de arquivo afirma:

A de ser prova e a de ser informação/testemunho, acabam por ser paralelas e inseparáveis. Ele nasce como prova, permanece como informação/testemunho. Ele tanto é registro de uma determinada ação, como registra ações que provocam outras ações. A gênese do documento de arquivo implica na relação entre a natureza da sua finalidade e a fórmula diplomática capaz de conferir autenticidade a ele e confiabilidade ao seu conteúdo.

A autora ainda faz a seguinte referência: “Na feliz expressão de Luciana Duranti, é o vínculo arquivístico o que transforma o documento em um verdadeiro documento de arquivo.” (BELLOTTO, 2014, p. 332).

Tessitore (2003, p. 11), ao discorrer sobre os documentos, faz o seguinte alerta: “[...] para que os documentos cumpram sua função social, administrativa, jurídica, técnica, científica, cultural, artística e/ou histórica é necessário que estejam preservados, organizados e acessíveis”.

Schellenberg (2004, p. 41), ao discorrer sobre os arquivos modernos, assim define documento:

Todos os livros, papéis, mapas, fotografias ou outras espécies documentárias, independente de sua apresentação física ou características, expedido ou recebido por qualquer entidade pública ou privada no exercício de seus encargos legais ou em função das suas atividades e preservados e depositados para preservação por aquela entidade ou por seus legítimos sucessores como prova de suas funções,

sua política, decisões, métodos, operações ou outras atividades, ou em virtude do valor informativo dos dados neles contidos.

Ainda segundo Schellenberg, sua definição foi “ligeiramente modificada”, da definição que consta na Lei de Destinação de Documentos (*Record Disposal Act*) de 7 de julho de 1943 (44 U.S. Code §366-80), quando se definiu documentos (*records*) como “[...] todo material que contenha prova de organização, funções, diretrizes, decisões, normas, operações ou outras atividades do governo”. Referindo-se a todo documento que possibilita provar a existência de tal órgão e/ou às atividades por ele desenvolvidas.

Duranti (1994, p. 50-51), privilegiando o caráter contextual do documento arquivístico, aponta as características desse tipo de material. São elas:

1 – a imparcialidade: os documentos são inerentemente verdadeiros. A autora utiliza, nesse momento, a concepção do arquivista inglês Hilary Jenkinson para reforçar seus argumentos. As razões de sua produção (para desenvolver atividades) e as circunstâncias de sua criação (rotinas processuais) asseguram o caráter de prova e de fidedignidade aos fatos e ações;

2 – a autenticidade: “os documentos são autênticos porque são criados tendo-se em mente a necessidade de agir através deles, são mantidos como garantias para futuras ações ou para informação. (...) Assim, os documentos são autênticos porque são criados, mantidos e conservados sob custódia de acordo com procedimentos regulares que podem ser comprovados”. Duranti ressalta que mesmo aqueles documentos produzidos à margem desses procedimentos estabelecidos e regulamentados podem ser considerados autênticos, tendo apenas o caráter fidedigno de prova documental comprometido;

3 – a naturalidade: os documentos de arquivo não são coletados artificialmente, mas surgem de acordo com o curso dos atos e ações de uma administração. “O fato de os documentos não serem concebidos fora dos requisitos da atividade prática, isto é, de se acumularem de maneira contínua e progressiva, como sedimentos de estratificações geológicas, dota-os de um elemento de coesão espontânea, ainda que estruturada”;

4 – o inter-relacionamento: “cada documento está intimamente relacionado ‘com outros tanto dentro quanto fora do grupo no qual está preservado e (...) seu significado depende dessas relações”. As relações entre os documentos, e entre eles e as transações das quais são resultantes, estabelecem o axioma de que um único documento não pode se constituir em testemunho suficiente do curso de fatos e atos passados: os documentos são interdependentes no que toca a seu significado e sua capacidade comprobatória.

5 – a unicidade: provém do fato de que cada registro documental assume um lugar único na estrutura documental do grupo ao qual pertence e no universo documental

Murguia (2011, p. 50) pontua sobre a valoração dos documentos ao afirmar que:

A Arquivologia aderiu à visão positivista, jogando no documento de arquivo três tipos de valores: administrativo, histórico e de informação, os quais sempre embasados nessa veracidade entendida no simples ser do documento. Isso ocorreu sem se perceber que paradoxalmente, é o respaldo, é o respeito institucional do arquivo e simplesmente ele, não o documento, que faz “dizer a verdade”.

E ainda complementa:

Essa percepção última procede das novas interpretações do documento. Essas percepções, em primeiro lugar, destacam a materialidade da informação, isso é, sua fixação, permanência e inscrição num suporte ou formato físico. O que faz o documento manipulável, organizável e estável. Em segundo lugar, essa materialidade permite sua inserção, uso e circulação social, isso é, possibilita que se tornem campo de ação e de expressão dos diferentes interesses, tensões e enfrentamentos dos grupos que se interpenetram dentro ou tangencialmente no documento (MURGUIA, 2011, p. 10-11).

Segundo o autor citado acima, são claros os princípios arquivísticos da proveniência e do respeito aos fundos, visto que, desde a produção do documento, seu uso e sua guarda lhe atribuem o valor e a veracidade, Pois, desde sua criação, são geridos para que seu valor e seu significado sejam preservados, visto que desempenham segundo o ICA (2010, p. 1):

[...] um papel essencial no desenvolvimento das sociedades ao contribuir para a constituição e salvaguarda da memória individual e coletiva. O livre acesso aos arquivos enriquece o conhecimento sobre a sociedade humana, promove a democracia, protege o direito dos cidadãos e aumenta a qualidade de vida.

Nesse contexto, podemos relativizar que, devido as suas peculiaridades os documentos de arquivos representam o direito da defesa de pessoas ou instituições, visto que, pelo simples fato de existirem, comprovam informações nele descritas, assim, verifica-se o valor de informação do documento.

A Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (CONARQ) (2006) definiu que o documento arquivístico é o “documento produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer de suas atividades, qualquer que seja o suporte”.

Diante do exposto, ao sistematizar os conceitos dos diferentes autores, verificamos que o documento arquivístico é o documento produzido por pessoa física ou jurídica ao cumprir suas atividades, podendo estar em qualquer suporte, mas que contenha uma forma física e que seu conteúdo seja estável. Assim, esse documento se diferencia dos demais tipos de documentos por sua autenticidade, naturalidade, unicidade e organicidade.

Duranti e Preston (2008 apud RONDINELLI, 2011) apontam que o documento arquivístico se constitui de informação e suporte, e que esses dois elementos são indissociáveis o que torna a sua forma fixa e seu conteúdo estável.

## **2.4 Documento Digital**

Com os avanços tecnológicos ampliados potencialmente pelas TIC, as inovações tecnológicas também reverberaram na arquivística. Nesse cenário, documentos que antes eram produzidos no meio analógico passam a ser produzidos no meio digital de maneira simples, rápida e com grande aceitação da sociedade, devido à praticidade para sua criação, para seu acesso e para a sua disseminação.

Ao ponderar sobre essa mudança, Sayão (2010, p. 70) comenta:

Os pesquisadores, professores, estudantes e outros leitores demandam formatos eletrônicos porque eles oferecem um mundo de vantagens em relação às formas impressas, especialmente no que diz respeito à busca, à recuperação, à navegação, à apresentação das informações e à capacidade de interoperarem com outras publicações eletrônicas que estão em rede.

Ferreira (2006, p. 17), ao falar sobre a simplicidade para criação e disseminação dos documentos nas redes, tece o seguinte comentário:

Nos dias de hoje, uma parte significativa da produção intelectual é realizada com o auxílio de ferramentas digitais. A simplicidade com que

o material digital pode ser criado e disseminado através das modernas redes de comunicação e a qualidade dos resultados obtidos são factores determinantes na adopção deste tipo de ferramentas.

Nesse contexto, os documentos digitais pelo seu valor histórico, social e informativo tornaram-se relevantes nos arquivos e são parte integrante do patrimônio documental da sociedade.

Tendo como base os conceitos já citados anteriormente neste trabalho de que o documento arquivístico é aquele que registra ações humanas independente da forma em que é apresentado ou da base em que está fixado, podemos inferir que os documentos gerados na forma digital durante as atividades desempenhadas por pessoas físicas ou jurídicas, em suportes como os magnéticos e óticos, também se constituem como documentos arquivísticos.

Preferencialmente, o termo documento eletrônico é o utilizado na literatura arquivística internacional, no entanto verifica-se que os conceitos a cerca de documento eletrônico, documento digital e objeto digital são distintos. Assim, tal conceitualização se apresenta dúbia, podendo suscitar imprecisão no entendimento dos conceitos da Arquivologia. Tecnicamente há diferença entre os termos, por esse motivo adotamos, neste trabalho, o termo Documento Digital.

Segundo o Glossário da Câmara Técnica de Documentos Eletrônicos (2014, p. 19), o documento eletrônico é “Informação registrada, codificada e, forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico” e o documento digital é a “[...] informação registrada, codificado em dígitos binários, acessível e interpretável por meio de um sistema computacional”, o que nos leva a afirmar que todo documento digital é eletrônico, mas nem todo documento eletrônico é digital. Para ilustração, podemos apontar uma fita VHS, em que a imagem e o som necessitam de um equipamento eletrônico para serem decodificados, porém não se apresentam codificados em bits.

Segundo Rondinelli (2013, p. 231):

[...] o ambiente digital vai além da peculiaridade do suporte. [...] o documento foge totalmente aos padrões mais conhecidos como a linguagem alfabética, registrada em papel e de leitura direta, bem como sua relação inextrincável com o suporte. No mundo digital, tudo é

codificado em linguagem binária que para se tornar acessível aos olhos humanos, precisa de intermediação de programas computacionais igualmente codificados em bits, numa sofisticação que passa despercebida à maioria dos usuários.

Rondinelli ainda nos apresenta o conceito de documento arquivístico digital a partir dos conceitos de documento, documento arquivístico e documento arquivístico digital da seguinte maneira:

Uma unidade indivisível da informação construída por uma mensagem fixada num suporte (registrada), com uma sintática estável [...] produzido e/ou recebido por uma pessoa física ou jurídica, no decorrer de suas atividades [...], codificado em dígitos binários e estável por um sistema computacional, em suporte magnético, ótico ou outro (RONDINELLI, 2013, p. 235).

Ao reconhecer que o documento digital, em nossos dias, é parte integrante do ambiente arquivístico, faz-se necessário verificar suas especificidades e complexidades. Devido ao seu contexto tecnológico, essa perspectiva requer que a Arquivologia se atualize e crie teorias contemporâneas que satisfaçam a abordagem dos documentos arquivísticos digitais (SANTOS; FLORES, 2015).

Os repositórios digitais serão tratados no capítulo 4.

## **2.5 Curadoria Digital**

A sociedade dispendeu grandes esforços para a disseminação e o tratamento da informação, criando formas e tecnologias, a fim de que essa fosse representada, reproduzida e preservada.

Com o advento das tecnologias e da globalização, evidenciaram-se as facilidades que o uso das tecnologias de Informação e comunicação representa para o acesso, a busca e a atualização das informações disponibilizadas na *Web*. Assim, as formas de representação da informação foram alteradas de maneira a ampliar o universo de usuários o que envolve todo o processo de tratamento da informação.

É inacreditável a quantidade de dados gerados e utilizados nas pesquisas, na administração pública e privada, na saúde e nos demais setores sociais que utilizam

dados informacionais que serão transformados em informações produzindo o conhecimento e conseqüentemente o esclarecimento e empoderamento do cidadão.

A preocupação com a divulgação da ciência é percebida desde o século XVI, quando cientistas se utilizavam das cartas para a comunicação de seus resultados de pesquisa que, por sua vez, deram origem aos periódicos científicos (MUELLER, CARIBÉ, 2010).

Segundo Marcondes et al. (2008, p. 22),

[...] o conhecimento científico, tão importante para nossa sociedade, vinha sendo guardado, preservado e disponibilizado desde a antiguidade nas coleções armazenadas em bibliotecas. O estatuto da guarda, preservação e disponibilização da cultura, dos conhecimentos em geral, e em especial do conhecimento científico, tão caro para as bibliotecas enquanto instituições vêm passando por um desafio com o surgimento da web.

No ambiente *Web*, a capacidade de registrar informações aumentou vertiginosamente. Em contraponto, vivenciamos a diminuição da longevidade dos meios usados para que a informação seja armazenada. É nesse contexto que surge a preocupação e o desafio para com a preservação digital devido à acelerada obsolescência tecnológica, digital, à fragilidade do objeto e à manutenção dos dados.

A necessidade de novas práticas relacionadas com o gerenciamento, tratamento e representação da informação digital faz a Curadoria Digital despontar uma nova área interdisciplinar que gerencie informações e dados durante todo seu ciclo de vida com a proposta e o desafio de preservar e transmiti-los num processo completo que planeja, avalia e reavalia as ações, visando à curadoria do objeto digital cuja a preservação digital se configura como parte desse processo.

Etimologicamente, a palavra curadoria tem origem do latim *curator*. Seu significado nos remete à ideia de “aquele que administra”, “aquele que tem cuidado e apreço”.

Quando vista nos dicionários, a definição para curadoria é: “ato ou efeito de curar, função, atributo, cargo, poder de curador, curatela” (HOUAISS, 2007, p. 892).

Já o conceito curadoria abrange um extenso campo de atividades, desde o artístico cultural até as perspectivas comerciais e acadêmicas.

Inicialmente o conceito era conhecido e relacionava-se ao curador das artes, que era a pessoa que fazia o processo de organização, cuidado e montagem de uma exposição artística que poderia ser formada por um conjunto de obras de um ou vários artistas. O curador era quem fazia a escolha e a seleção prévia do que deveria ser exposto.

No âmbito judicial, a curadoria significa que uma pessoa é responsável por organizar e administrar os bens de um menor emancipado ou de alguém que esteja ausente de suas obrigações. O ato de “curar” está relacionado com o zelo, com o cuidado e com a atenção com algo.

O termo Curadoria Digital surgiu quando o *Digital Preservation Coalition* e *British National Space Centre* organizaram o seminário denominado “*Digital Curation: Digital Archives, Libraries and e-Science*” em 19 de outubro de 2001. No ano de 2002, o *Joint Information Systems Committee* (JISC) fez a publicação do “*Inviation to tender: requirement and feasibility study on preservation of e-prints*” que resultou na criação do *Digital Curation Centre* (DCC), em 1 de março de 2004, um centro nacional para resolver os desafios da Curadoria Digital que se deu após uma resposta bem sucedida a JISC por um consórcio formado pelas universidades de Edimburgo e Glaslow que sediaram a *e-Science Centre National*, UKOLN da Univesidade de Bath, e STFC.

Segundo Beagrie (2004, p. 7), o uso do termo Curadoria Digital.

[...] está sendo usado cada vez mais para as ações necessárias para manter dados de pesquisa em meio digital e outros materiais ao longo de seus ciclos de vida e do tempo para as gerações atuais e futuras de usuários. Implícitas nesta definição estão os processos de arquivamento digital e preservação digital, mas também inclui os processos necessários para a criação de dados de qualidade e gestão, e a capacidade de acrescentar valor aos dados para a produção de novas fontes de informação e conhecimento.

Em dias atuais, com o crescimento do mundo digital do qual fazemos parte, mudamos a nossa maneira de agir e reagir em todas as áreas do conhecimento, de busca e de acesso às informações. Nesse contexto, a Curadoria Digital, definida por Tibbo, Hank e Lee (2008, p. 235) como “[...] a gestão ativa e preservação de recursos através de seu ciclo de vida completo”, muito nos auxilia, pois, além de assegurar a preservação dos dados e informações a longo prazo, é um processo que envolve a

gestão dos dados da pesquisa desde sua descoberta, planejamento e interpretação, objetivando seu uso e reuso.

Ainda que o conceito Curadoria Digital seja novo, portanto em evolução, podemos vislumbrar uma saída para algumas de nossas inquietações sobre o futuro do gerenciamento dessa massa de dados produzida, visando sua preservação, seu uso e seu compartilhamento. Frente a essas novas perspectivas, Sayão e Sales (2012, p. 184) fazem o seguinte apontamento.

[...] os conhecimentos e as práticas acumuladas na última década em preservação e acesso a recursos digitais resultaram num conjunto de estratégias e abordagens tecnológicas e atividades que agora são coletivamente conhecidas como “Curadoria Digital”. Ainda que seja um conceito em evolução, já está estabelecido que a Curadoria Digital envolve a gestão atuante e a preservação de recursos digitais durante todo o ciclo de vida de interesse do mundo acadêmico e científico, tendo como perspectiva o desafio temporal de atender a geração atuais e futuras de usuários.

É nesse crescente universo de dados que a Curadoria Digital atua sobre fatores de risco como: tecnologia obsoleta; fragilidade tecnológica; falta de entendimento sobre o que é uma boa prática digital; recursos inadequados e incertezas sobre a Curadoria Digital que comprometem todo o processo de gestão de dados.

A Curadoria Digital também se faz necessária por outras razões. Segundo Rosenzweig (2003, p. 64, tradução nossa),

A Curadoria Digital é importante devido às outras formas de trabalho que a tecnologia tem proporcionado, inclusive possibilitando que pesquisadores de diferentes partes do mundo se conectem a partir de uma rede de computadores para gerar e compartilhar dados.

A apresentação, o acesso e uso das informações foram modificados frente às novas formas de trabalho. Um pesquisador tem a possibilidade de trabalhar com um texto multidimensional, e o que a *Association of Research Libraries* (ARL), previu no ano de 2006, já é uma realidade em nossos dias.

Não apenas haverá um texto, um hiperlink de literatura relacionada e citações do artigo, haverá links para os dados relatados no interior do artigo, através de gráficos, tabelas e ilustrações que serão conectadas

com um conjunto de dados relacionados (ASSOCIATION OF RESEARCH LIBRARIES, 2006, p. 141, tradução nossa).

Segundo Santos (2014, p. 40), a Curadoria Digital é responsável pela:

[...] seleção, preservação, manutenção, coleção e arquivamento de conjuntos digitais. Curadoria Digital também é o processo de estabelecimento e desenvolvimento de repositórios de conjuntos digitais para referência corrente e futura para pesquisadores, cientistas e estudiosos em geral.

Ross Harvey (2010) nos aponta que a Curadoria Digital é todo um processo e que o arquivamento digital e a preservação digital são apenas partes desse processo para a garantia de que os dados digitais criados hoje sobrevivam até amanhã. Desse modo, dele faz parte o desenvolvimento de um conjunto de técnicas que abordem a Curadoria Digital, sendo definida por ele como:

[...] gestão ativa de dados durante o tempo em que ele continua a ser: acadêmico, científico, pesquisável, administrável e/ou de interesse pessoal, com objetivos de apoiar sua reprodutibilidade, reutilização e agregando valor a esses dados. Gerenciando-os do momento de sua criação, até que eles sejam determinados como não úteis e garantindo a sua acessibilidade em longo prazo, assim como a sua preservação, autenticidade e integridade.

Para Sayão e Sales (2012, p. 180), o conceito de Curadoria Digital surge para que possa ser feita a gestão ativa dos dados de pesquisa e seu principal desafio:

[...] recai na necessidade de se preservar não somente o conjunto de dados, mas de preservar, sobretudo, a capacidade que ele possui de transmitir conhecimento para uso futuro das comunidades interessadas. Isto significa que os ativos genuínos da pesquisa científica devem permitir que futuros usuários reanalisem os dados dentro de novos contextos.

A *Digital Curation Curriculum* (DigCCurr) tem uma descrição que é definida como:

Nossa cultura herdada, o conhecimento científico moderno, todo comércio e governo dependem da preservação de dados autênticos e confiáveis de registros e objetos digitais. Enquanto dados digitais asseguram o acesso, a inerente fragilidade de mídia e arquivos, a rápida

obsolescência de software e hardware, a necessidade de sistemas de arquivos e metadados bem construídos, conferem a esses materiais risco e dão uma pequena esperança de longevidade da informação que não é intencionalmente preservada. Uma década de trabalho em preservação digital e acesso resultou em uma emergente e complexa compilação de estratégias de ciclo de vida de dados, além de abordagens tecnológicas e atividades que hoje são chamadas de “Curadoria Digital” (DIGITAL CURATION CURRICULUM, 2006).

Diante do exposto acima, é necessário destacar que a Curadoria Digital reflete uma abordagem holística para o processo de gerenciamento do objeto digital, incluindo atividades que abarcam todo ciclo de vida desses objetos para que esses possam ser recuperados, acessados e satisfaçam as necessidades informacionais do usuário que deles necessite.

Podemos afirmar que a Curadoria Digital é o processo feito no desenvolvimento de repositórios digitais, onde documentos digitais são armazenados para que as informações ali disponibilizadas possam ser acessadas, utilizadas e reutilizadas por qualquer pessoa (especialista ou não) no presente ou no futuro. Assim, estabelece, mantém e acrescenta valores aos repositórios de documentos digitais.

Nesse cenário, a Curadoria Digital deve ser realizada por qualquer profissional que tenha a informação como insumo de trabalho, sejam eles bibliotecários, arquivistas, museólogos, historiadores, entre outros.

Neste estudo, vamos nos concentrar na Arquivologia, em que o arquivista, ao criar um Repositório Digital Confiável, terá responsabilidade com a preservação digital e com as transformações associadas como a migração por exemplo, visto que atuam como administradores de longo prazo dos dados e devem assegurar a disponibilidade de uso e reuso dos dados e nesse ambiente encontra uma maneira eficiente de fazê-lo, isto é, gerenciar, preservar dar acesso à memória social digitalmente.

Brophy e Frey (2006, apud HARVEY, 2010, p. 6) descrevem algumas atividades que são realizadas pela Curadoria Digital:

- Manter as conexões entre informação digital e anotações associadas ou materiais publicados, incluindo citações.
- Garantir acesso a longo prazo e reusabilidade da informação digital;
- Realizar, atividades arquivísticas na informação digital como seleção etc.

- Garantir a autenticidade, integridade e proveniência da informação digital e a manutenção dessas características ao longo do tempo;
- Realizar atividades de preservação;
- Manter os componentes de *hardware* hábeis para ter a informação ao longo do tempo;
- Gerenciar riscos da informação digital.

Devemos ressaltar que a curadoria não é arquivamento digital, processamento de *backup* e manutenção como estratégias de preservação ao longo prazo (DIGITAL PRESERVATION COALITION, 2008). E não é preservação digital todo tipo de ação que requer a manutenção para o acesso de materiais digitais além do limite das falhas de mídia e mudanças tecnológicas (DIGITAL PRESERVATION COALITION, 2008, p. 24) ou as “[...] políticas, estratégias e ações que asseguram o acesso ao conteúdo digital ao longo do tempo”.

Ainda que arquivamento e preservação digital sejam importantes, não podemos considerá-los Curadoria Digital. A Curadoria Digital é um conceito mais inclusivo que os outros, já que agrega uma grande gama de processos aplicados a objetos digitais através do ciclo de vida da informação digital.

Nos arquivos, geralmente a atenção profissional está voltada para as coleções digitais com a digitalização e acesso aos conteúdos digitais, mas isso é insuficiente para o processo de Curadoria Digital, pois ela se preocupa com ciclo de vida completo e a usabilidade futura, assegurando seu acesso a longo prazo, sua preservação, sua autenticidade e integridade.

Seamus Ross (2007, p. 2, tradução nossa), pesquisador renomado e experiente em diferentes áreas da Curadoria Digital descreve as razões pelas quais os objetos digitais e dados se tornam inutilizáveis:

Eles são fronteirços em diferentes níveis na aplicação de diferentes hardwares que foram usados na criação ou gestão. Eles são propensos a serem corrompidos. Eles são facilmente mal identificados. Eles são geralmente pobremente descritos.

Vista como necessária e como uma questão de urgência, a Curadoria Digital é entendida por qualquer indivíduo que se utilize de computadores. No ano de 2003, a

UNESCO fez o lançamento da *Guidelines for the Preservation of Digital Heritage* e aponta as seguintes ameaças para continuidade digital:

- Os suportes usados para armazenar os materiais digitais são geralmente instáveis e deterioram-se com poucos anos, ou no máximo, décadas.
- Uso de materiais digitais depende de meios de acesso que funcionam de maneiras distintas, geralmente com combinações complexas de ferramentas incluindo *hardware* e *software*, que normalmente tornam-se obsoletos e são substituídos por novas ferramentas que funcionam de maneira diferente.
- Os materiais podem ser perdidos em caso de catástrofes como incêndios, inundações, falha do equipamento, vírus, ou ataque direto que desativa os dados armazenados e os sistemas operacionais.
- Barreiras de acesso, como a proteção de senha, criptografia, dispositivos de segurança, podem impedir o acesso contínuo para além das circunstâncias limitadas para qual foram concebidas.
- O valor do material não pode ser reconhecido antes de ser perdido ou alterado.
- Ninguém deve ser responsabilizado pelo material, ainda que seu valor seja reconhecido.
- Poderá haver insuficiência de recursos disponíveis para sustentar a ação de preservação.
- Poderá não ser possível negociar as permissões legais para a necessidade de preservação.
- Pode não haver tempo ou habilidades disponíveis para responder com rapidez a uma mudança tecnológica repentina.
- Os materiais digitais podem ser bem protegidos, mas tão mal identificados e descritos que usuários potenciais podem não encontrá-los.
- Aspectos críticos de funcionalidade como formatação de documentos ou as regras de operação de bancos de dados, podem não ser reconhecidos, descartados ou danificados no processo de preservação (NATIONAL LIBRARY OF AUSTRALIA, 2003, p. 30-31).

Devido à grande quantidade de dados produzidos em formato digital e sua natureza dinâmica, essa se configura como outra ameaça à continuidade digital e desafia a capacidade de coleta, de armazenamento e de acesso a esses dados. Esse conjunto de fatores indica que as decisões devem ser tomadas de acordo com a Curadoria de Dados e não ser tratado como preservação digital.

Segundo Harvey (2010, p. 10):

As respostas a essas ameaças de continuidade digital que são baseadas em abordagens de preservação tradicionais não funcionam.

Simplemente capturar dados em mídias de armazenamento estáveis e depois copiá-las em novas mídias quando as anteriores se tornarem obsoletas é uma ameaça. Dados digitais devem ser geridos desde sua criação se a pretensão for de sobrevivência.

Diante disso, podemos afirmar que a gestão ativa dos dados por meio de seu ciclo de vida é condição *Sine qua non* para a Curadoria Digital.

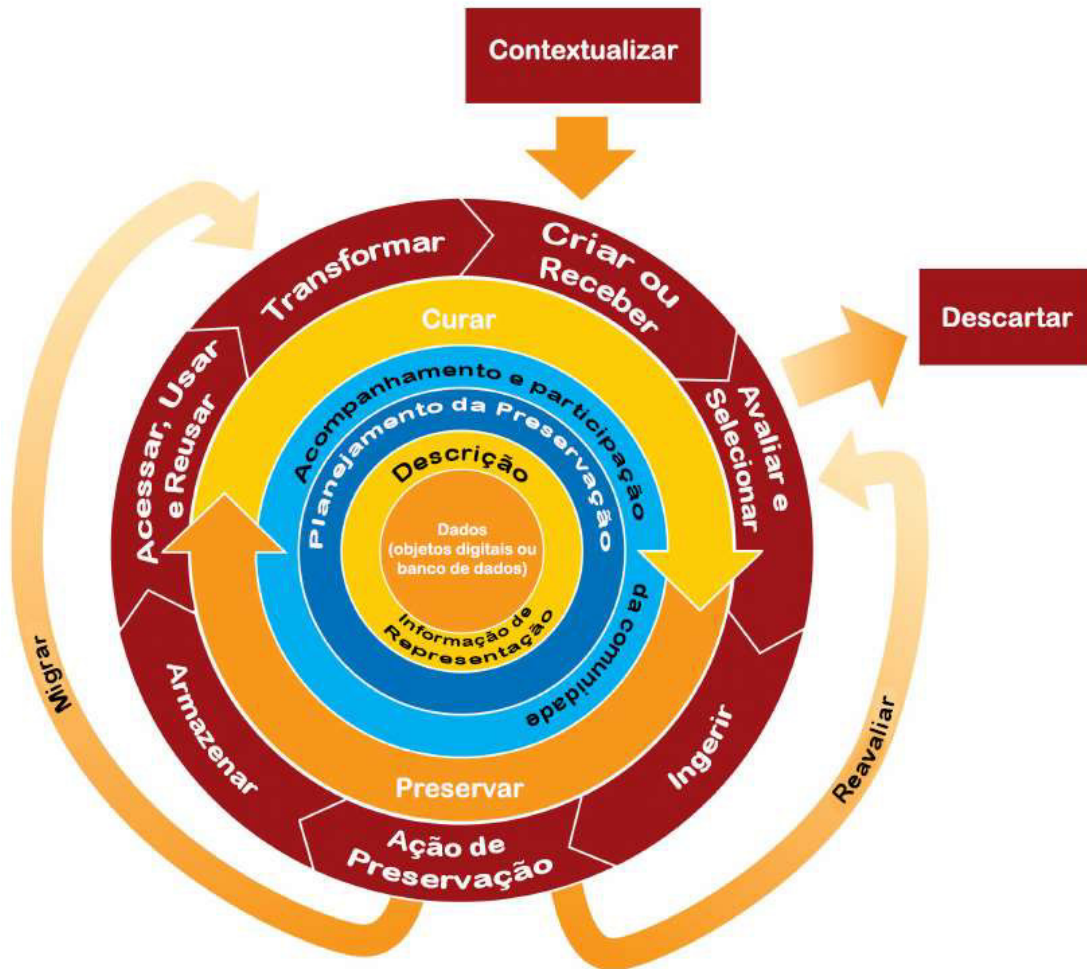
## 2.6 Ciclo de vida da Curadoria Digital

A Curadoria Digital abarca todo o ciclo de vida dos documentos digitais para que haja sucesso no processo curatorial. Assim, um Modelo de Ciclo de Vida de Curadoria, foi desenvolvido pelo *Digital Curation Centre*, demonstrando numa visão geral quais são as etapas necessárias para a curadoria e a preservação dos dados. Nesse contexto, é possível que o ciclo de vida garanta que todas as etapas do ciclo sejam identificadas e planejadas, que as ações necessárias sejam também desenvolvidas numa sequência correta. Tal processo garantirá a manutenção da autenticidade, confiabilidade, integridade e usabilidade do objeto digital (HIGGINS, 2008).

Assim, o *Digital Curation Centre* (2008) propõe um Modelo do Ciclo de Vida da Curadoria, expresso graficamente, conforme Figura 1 a seguir, que descreve as etapas que devem ser seguidas, bem como o planejamento das atividades que deverão ser desenvolvidas pelas organizações. Logo, o ciclo de vida dos dados é a forma de como os dados são criados, como são usados antes que cheguem a um arquivo e como e por quem serão utilizados no futuro.

Cuidando de todo processo de ciclo de vida dos dados, desde a criação até a manutenção e preparando a forma como os dados devem ser ajustados ou migrados, serão tomadas decisões desde o início do processo, no qual tais decisões garantirão o acesso aos dados no futuro. Cabe ressaltar que nem sempre passar por todos os processos é uma regra a todas as organizações, porém os processos que compõem a curadoria deverão ser adequados à realidade de cada instituição.

**Figura 1** - Ciclo de vida da Curadoria Digital



**Fonte:** Digital Curation Centre (2008)

Os elementos-chave do modelo proposto pelo DCC são: dado, objetos digitais e o banco de dados.

No centro do ciclo de vida e das demais ações, está o dado digital, o qual se configura como qualquer informação codificada em formato binário, podendo tanto ser dado nascido digital, como também poderá ser migrado o que acontece a partir do processo de digitalização.

O universo dos dados é composto por:

**Objetos digitais:** podem ser simples e são aqueles itens digitais compostos por um único arquivo como os arquivos de textos, arquivos de imagens ou arquivos de som

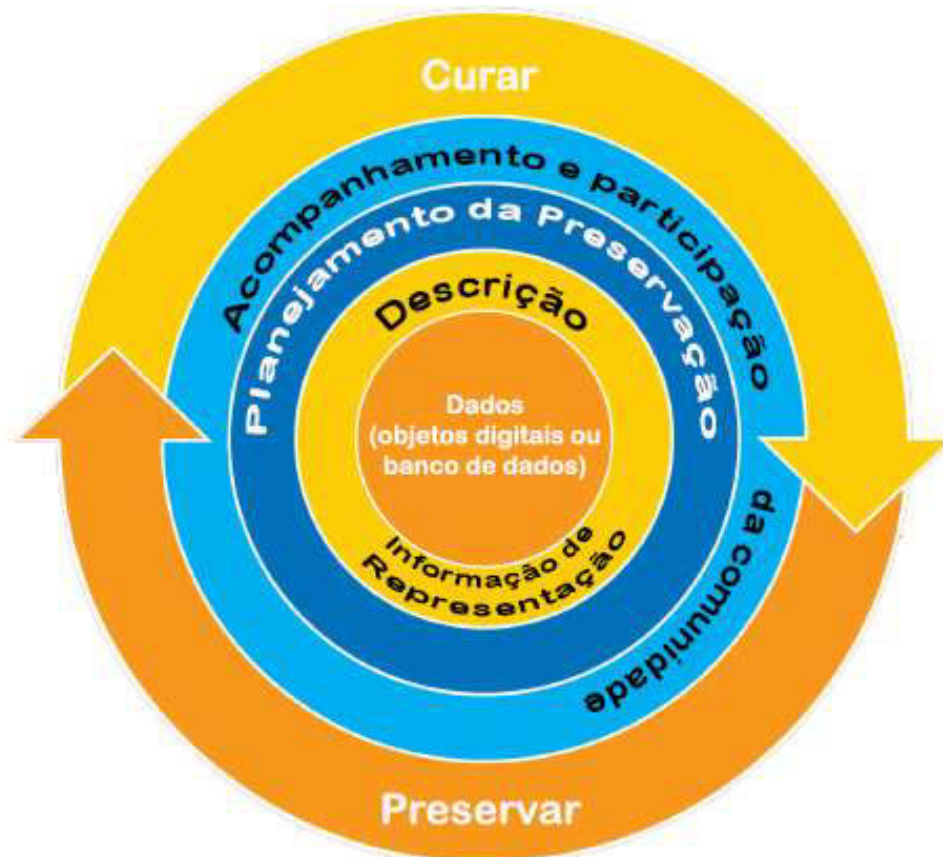
juntamente com seus identificadores relacionados e metadados; ou os objetos digitais complexos que são formados pela combinação de uma quantidade de outros objetos digitais, como um *website*;

**Banco de dados:** coleções estruturadas de registro ou dados armazenados em um sistema de computador.

Para a efetivação do processo de curadoria proposto pelo modelo do DCC, ações devem ser tomadas no decorrer do processo. São propostos três tipos de ações: ações para todo ciclo de vida; ações sequenciais e ações ocasionais. As ações serão exemplificadas nas figuras 2, 3 e 4.

A primeira ação proposta pelo modelo do DCC - ações para todo ciclo de vida - são assim chamadas por compreenderem atividades que vão entremear todo ciclo de vida da curadoria digital. Podemos visualizar essas ações dentro do ciclo de vida da Curadoria Digital na Figura 2, a seguir.

**Figura 2** - Ações para todo ciclo de vida da Curadoria Digital



**Fonte:** Adaptado de Digital Curation Centre (2008)

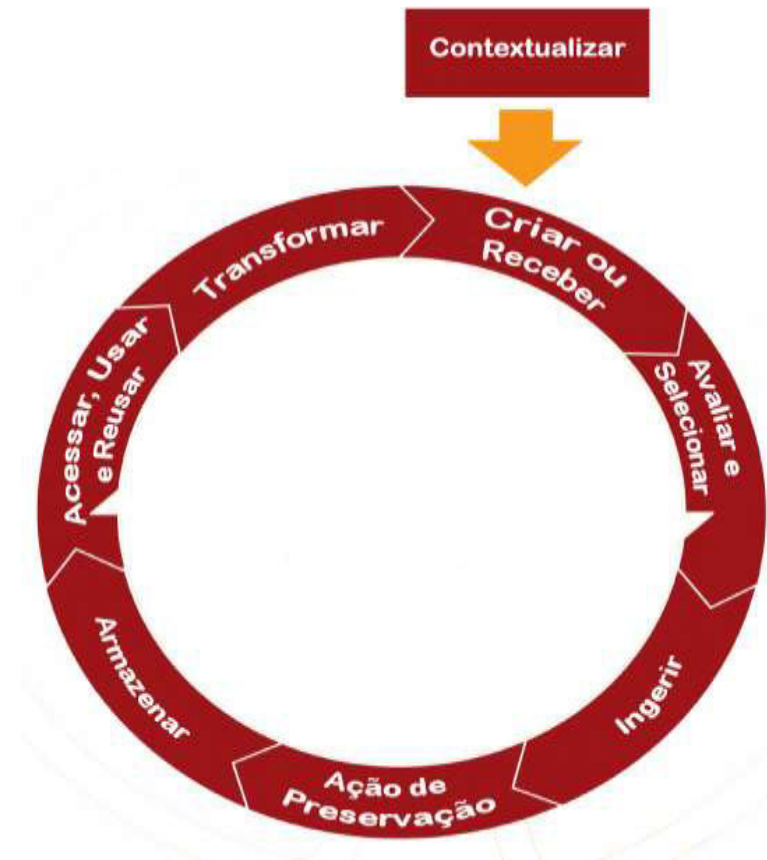
Partindo do centro do Ciclo de Vida da Curadoria Digital, onde se encontram os dados, os objetos digitais e o banco de dados, as ações propostas serão para todo ciclo de vida da Curadoria Digital que em consonância com o *Digital Curation Centre* (2008) são:

1. Descrição e representação da informação: é efetivada pela atribuição dos metadados descritivos, administrativos, técnicos, estruturais e de preservação, utilizando padrões apropriados para que se garanta a descrição e o controle adequado em longo prazo. Também compreende a coleta e a atribuição de informações de representações necessárias para o entendimento do dado e para sua apresentação (SAYÃO; SALES, 2012).
2. Planejamento da preservação: que é plano para a preservação de todo ciclo de vida da curadoria do material digital, incluindo o plano de gestão, administração, políticas e tecnologias.
3. Acompanhamento e Participação da Comunidade: nesse momento, deve-se manter o acompanhamento das atividades comunitárias, quando a comunidade está envolvida com o acervo que será curado; participar no desenvolvimento de padrões, de ferramentas, de políticas e de *software* adequados.
4. Curadoria e preservação: é preciso estar atento e sempre que necessário, empreender ações administrativas e gerenciais previstas para promover a curadoria e preservação ao longo do ciclo de vida de curadoria.

Já as Ações Sequenciais que devem ser realizadas de forma sistemática e sequencial são as que devem ser cumpridas frequentemente, visto que essas ações asseguram que o dado se manterá num ininterrupto processo de curadoria. Segundo Sayão e Sales (2012, p. 186), “Essa sequência não é para ser cumprida meramente uma vez do começo ao fim; na realidade ela forma as bases da cadeia de curadoria e continua ciclicamente todo o tempo em que o dado estiver sob curadoria”.

Para uma melhor visualização, essas ações poderão ser verificadas na Figura 3.

**Figura 3** - Ações sequenciais do ciclo de vida da Curadoria Digital



**Fonte:** Adaptado de Digital Curation Centre (2008)

Para esta etapa, o DCC elencou uma sequência de ações do modelo de Ciclo de Vida da Curadoria Digital com os seguintes estágios:

1. **Conceitualização:** Conceber e planejar a criação de dados, incluindo métodos de captura e as opções de armazenamento que abarcam as questões de propriedade intelectual, embargos e restrições, financiamento, responsabilidades, objetivos específicos de pesquisa, ferramentas de captura e calibração devem ser registrados.
2. **Criação e/ou recebimento:** Criação de dados incluindo esquemas de metadados que são necessários à sua gestão ou compreensão como os metadados administrativos, descritivos, estruturais e técnicos (metadados de preservação podem também ser adicionados na criação do dado). Como nem

sempre os dados são arquivados por quem os gerou, esse estágio inclui também a representação descritiva e temática dos documentos digitais,

3. Avaliação e seleção: O dado deverá ser avaliado e selecionado, pois será o objeto dos processos de curadoria e de preservação por longo prazo. Nessa ação, faz-se necessário aderir à orientação quanto às boas práticas, às políticas pertinentes e às exigências legais.
4. Arquivamento: Transferir do dado para um arquivo, um repositório, um centro de dados ou a outro custodiante apropriado.
5. Ações de preservação: Desenvolver ações para que a preservação de longo prazo e a retenção do dado de natureza oficial seja assegurada; ações de preservação devem possibilitar que o dado permaneça autêntico, confiável e capaz de ser usado, mantendo sua integridade. Essas ações incluem a higienização, validação, atribuição de metadados de preservação, atribuindo representação à informação e garantindo estruturas de dados aceitáveis ou formatos de arquivos.
6. Armazenamento: Armazenar o dado de maneira segura, mantendo a aderência aos padrões relevantes.
7. Acesso, uso e reuso: Garantir que o dado possa dia a dia ser acessado em uma base tanto pela sua comunidade-alvo, quanto pelos demais usuários interessados no reuso do dado. Essa base pode estar sob forma de informações publicadas e disponíveis para as comunidades interessadas, porém o controle de acesso e procedimentos de autenticação podem ser aplicados.
8. Transformação: Compreende a criação de novos dados a partir do original que poderá ser feito pela migração para um formato diferente, ou através da criação de um subconjunto, pela seleção ou consulta, para criação de resultados derivados que podem ser publicados.

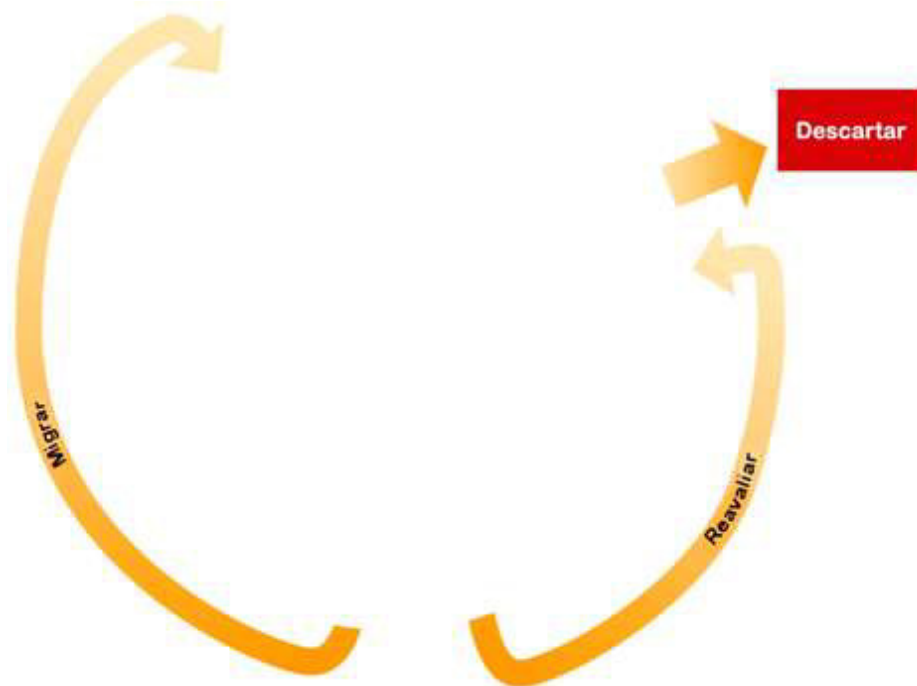
Conforme citado anteriormente, o Modelo também estabelece ações ocasionais que serão aplicadas eventualmente, ou seja, somente quando houver necessidade.

Sayão e Sales (2012, p. 187) ao discorrerem sobre essa etapa, fazem o seguinte apontamento:

Essas ações interrompem ou reordenam as ações sequenciais como desdobramento de uma decisão. Por exemplo, após uma avaliação pode ser decidido que o dado em questão não se enquadra no escopo de um repositório digital, isso implica que ele deve ser transferido para outro custodiante, Em outra situação, o dado deve ser destruído, possivelmente por motivações legais.

Na Figura 4, podemos visualizar as ações ocasionais que compõem a terceira fase do ciclo de vida da Curadoria Digital.

**Figura 4** - Ações ocasionais do ciclo de vida da Curadoria Digital



**Fonte:** Adaptado de Digital Curation Centre (2008)

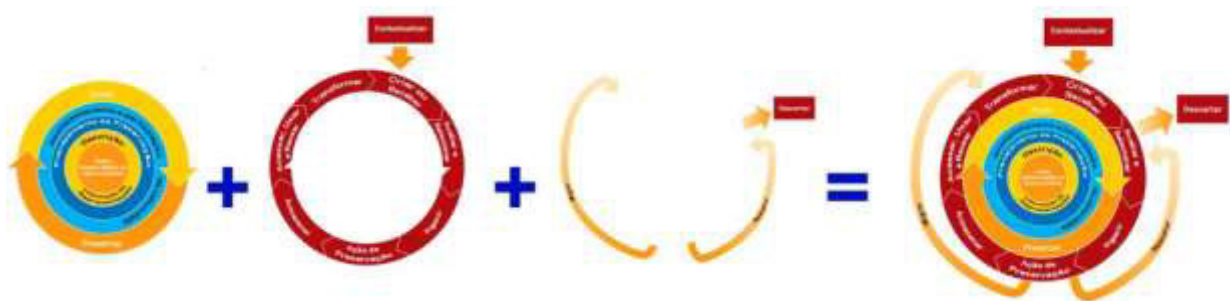
Fazem parte da última sequência de ações propostas pelo DCC para o Modelo de Ciclo de Vida da Curadoria Digital, as seguintes ações:

1. Descarte: Deverão ser descartados os dados que não foram selecionados para a curadoria de longo prazo e preservação, considerando as políticas documentadas, as diretrizes ou as exigências legais.
2. Reavaliação: Sempre que necessário fazer o retorno do dado em que os procedimentos de avaliação tiverem falhas, para que nova avaliação seja feita e, se possível, selecioná-lo para a curadoria;
3. Migração: Fazer a migração dos dados para um formato diferente; essa ação poderá ocorrer para que ele seja compatibilizado com o ambiente de armazenamento ou então para assegurar a imunidade do dado contra a obsolescência do *hardware* ou do *software*.

Diante do exposto, verifica-se que o Modelo proposto pelo DCC não somente nos possibilita uma percepção sobre o conjunto de funções pertinentes à curadoria, como também especifica papéis, responsabilidades e conceitos ao explicitar a infraestrutura de padronização e as tecnologias que devem ser implementadas (SAYÃO; SALES, 2012).

Todos os processos realizados na Curadoria Digital, conforme Figura 5, apresentada a seguir, são relevantes e complexos, bem como os cuidados que deverão ser tomados com o objeto digital.

**Figura 5 - Fases do ciclo de vida da Curadoria Digital**



**Fonte:** Adaptado de Digital Curation Centre (2008)

Segundo Yamaoka (2012, p. 70), o processo proposto por meio da Curadoria Digital cumpre seu objetivo de:

Salvaguardar os objetos digitais, possibilitando o acesso o uso e o reuso em todo seu ciclo de vida, permitindo: manter o documento íntegro e acessível, enquanto esse possuir valor jurídico (evidência); extrair novos conhecimentos (valor informacional); preservar a memória da sociedade (valor histórico) e evitar o retrabalho de recriar os dados já produzidos.

É bem possível que a Curadoria Digital, a partir dos dados, norteie uma alteração no ciclo de vida dos documentos arquivísticos, beneficiando o acesso persistente a dados digitais confiáveis ao melhorar sua qualidade no contexto da pesquisa e ao verificar sua autenticidade, contribuindo para que seja assegurada aos dados validade como registro arquivístico, apontando que poderão ser usados no futuro como evidência legal (SAYÃOS; SALES, 2012).

No próximo capítulo, discorreremos sobre como o arquivista pode propiciar a acesso à informação norteados pela Lei nº 12.527, conhecida como Lei de Acesso à Informação no Brasil, desde o ano de 2012, a Lei de Acesso à Informação (LAI), que tem como objetivo a transparência de informações custodiados pelos órgãos públicos e os saberes e fazeres do profissional arquivista.

### 3 ACESSO À INFORMAÇÃO E O ARQUIVISTA

Este capítulo discorre sobre a Lei de Acesso à Informação no âmbito nacional e internacional e suas principais propriedades no Brasil, sobre os fazeres e saberes do arquivista e quais as boas práticas profissionais que facilitam o acesso a documentos e informações arquivísticas.

#### 3.1 Lei de Acesso à Informação - LAI

Partindo da premissa que a informação é um direito fundamental de todo ser humano, não deverá haver barreiras para o acesso que se configura como condição *sine qua non* para a avaliação e participação ativa do cidadão na sociedade, visto que, a partir do acesso, há a possibilidade de ampliação de sua autonomia, pertencimento e empoderamento. Neste capítulo, serão apresentadas as principais propriedades da Lei de Acesso à Informação, retratando no âmbito internacional, quando e quais países incluíram a LAI em suas atividades e como o Brasil se encontra no cenário mundial no que diz respeito às leis de acesso.

Para Banisar (2006, p. 18, tradução nossa),

Somente após a Segunda Guerra Mundial, com a criação das Nações Unidas e das normas internacionais sobre direitos humanos, o direito à informação começou a se espalhar. [...] países começaram a promulgar leis abrangentes de acesso a documentos e informações.

Canavaggio e Balafrej (2011) também pactuam dessa mesma ideia e ressaltam que as mudanças relacionadas à criação de leis de acesso à informação somente se concretizaram após a Segunda Guerra Mundial e com a proclamação da Declaração Universal dos Direitos Humanos (DUHU). Desde então, foram efetivadas as discussões a respeito da lei de acesso à informação nas agendas dos governos ao redor do mundo e concretizadas a partir de pressões feitas pela comunidade internacional, com a constatação de que os direitos humanos haviam sido violados na guerra e somente o acesso aos documentos do pós-guerra poderiam comprovar os excessos.

No ano de 1948, na Assembleia Geral das Nações Unidas em Paris, foi proclamada a Declaração Universal dos Direitos Humanos, que delinea os direitos

humanos básicos, estabelecendo em seu artigo XIX que: “Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independente de fronteiras” (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009, p. 10-11). Com isso, declarações e legislações no âmbito profissional ou civil confirmam o direito e a relevância do acesso livre à informação.

No mesmo ano foi fundada, no continente americano, a Organização dos Estados Americanos (OEA), com o objetivo garantir soluções pacíficas para as divergências entre os países membros e para que o acesso à informação fosse tido como fundamental.

No ano de 1766, a Suécia foi o primeiro país a ter uma legislação que referenciasse o acesso à informação como um direito do cidadão, fato que a referencia como um marco legal no que diz respeito ao acesso à informação no contexto mundial, desta feita a “Ordenança sobre a liberdade de escrita e de imprensa” previa que:

Em adição aos registros de processos e outros assuntos referidos no texto original, todos que tiverem um caso ou outros procedimentos no tocante aos seus direitos perante qualquer tribunal ou órgão público como também perante os Estados do Reino, seus comitês seletos e permanentes, estarão livres para publicar considerações do mesmo juntamente com os documentos relacionados que se considere necessário. Contudo devem manter a verdade, cientes das responsabilidades previstas na lei (FREDERIC, 1766 apud ANDERS CHYDENIUS FOUNDATION, 2006, p. 14, tradução nossa).

Mendel (2009, p. 109), ao discorrer sobre o reconhecimento do direito de acesso à informação pela Suécia, declara:

É singular no sentido de ter sido a primeiro país do mundo ao adotar uma lei que concede aos indivíduos o direito de acesso à informação mantida por órgãos públicos, tendo incorporado disposições de direito à informação na Lei de Liberdade de Imprensa original em 1766.

Ainda que promulgasse a Lei de Acesso à Informação no ano de 1985, a Colômbia, desde 1888, permitia que os cidadãos solicitassem documentos que estivessem em custódia de órgãos governamentais ou ainda que se encontrassem nos

arquivos do governo. Após 200 anos da iniciativa da Suécia, os Estados Unidos, em 1966, aprovam a *Freedom of Information Act*.

Segundo Mendel (2009, p. 3),

Nos últimos anos, principalmente na passagem da década de 90 para os anos 2000, houve uma verdadeira revolução no direito à informação, que é comumente compreendido como o direito de acesso à informação mantida por órgãos públicos. [...] Em 1990, nenhuma organização intergovernamental reconhecia o direito à informação. [...] havia uma visão predominante do direito à informação como uma medida de governança administrativa. [...] hoje este direito é cada vez mais considerado como um direito humano fundamental.

O autor também aponta que bancos de desenvolvimento e instituições internacionais adotaram políticas de divulgação de informações. Vale destacar que, até os anos 90, somente 13 países haviam adotado leis de acesso à informação. De 1990 a 2016, ano que se encerra esta pesquisa, 114 países ao redor do mundo já adotam leis que garantam o acesso à população. O Quadro 1 demonstra a sequência da adoção das Leis de Acesso à Informação no mundo.

**Quadro 1** - Países que adotaram Leis de Acesso à Informação até 2016

Período	Nº de países	País
1776	1	Suécia
Década de 1950	1	Finlândia
Década de 1960	1	Estados Unidos da América
Década de 1970	4	Noruega, Dinamarca, Holanda e França.
Década de 1980	6	Nova Zelândia, Austrália, Canadá, Colômbia, Grécia e Áustria.
Década de 1990	19	Itália, Hungria, Portugal, Belize, Bélgica, Coreia do Sul, Islândia, Lituânia, Irlanda, Tailândia, Uzbequistão, Letônia, Israel, Geórgia, Trindade e Tobago, República Tcheca, Albânia e Liechtenstein.
Década de 2000	51	Moldávia, Estônia, República Eslovaca, África do Sul, Bulgária, Bósnia-Herzegovina, Reino Unido, Polônia, Romênia, Zimbábue, Panamá, México, Jamaica, Paquistão, Angola, Tajiquistão, Armênia, Eslovênia, Croácia, Sérvia, Peru, Kosovo, São Vicente e Granadinas, Turquia, Argentina, Suíça, Antígua e Barbuda, República Dominicana, Equador, Uganda, Montenegro, Índia, Taiwan, Azerbaijão, Honduras, Alemanha, Macedônia, Nicarágua, Nepal, República do Quirguistão, Jordânia, China, Bangladesh, Etiópia, Guatemala, Malta, Chile, Uruguai, Indonésia, Ilhas Cook e Rússia.
Década de 2010	31	República da Libéria, Guiné-Conacri, Mongólia, El Salvador, Brasil, Ucrânia, Nigéria, Tunísia, República do Niger, Iêmen, Serra Leoa, Guiana, Ruanda, Costa do Marfim, Espanha, Maldivia, Paraguai, Sri Lanka, Afeganistão, Burkina Faso, Togo, Vietnam, Moçambique, Filipinas.
Total de Países	114	

**Fonte:** Centre for Law and Democracy (2016)

O Brasil foi o 90º país a instituir a LAI no contexto mundial. Ainda que esse direito tenha sido determinado na Constituição de 1988, a criação de uma lei específica só ocorreu vinte anos mais tarde. A seguir, elencaremos os textos legais que asseguram o acesso aos documentos e à informação no Brasil:

1. A Constituição da República Federativa do Brasil, de 1988, Art.5º, XIV assegura o acesso à informação, resguardando o sigilo da fonte e XXXIII, sendo que todos têm “o direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do estado” (BRASIL, 1988).
2. A Lei Nº 9.507, de 12 de novembro de 1997, regulamenta o direito de acesso à informações e disciplina o rito processual do *habeas data*. Os registros ou banco de dados serão de caráter público se contiverem informações utilizadas especificamente pela organização ou instituição que as produziu;
3. O Decreto Nº 3.505, de 13 de junho de 2000, publicado no Diário Oficial da União (DOU) de 14/06/2000, institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, garantindo o acesso aos sistemas de informação somente para usuários autorizados, para evitar modificação ou perda de informação;
4. O Decreto nº 4.553, de 27 de dezembro de 2002, determina a preservação de dados, informações e materiais sigilosos, sendo que os últimos possuem acesso restrito. “Os dados ou informações sigilosas serão classificados em ultra-secretos, secretos, confidenciais e reservados em razão do seu teor ou de seus elementos intrínsecos”.
5. A resolução Nº 20, de 16 de julho de 2004, inclui documentos digitais nos programas de gestão de documentos arquivísticos das instituições que fazem parte do Sistema Nacional de Arquivos. É dever do Poder Público tornar acessível aos cidadãos as informações contidas nos documentos arquivísticos das instituições contidas nos documentos de caráter governamental.
6. Lei nº 12.527, de 18 de novembro de 2011 (que consta no anexo A), dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º no inciso II § 3º do art.37 e no § 2º do art.216 da

Constituição Federal, no seu capítulo II, dispõe sobre o acesso a informação e sua divulgação.

7. Decreto nº 7.724, de 16 de maio de 2012, regulamenta Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação.
8. Decreto nº 7.845, de 14 de novembro de 2012, regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo e dispõe sobre o Núcleo de Segurança e Credenciamento.

Também foram criadas leis que asseguram o direito à acessibilidade das pessoas portadoras de deficiências ou com mobilidade reduzida que podem ser percebidas também como leis que oportunizam o acesso às informações como o Decreto Lei de nº 5.296, de 2 de dezembro de 2004, que define acessibilidade como:

I – acessibilidade: condição para utilização, com segurança e autonomia, total ou assistida, dos espaços, mobiliários e equipamentos urbanos, das edificações, dos serviços de transporte e dos dispositivos, sistemas e meios de comunicação e informação, por pessoa portadora de deficiência ou com mobilidade reduzida;

II – barreiras: qualquer entrave ou obstáculo que limite ou impeça o acesso, a liberdade de movimento, a circulação com segurança e a possibilidade de as pessoas se comunicarem ou terem acesso à informação (BRASIL, 2004).

Esse decreto também define outras barreiras da comunicação:

d) barreiras nas comunicações e informações: qualquer entrave ou obstáculo que dificulte ou impossibilite a expressão ou o recebimento de mensagens por intermédio dos dispositivos, meios ou sistemas de comunicação, sejam ou não de massa, bem como aqueles que dificultem ou impossibilitem o acesso à informação (BRASIL, 2004).

A lei de acesso à informação, no Brasil, segundo o Freedom Info<sup>1</sup>, é resultado de seis anos de campanhas de grupos civis e organizações como a Associação Brasileira

---

<sup>1</sup> O portal [freedominfo.org](http://freedominfo.org) é uma rede virtual que une movimentos que lutam por abertura de informações. Funciona como um repositório sobre a memória institucional de campanhas de liberdade de informação em todo o mundo (FREEDOM INFO, 2013).

de Jornalismo Investigativo que foram os responsáveis pela organização do primeiro Seminário de Direito de Acesso a Informação Pública no ano de 2003, originando, a partir daí, o estabelecimento do Fórum Brasileiro para o Direito de Acesso à Informação Pública, formado por alianças de organizações dedicadas a promover o direito de acesso à informação objetivando a adoção de uma legislação própria.

No ano de 2005, foi formado por membros da Controladoria Geral da União, representantes do Ministério Público Federal e da Associação Brasileira de Imprensa e da Transparência Brasil o grupo de trabalho do Conselho de Transparência Pública e Combate a Corrupção. No final do ano de 2007, a Ordem dos Advogados do Brasil (OAB) moveu uma ação de inconstitucionalidade ao Supremo Tribunal Federal, contra as disposições da Lei Nacional de Arquivos (Lei nº 8.159) e da Lei de Classificação de Documentos (Lei nº 11.111), visto que permitiam a classificação de documentos por prazo indeterminado.

Em abril do ano de 2009, aconteceu o segundo Seminário Internacional de Acesso à Informação Pública, e o Poder Executivo enviou o projeto de lei que regulamentava o acesso às informações públicas (Projeto de Lei 5228/2009), que chegou ao Senado em 2010 e foi promulgada em 18 de novembro de 2011 como Lei nº 12.527 - Lei de Acesso à Informação e entrou em vigor seis meses depois, visto que foi regulamentada pelo Decreto nº 7.724, de 16 de maio de 2012.

### **3.1.1 O direito ao acesso à informação no Brasil**

Tendo em vista o cenário de acesso à informação pública, no que se refere às informações relativas à transparência pública, a lei 12.527/11 objetiva divulgar diversos aspectos da administração pública. Em seu primeiro artigo, baliza sua finalidade que é de garantir o acesso às informações a partir do disposto sobre os procedimentos que devem ser observados pela União, Estados, Distrito Federal e Municípios. Apresenta, em seu artigo terceiro, as diretrizes que devem se executadas para que seja assegurado o direito fundamental de acesso à informação: observância da publicidade como preceito geral e do sigilo como exceção; divulgação de informações de interesse público, independente de solicitações; utilização dos meios de comunicação

viabilizados pela tecnologia da informação; fomento ao desenvolvimento da cultura e da transparência na administração pública; desenvolvimento do controle social da administração pública.

Quanto a sua abrangência, a LAI subordina todos os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo e Judiciário, às autarquias, às fundações públicas, às empresas públicas, às sociedades de economia mista, às entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios e às entidades sem fins lucrativos que recebam recursos públicos (CONTROLADORIA GERAL DA UNIÃO, 2014).

Tendo como premissa o acesso como regra e o sigilo como exceção, os artigos da Lei 12.527:11 que versam sobre acesso são: Artigo 10º prevê que: “Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades. [...] por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida” (BRASIL, 2011). Prevê também, nesse mesmo artigo, parágrafo terceiro, que “[...] são vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público” (BRASIL, 2011).

O artigo 21º é claro ao declarar que: “[...] não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais” (BRASIL, 2011). Ainda, em seu parágrafo único, afirma que “[...] informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objetos de restrição de acesso” (BRASIL, 2011).

No artigo 23º, a lei prevê exceções de acesso que incluem as informações consideradas:

[...] imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:

I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados ou organismos internacionais;

III - pôr em risco a vida, a segurança ou a saúde da população;  
 IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;  
 V - prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas;  
 VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;  
 VII – pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares;  
 VIII – comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações (BRASIL, 2011).

Seu artigo 24<sup>o</sup> apresenta os graus e prazos de sigilo de classificação da informação que estão em poder de órgão e entidades públicas. Os prazos máximos de restrições de acesso são:

- I – ultrassecreta: 25 (vinte e cinco) anos;
- II – secreta: 15 (quinze) anos;
- III – reservadas: 5 (cinco) anos.

Quanto à proteção das informações sigilosas, o artigo 25<sup>o</sup> considera que é “[...] dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção” (BRASIL, 2011).

O artigo 31<sup>o</sup> discorre sobre o prazo de sigilo no que diz respeito às informações pessoais, relativas à intimidade, vida privada, honra e imagem.

- I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100(cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
- II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem (BRASIL, 2011).

A lei também faz referência aos funcionários públicos que a descumprirem, e quais serão suas penas. Assim, em seu artigo 32<sup>o</sup> declara o que constituem em condutas ilícitas e que serão atribuídas ao agente público ou militar, dentre elas:

I - recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;  
II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;  
III - agir com dolo ou má-fé na análise das solicitações de acesso à informação (BRASIL, 2011).

Dentre as sanções previstas no artigo 33º a que estão sujeitos os agentes públicos que descumprirem a LAI figuram:

I – advertência;

II – multa;

III – rescisão do vínculo com o poder público.

Conforme já citado anteriormente, a lei 12.527:11, regulamentada pelo Decreto nº 7.845, de 14 de novembro de 2012, em seu artigo 40º dispõe:

As informações classificadas como documentos de guarda permanente que forem objeto de desclassificação serão encaminhadas ao Arquivo Nacional, ao arquivo permanente do órgão público, da entidade pública ou da instituição de caráter público, para fins de organização, preservação e acesso (BRASIL, 2011).

Diante do exposto, podemos afirmar que o acesso à informação necessita de dispositivos legais para que esse seja garantido, porém são necessários práticas e mecanismos que protejam sua efetivação e seja firmada a participação do cidadão na vida democrática do país. Canavaggio e Balafrej (2011, p. 21-22, tradução nossa) ao discorrerem a respeito da importância do acesso pela sociedade pontuam:

O acesso à informação se encontra no coração das estratégias desenvolvidas pelas organizações intragovernamentais e das ações conduzidas pela sociedade internacional na: luta contra impunidade, luta contra corrupção e promoção da boa governança.

Para que o acesso como recomendado pela lei seja possibilitado, é necessário que a informação solicitada esteja organizada e disponível para que possa ser

encontrada, acessada, usada e reusada. Nesse contexto, Rousseau e Couture (1994, p. 159) afirmam:

O desenvolvimento de uma arquivística nacional eficaz e dinâmica não pode ocorrer sem um determinado quadro jurídico, o qual registra uma tomada de consciência da importância dos arquivos por parte dos decisores. Esta condição é seguramente necessária, não é, contudo suficiente se não for acompanhada dos recursos humanos, financeiros e materiais, indispensáveis à criação de uma verdadeira política de arquivos.

O quadro jurídico como apontado é de importância capital para que informações e documentos sejam acessados, porém é necessário que boas práticas e métodos eficientes façam parte da rotina de trabalho do arquivista no que tange à disponibilização dos documentos e das informações.

Segundo Bellotto (1989, p. 81), “[...] a finalidade última dos arquivos, seu objetivo maior, é, pois, comprovadamente, o acesso à informação, seja em que idade documental for e, conseqüentemente, em que âmbito arquivístico for”. Devemos ressaltar que, desde o ano de 1989, está assegurado por lei o acesso aos documentos a toda sociedade.

Dotti (1990, p. 165) ao discorrer sobre o direito à informação afirma que:

O direito à informação é um direito universal, inviolável e inalterável do homem moderno, posto que está fundamentado na natureza humana. Ele se movimenta na forma ativa e passiva: de uma parte a procura da informação e, de outra, a possibilidade em favor de todos de a receber.

Segundo Ardenghi (2012, p. 243), “O direito à informação, como alicerce fundamental, para a preservação da verdade factual, é indispensável e requer a informação exata e honesta”. Nesse cenário, o público alvo de instituições arquivísticas necessita que as informações custodiadas em repositórios arquivísticos digitais sejam confiáveis e se encontrem acessíveis de maneira fácil e intuitiva.

Note-se que a promulgação da LAI, no ano de 2012, intensificou o debate a respeito da adoção de boas práticas arquivísticas para a otimização e ampliação do acesso à informação. Porém, para que seja possível o acesso, em qualquer âmbito, faz-se imprescindível uma estrutura arquivística composta de: recursos humanos, recursos

materiais, recursos tecnológicos e metodologias que possibilitem que documentos e informações atendam às necessidades informacionais de sua comunidade alvo (CARVALHO; CIANCONI, 2015). Para tanto, é necessário ter clareza do papel do arquivista como profissional da informação que propiciará o acesso às informações agora garantidas por lei a todo cidadão brasileiro.

### **3.2 Saberes e fazeres do arquivista**

Estamos cada vez mais distantes dos tempos em que o arquivista exercia sua profissão sozinho, em meio a um caos de papéis e livros. Com o processo de dinamização e disseminação da informação, documentos são criados e mantidos em sistemas de informações na forma de banco de dados, assim, abrigam um extraordinário volume de informações que necessitam de tratamento, para que possam ser disponibilizadas.

Para Viana (2015, p. 15),

O contexto arquivístico contemporâneo também tem se mostrado dinâmico na medida que em outras áreas do conhecimento reconhecem nos arquivos a fonte primária de temas adjacentes aos seus interesses, como os que envolvem a cultura, o patrimônio, a memória, o esquecimento, entre outros.

Rousseau e Couture (1994, p. 262), ao discorrerem sobre como seria um arquivista completo, apontam dois aspectos que para eles são essenciais: “[...] devem ser capazes de intervir na totalidade dos suportes de arquivos, e o seu campo de actividade deve cobrir todo o ciclo de vida dos documentos”.

Grimard (1989 apud ROUSSEAU; COUTURE, 1994, p. 263-264), ao abordar as questões que o arquivista deve responder, estabelece:

[...] deve ser um profissional capaz de assegurar a salvaguarda da memória coletiva. [...] deve participar, através das suas intervenções, no respeito dos direitos da pessoa. Necessita efetivamente de assumir a parte que lhe cabe na organização e no tratamento da informação, respeitando as leis de acesso à informação e as que visem a protecção da vida privada. [...] deve ser capaz de assegurar uma organização e um tratamento dos arquivos que tenham em conta as normas legais.

Jardim (1995, p. 73), ao discorrer sobre a atuação dos profissionais arquivistas, declara: “Neste palco nem sempre iluminado, uma categoria profissional ainda emergente, a dos arquivistas, é o principal ator, quase um figurante contido e perifericamente situado nesta cena”. Podemos perceber que o autor pondera que o arquivista deve assumir seu papel de ator participante.

Ribeiro (2002, p. 20), em uma visão mais atualizada, afirma que, a partir da década de 90 do século XX:

No contexto socioeconômico, cultural e tecnológico da sociedade da informação, a Arquivística entrou definitivamente em uma nova fase – a era pós-custodial – em que os arquivos emergem como sistemas de informação social, cuja complexidade não se confina apenas à organização material dos documentos e ao seu tratamento técnico.

Assim, segundo a autora, o arquivista deixa de ser somente o preparador de instrumentos de pesquisa para servir o historiador e

[...] começa a dar lugar ao profissional/cientista da informação que numa relação de interdisciplinaridade, colabora com o historiador partilhando algo em comum – a Informação. Contudo, enquanto o historiador se serve dos arquivos como fontes de informação o arquivista relaciona-se com a informação de modo completamente diverso (RIBEIRO, 2002, p. 20).

Segundo o Conselho Internacional de Arquivos (2012, p. 12), os arquivistas são profissionais,

[...] responsáveis pelo planejamento, implementação e manutenção dos sistemas de controle de acesso. [...] devem entender os princípios básicos de acesso, a necessidade de manipulação segura de informações restritas, e a responsabilidade de não divulgar informações a menos que estas se tenham tornado públicas por meio de procedimentos aprovados. Os arquivistas que participam do processo de tomada de decisão sobre acesso devem ter uma boa compreensão das leis pertinentes e das práticas de acesso, bem como das necessidades dos pesquisadores.

Para os autores, no que tange à aplicação da Lei 12.527:11, o arquivista é o profissional responsável por sua análise, objetivando transparência das ações públicas

que, dessa maneira, garantirá e protegerá o direito do cidadão no que diz respeito ao acesso à informação.

Banisar (2006, p. 58, tradução nossa) nos alerta que a organização da informação arquivística e a eficiência de seus sistemas são condições ímpares para que seja assegurado o acesso.

Para que a liberdade de informação funcione, é necessário que exista um sistema de manutenção de registros que permita uma coleta, indexação, armazenamento e descarte de informações. Muitos países possuem sistemas de arquivos deficientes o que prejudica seriamente os esforços para recuperar informações.

Podemos perceber que esta preocupação é partilhada por Mendel (2009) ao dizer que um dos maiores obstáculos que vários países enfrentam, no que se refere ao acesso à informação, é o estado em que se encontram os documentos e por Canavaggio e Balafrej (2011, p. 23, tradução nossa), tendo em vista a afirmação dos autores de que “[...] um sistema nacional de arquivos públicos sólido é indispensável para assegurar a preservação a longo prazo e o acesso aos documentos que provam a existência do Estado de Direitos dos indivíduos”.

Diante do exposto, temos a certeza de que, para a disseminação e acesso à informação, faz-se urgente que o arquivista assuma seu papel de Usuário-Chave. Segundo Mueller (1996, p. 271), o profissional deve ser: “[...] vivo e atuante. Como? Através do aprimoramento contínuo e afinado com a realidade”. Tal dinamismo será possível a partir de uma postura crítica de si mesmo e pela percepção da necessidade de uma busca constante de atualização, pois os formatos de apresentação da informação: analógico, digital e híbrido, os sistemas de informação os segmentos de bens e serviços são temas desafiadores para os arquivistas.

As TIC são ferramentas básicas do arquivista, visto que deve ser o instrumento de trabalho para profissionais que têm como objeto de trabalho a informação, uma vez que a organização, o tratamento, a disponibilização, o acesso, a busca, a recuperação, o uso e reuso, a partir do uso das tecnologias, são mais eficientes e eficazes.

Cook (2011, p. 249) é categórico ao afirmar que “[...] as leis de acesso à informação exigem práticas viáveis de gestão de documentos. Claramente, não faz

sentido dar às pessoas o direito de acesso a documento ou a informações, quando os documentos não podem ser encontrados”.

Além de proporcionar o acesso à história para a construção da memória, ao facilitar o acesso aos documentos e informações, o profissional arquivista propicia ao cidadão o sentimento de pertencimento e conseqüentemente o empoderamento social. Assim, a sua atuação vai muito além da organização, portanto é ele quem dará valorização às informações, além de ter um papel determinante na tomada de decisões e no gerenciamento de pessoas.

Segundo dados de pesquisa feita por Anna, Campos e Calmon (2015, p. 14), ao perguntarem a arquivistas atuantes se o profissional tem poder decisório e delegação para gerenciar pessoas, obtiveram a seguinte resposta: “O mesmo é responsável por todas as atividades no setor e ainda possui poder de decisão; quando há necessidade de gerenciar pessoas, isso é feito naturalmente”.

Dessa feita, faz-se necessário estabelecer programas de gestão dos documentos, para que seja garantido o acesso e por conseguinte o seu uso e reuso.

Após o estudo sobre Acesso, Lei de Acesso à Informação e do Profissional Arquivista e, fundamentada nos estudos de Ribeiro (2002), Santos (2002), Valentim (2002), Bellotto (2004) e Sayão e Sales (2012), apresenta-se a sistematização de ações do profissional que possibilita e/ou facilita o acesso às informações arquivísticas, além do tratamento documental de avaliação, descrição, indexação, eliminação, arquivamento e disponibilização da informação conforme as normas arquivísticas.

**Quadro 2** - Ações do arquivista para o acesso a documentos e informações

Conhecer a Lei nº 12527 - Lei de Acesso à Informação e a Lei nº 8.159 - Lei dos arquivos.
Trabalhar com uma equipe multidisciplinar.
Utilizar as tecnologias de Informação e Comunicação como ferramentas básicas de trabalho.
Ser parte integrante em equipes para criação de repositórios arquivísticos digitais confiáveis.
Entender e utilizar os processos do Ciclo de Vida da Curadoria Digital.

Trabalhar para a disponibilização dos dados, das informações e dos documentos na ambiência digital, conhecendo metadados arquivísticos disponíveis para a descrição e gestão do acervo, no favorecimento ao acesso à informação.
Assegurar que as políticas de acesso e as regras da instituição sejam conhecidas de maneira clara para o público especialista ou não.
Capacitar-se constantemente
Partir da premissa que o Acesso é a Regra e o Sigilo a Exceção.

**Fonte:** Elaborado pela autora

No Quadro 2, pode-se visualizar as ações que o Arquivista deve ter diante a demanda para satisfação das necessidades informacionais, considerando ciberespaço que rompe a distância física, temporal e as barreiras geográficas.

Santos (2002, p. 103) admite que o ponto de partida para o profissional da informação “[...] se legitima no contexto da sociedade contemporânea, que se encontra em processo acelerado de transformações e rupturas, sob o signo do acesso e detenção da informação”. Pode-se trazer esse apontamento para arquivologia, visto que, como afirma a autora: “Tais transformações exigem definições e redefinições de métodos que valorizem e destaquem os aspectos importantes desta relação de disponibilização e disseminação da informação”.

Ainda ao discorrer sobre o assunto, Santos (2002, p. 103) também identifica a informação como matéria prima do mundo contemporâneo, juntamente com as tecnologias disponíveis e vincula que “[...] o conhecimento por parte do profissional sobre o fluxo da informação, a percepção do ambiente informacional, a destreza do manuseio e no uso de recursos tecnológicos favorecerá o acesso”.

A presença das tecnologias, no cotidiano dos sujeitos, determina comportamentos, cria necessidades e forma opiniões o que torna a atuação de arquivistas necessária no processo de acesso e uso da informação que se encontra alocada em diferentes suportes (SANTOS, 2002).

Iacovino (2016, p. 262), ao refletir sobre documentos como prova e como memória, em um arquivo institucional ou não, afirma: “[...] no mundo atual, marcado

pela comunicação instantânea, documentos confiáveis e autênticos permanecem sendo essenciais, para a responsabilidade pessoal, institucional e coletiva”.

Os documentos arquivísticos precisam estar custodiados de maneira que preservem sua autenticidade, integridade e confiabilidade. Porém devem ser disponibilizados de maneira fácil, rápida e intuitiva, para tanto é fundamental que a formação do arquivista atenda a demanda social e que haja ações que divulguem o profissional para o mercado.

A confiabilidade dos Repositórios Digitais será o tema tratado no próximo capítulo.

## **4 CONFIABILIDADE EM ARQUIVOS DIGITAIS: UM CAMINHO PARA REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS**

Neste capítulo, o objetivo é falar de confiabilidade para a construção de repositórios arquivísticos digitais, pois se faz urgente que tais repositórios forneçam acesso confiável e de longo prazo dos recursos digitais por eles custodiados à sua comunidade alvo agora e no futuro. Entretanto, não se pode falar de confiabilidade sem antes explicitar as características e conceitos de repositórios digitais e repositórios arquivísticos digitais.

### **4.1 Repositórios digitais**

Com a expansão da Internet, a partir dos anos 1990, as instituições culturais, como os arquivos, as bibliotecas e os museus, passaram a fazer cópias digitais dos documentos por ela custodiados, valendo-se das Tecnologias de Informação e Comunicação (TIC), pois dessa maneira podiam disponibilizar seus conteúdos. Tal atividade possibilitou, sem dúvida, a ampliação do acesso à informação e conseqüentemente ao conhecimento.

Com o passar dos anos, aumentou-se o número das digitalizações no setor que custodia o patrimônio cultural. Assim, para que fosse possível monitorar os assuntos relacionados à salvaguarda das informações e dos documentos, foi encomendado pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), como parte do Programa da Memória do Mundo, um estudo sobre os Repositórios de pesquisa *Open Source*, o que permitiu tanto a análise das lacunas existentes e que fossem feitas recomendações de desenvolvimento de uma fonte digital aberta para o sistema de preservação.

A partir dos estudos e de seus resultados, no ano de 2007, a UNESCO apresenta o documento *Towards an Open Source Repository and Preservation System - Recommendations on the Implementation of an Open Source Digital Archival and Preservation System and on Related Software Development*, que apresenta a seguinte declaração:

[...] para objetos digitais simples, a solução para a preservação digital é relativamente bem compreendida, são necessárias ferramentas acessíveis, tecnologia e formação na utilização desses sistemas. [...] Não existe um suporte, de armazenamento permanente ou definitivo, nem haverá no futuro previsível. Ao contrário, é necessário elaborar sistemas para gerir a mudança inevitável de um sistema para o outro. O objetivo e a ênfase na preservação digital é construir sistemas sustentáveis ao invés de portadores permanentes. ...) É apenas encontrar uma solução para este problema, uma abordagem sustentável será encontrada para atender às necessidades de muitas comunidades (BRADLEY; LEI; BLACKALL, 2007, p. 3, tradução nossa).

O documento aponta que os sistemas de preservação devem considerar todas as questões pertinentes aos repositórios digitais, devem utilizar soluções de preservação já desenvolvidas, para que o custo na sua criação possa ser diminuído. Observa também que o modelo de funcionamento de um repositório digital sustentável deve ser constante, sempre ser atualizado e desenvolvido de acordo com as necessidades institucionais identificadas.

Owen (2007, p. 49, tradução nossa) tem uma visão mais objetiva para a solução do problema de preservação do patrimônio digital, com o seguinte apontamento:

[...] um novo tipo de instituições patrimoniais deveriam ser criadas para materiais digitais provisoriamente poderia ser chamado de Repositório do Patrimônio Digital. [...] seria caracterizada como: Instituição de memória para a sociedade digital, abrangendo toda a gama de materiais digitais (e seus processos subjacentes à criação e utilização) através do qual a sociedade se expressa (tecido digital da sociedade); - Nova instituição ao lado de arquivos, bibliotecas e museus.

Apesar de propor a criação de uma nova instituição que ficaria responsável por materiais digitais, o autor reconhece que as instituições já existentes como os arquivos, as bibliotecas e os museus, ligadas à cultura como um todo e à cultura oficial, devem dar continuidade ao seu trabalho de preservação do patrimônio pré-digital.

No início da década de 1990, no Laboratório Nacional Los Alamos, Novo México, nos Estados Unidos da América (EUA), surgiu o primeiro repositório digital, o qual foi denominado *LANL preprint archive*, foi organizado por Paul Gispang, como um arquivo para *preprints* na física, e depois expandido, incluindo astronomia, ciência da computação, física, matemática e ciência não linear, biologia quantitativa, e estatística. Em 1999, teve seu nome alterado para arXiv, com o objetivo de ampliação e

flexibilidade. O repositório arXiv foi criado de forma experimental como uma alternativa ao modelo adotado no processo de comunicação científica, propiciado pela crise das revistas científicas (ALVES, 2008). O arXiv (arXiv.org) é mantido atualmente pela *Cornell University* e pela *National Science Foundation*.

Nesse contexto, os repositórios digitais emergem como uma possibilidade de acesso, de disseminação e de preservação da produção científica que, ao longo dos anos, tem seu crescimento acelerado.

Kuramoto (2006, p. 96) faz o seguinte comentário sobre a criação dos repositórios digitais:

No final da década de 90, surgem diversas manifestações em favor do acesso aberto ou acesso livre à informação científica, consequência das dificuldades encontradas em face da crise dos periódicos científicos. Buscaram-se alternativas de soluções no sentido de manter o acesso a essas revistas por meio de formações de consórcios, criando-se portais de acesso às revistas eletrônicas, mas as negociações com os editores de fora são difíceis.

Em 1996, uma força tarefa realizada pelo *Archiving do Digital Information* da *Commission on Preservation & Access* (CPA/RLG) apresenta o conceito de repositório ao falar sobre o desenvolvimento de um sistema nacional de Arquivos digitais :

[...] repositórios de informação digital que são coletivamente responsáveis para a acessibilidade de longo prazo do patrimônio social, econômico, cultural e da herança intelectual instanciado em formato digital. Os arquivos digitais são distintos das bibliotecas digitais no sentido de que estas, são repositórios que recolhem e dão acesso à informação digital, porém, podem ou não prover a longo prazo armazenamento e acesso a essa informação (WATERS; GARRETT, 1996, p. 3)

Diante do exposto, podemos considerar que os Repositórios Digitais – RDs são formados a partir de coleções digitais que podem ser construídas de formas e com propósitos diferentes, porém atuam como provedores dos dados que fazem o gerenciamento da informação. Para Viana, Márdero Arellano e Shintaku (2005, p. 3) o repositório digital se configura como:

[...] uma forma de armazenamento de objetos digitais que tem a capacidade de manter e gerenciar material por longos períodos e prover

o acesso apropriado. Essa estratégia foi possibilitada pela queda nos preços de armazenamento, pelo uso dos padrões como o protocolo de coleta de metadados da Iniciativa dos Arquivos Abertos (OAI-PMH), e pelos avanços no desenvolvimento dos padrões de metadados que dão suporte ao modelo de comunicação dos arquivos abertos.

No documento de Hayes (2005), *Digital repositories*, um repositório digital é “[...] onde conteúdos digitais estão armazenados e podem ser pesquisados e recuperados para uso posterior [...]” e ainda “[...] suporta mecanismos de importação, exportação, identificação, armazenamento e recuperação de recursos digitais”.

Essa definição é geral e pode ser aplicada a diferentes sistemas de informação. Faz-se necessário especificar os aspectos e características dos repositórios digitais que os diferenciam de base de dados, de sistemas de gestão de conteúdo e de outros que armazenam conteúdos digitais. Assim, recorreremos aos apontamentos de Heery e Anderson (2005, p. 1-2) que identificam quatro características como diferenciais dos repositórios em relação a outras coleções digitais: “Os conteúdos são depositados num repositório, quer pelo autor, proprietário ou por terceiro; a arquitetura do repositório gere tanto conteúdo como metadados e o repositório oferece um conjunto de serviços básicos mínimos, ex.: colocar, encontrar, pesquisar, controle de acesso”.

Na perspectiva de Márdero Arellano (2008, p. 124-125), um repositório digital é:

[...] um serviço de armazenamento de objetos digitais que tem a capacidade de manter e gerenciar materiais por longos períodos de tempo e prover o seu acesso apropriado. [...] compreendem um conjunto de ferramentas necessárias para os produtores, disseminadores e usuários de documentos digitais.

Para o autor supracitado, os repositórios têm ainda como objetivo o acesso aos documentos e às informações e o armazenamento de recursos.

Sayão e Marcondes (2009) apontam que os repositórios funcionam como uma base de dados na *Web* onde são depositadas produções e objetos informacionais, sendo disponibilizados dessa forma, para quem os procura. Os autores apresentam a seguinte concepção de repositórios digitais:

[...] um simples armazenador estático de informação digital com capacidade de recuperação foi rapidamente ultrapassado. A ideia

original deslocou-se para um conceito mais sofisticado de sistema de informação que incorpora a facilidade da comunicação, da colaboração e de outras formas de interação dinâmica entre usuários (SAYÃO; MARCONDES, 2009, p. 26).

Segundo Ferreira (2009), os repositórios digitais surgiram também como uma estratégia amparada pela Iniciativa dos Arquivos Abertos e pelo Movimento de Acesso Livre como instrumento de ação política; passaram, assim a ocupar um importante papel na discussão a respeito de direitos autorais, aumentando o impacto da Ciência e Tecnologia no âmbito científico, tecnológico e social.

Camargo e Vidotti (2009, p. 55), ao discorrerem sobre repositórios digitais afirmam que:

[...] repositórios digitais possibilitam o controle, a preservação e a visibilidade da produção científica, minimizando custos de publicações e permitindo o acesso irrestrito de outras comunidades universitárias e de pesquisa e da sociedade em geral.

O repositório digital favorece o armazenamento de um número grande de documentos, possibilitando assim que recursos sejam disponibilizados e preservados de forma que esses materiais possam ser acessados em longo prazo.

Para o Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) (20-),

Os repositórios digitais podem ser considerados uma inovação no gerenciamento da informação digital. Editoras, bibliotecas, arquivos e centros de informação em vários países estão criando grandes repositórios de informação digital, contendo diferentes tipos de conteúdos e formatos de arquivos digitais.

Nesse cenário, repositórios poderão ser apresentados de diferentes formas, para diferentes contextos, comunidades e objetivos quando determinados pela sua criação e funcionamento, ou também ser colaborativos, bem como apresentar ínfimo o alto nível de controle e acesso (MASSON, 2008).

Ainda segundo Masson (2008), os repositórios digitais objetivam preservar publicações criadas em meio digital, ou que sejam digitalizadas, para que corroborem com a memória institucional e estejam disponíveis e acessíveis para consulta.

Diante do exposto, temos a clareza de que os repositórios digitais são sistemas de informação que fazem o gerenciamento e o armazenamento de coleções de objetos digitais, por um longo período de tempo e proveem o acesso apropriado.

As Instituições que utilizam os repositórios são responsáveis por tal sistema de informação, cabendo a elas definir quais os objetivos, a finalidade e o tipo de repositório que devem colocar à disposição de sua comunidade, considerando: os documentos armazenados, as necessidades de sua comunidade de usuários, a acessibilidade, a durabilidade, a flexibilidade, a reutilização e a interoperabilidade; tendo como foco a garantia da confidencialidade, da autenticidade e da integridade da informação. O próximo item abordará os requisitos para a garantia da confiabilidade.

## **4.2 Repositórios digitais confiáveis**

Para que seja possível a preservação dos documentos e do patrimônio digital, é necessária a criação de repositórios digitais confiáveis. Para tanto, no ano de 2000, essa questão começou a ser tratada pelo *Research Libraries Group* (RLG) e o *Online Computer Library Center* (OCLC).

No ano de 2002, como resultado dos estudos e análise desse grupo de trabalho, foi publicado o relatório *Trusted Digital Repositories: Attributes and Responsibilities*, o que norteou a identificação de características para repositórios digitais para organizações de investigação, consolidando o modelo *Open Archival Information System* (OAIS). A sigla foi traduzida para o português como Sistema Aberto de Arquivamento de Informação (SAAI).

O modelo de referência OAIS, desenvolvido em 2002, a fim de que fosse normalizada a prática de preservação digital, ofereceu um conjunto de recomendações para que fossem implementados os programas de preservação. Assim, o OAIS refere-se a todas as questões técnicas do ciclo de vida de um objeto digital, desde a Recepção, Armazenamento, Gestão de Dados, Administração, Acesso até o Planejamento de preservação.

Segundo Lavoie (2004, p. 4, tradução nossa), quando se apresenta o Modelo de Referência para um Sistema de Informação Aberta de Arquivo ou OAIS, o termo

“Aberto” significa que: “[...] foi lançado em um fórum para um público aberto, em que qualquer interessado foi encorajado a participar”, poderá, entretanto, haver restrições de acesso à informação arquivada.

O autor afirma também que no modelo OAIS o arquivo é “[...] uma organização de pessoas e sistemas que aceitaram a responsabilidade de preservar a informação e torná-la disponível para uma comunidade-alvo” (LAVOIE, 2004, p. 4, tradução nossa), confirmando a premissa de que os repositórios têm como funções primeiras a conservação e a comunicação da informação.

O OAIS trata também das questões de metainformação, e recomenda quatro tipos de metainformação para cada objeto digital:

- Informação de referenciação (identificação);
- Informação de proveniência (incluindo o histórico de proveniência);
- Contexto e frigidéz (indicadores de autenticidade);
- Representação (formação, estrutura de arquivo, é o que confere o sentido ao *bitstream* de um objeto).

O documento *Trusted Digital Repositories: Attributes and Responsibilities: An RLG-OLCL Report (2002)*, elaborado pelo grupo de trabalho RLG e OCLC, formula as bases conceituais definidas como Repositórios Digitais Confiáveis e estabelece a definição, os atributos e as responsabilidades que devem ser assumidas para a criação de um Repositório Digital Confiável. O documento traz também uma discussão a respeito de se recriar a ideia de confiança, muito pertinente para a instituição do Patrimônio Cultural tratada nesta pesquisa.

Para o grupo de trabalho RLG/OCLC (2002, p. 5, tradução nossa), a definição de repositório digital confiável é: “[...] aquele cuja missão é possibilitar o acesso confiável, em longo prazo, aos recursos digitais, por ele gerido à sua comunidade alvo, agora e no futuro”.

O documento assinala que o sucesso no cumprimento de sua missão está relacionado aos deveres que os repositórios digitais devem:

- Aceitar, em nome de seus depositários, a responsabilidade pela manutenção, a longo prazo, de recursos digitais para seu uso agora e no futuro;
- Contar com um sistema organizacional que apoie não somente a visibilidade de longo prazo de repositório, mas também a informação digital em que ele tenha responsabilidade;
- Demonstrar responsabilidade fiscal e sustentabilidade;
- Projetar seu(s) sistema(s) em conformidade com as convenções e padrões aceitos para assegurar a gestão, o acesso e a segurança contínua dos materiais depositados;
- Estabelecer metodologias para avaliação dos sistemas que considerem as expectativas de confiabilidade esperadas pela comunidade;
- Ser dependente para desempenhar suas responsabilidades de longo prazo aos depositários e aos usuários de maneira aberta e explícita;
- Ter políticas, práticas e desempenho que possam ser auditáveis e mensuráveis;
- Cumprir o conjunto de responsabilidades.

O relatório identifica e aponta os atributos primários que um repositório digital confiável deve possuir, estabelecendo um rol de requisitos que abarcam diferentes situações e responsabilidades, e oferece uma base do que se pode esperar de um repositório confiável.

Esses atributos são:

- Estar em conformidade com o modelo OAIS;
- Ter responsabilidade Administrativa;
- Oferecer viabilidade Organizacional;
- Possuir sustentabilidade Financeira;
- Possuir adequação tecnológica e de procedimentos;
- Ter segurança do Sistema;
- Oferecer responsabilidade de procedimentos.

O requisito - estar em conformidade com o modelo OAIS -, é a condição primeira de um repositório. A Figura 6 demonstra o que é o Modelo de ambiente de um OAIS.

**Figura 6** - Modelo de ambiente de um OAIS



**Fonte:** Consultative Committee for Space Data Systems (2012, p. 22, tradução nossa)

Fazem parte do ambiente externo do OAIS três intervenientes: o Produtor, o Administrador e o Consumidor.

O Produtor é a pessoa que fornece a informação a ser preservada, o Administrador é quem vai fornecer a política geral do arquivo OAIS e fazer o controle da gestão e o Consumidor são as pessoas que interagem com os serviços do OAIS, isto é, procuram e adquirem a informação que se encontra no arquivo OAIS (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2012).

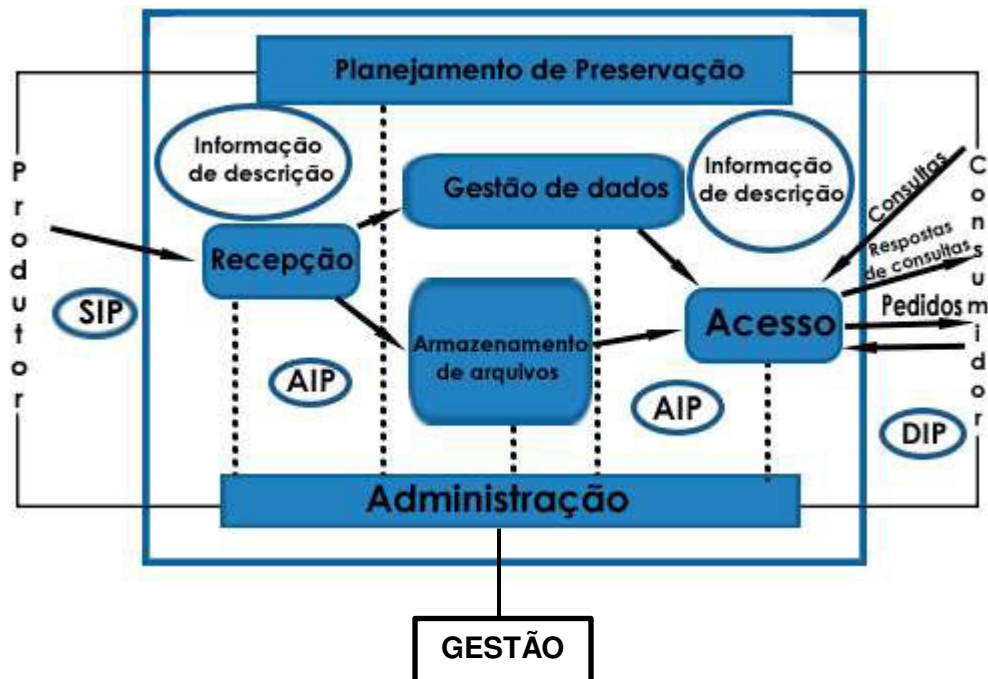
O OAIS é composto de seis entidades funcionais e que se relacionam com o produtor, o consumidor e o Administrador. São elas: recepção, gerenciamento de dados, armazenamento de arquivo, acesso, planejamento de preservação e administração do sistema. “As linhas que conectam as entidades identificam os caminhos de comunicação sobre o qual a informação flui nos dois sentidos.” (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2012, p. 41).

Thomaz e Soares (2004, p. 12) descrevem os três pacotes de informação que estão dentro do esquema OAIS que são:

- Pacote de Submissão de Informação (PSI), pacote enviado do Produtor para o Arquivo;
- Pacote de Arquivamento de Informação (PAI), pacote de Informação efetivamente armazenado dentro do arquivo;
- e Pacote de Disseminação da Informação (PDI), pacote transferido do Arquivo para um Consumidor em resposta a uma solicitação.

O modelo funcional OAIS inclui um modelo funcional, conforme Figura 7 e, em um primeiro nível de detalhamento, podemos identificar as seis entidades funcionais citadas anteriormente.

**Figura 7 - Entidades funcionais OAIS**



**Fonte:** Consultative Committee for Space Data Systems (2012, p. 41)

Nesse modelo funcional, podemos verificar a responsabilidade de cada entidade por algum dos processos do sistema no ambiente OAIS.

Entidade Recepção: é responsável pelo recebimento e tratamento dos PSIs dos produtores e (ou de componentes internos sob o controle da Administração do Sistema) e pelo envio do PAI para o armazenamento das informações descritivas (metadados)

para o gerenciamento dos dados, de acordo com a formatação e os padrões de documentos definidos (GRÁCIO, 2011).

Entidade Armazenamento: lida com o armazenamento, manutenção e recuperação de PAIs, de acordo com diversos critérios já estabelecidos e, quando solicitado, fornece os pacotes para a entidade Acesso (GRÁCIO, 2011).

Entidade Gerenciamento de Dados: armazena, faz a manutenção e a recuperação da informação descritiva e dos dados administrativos utilizados para gerenciá-la (GRÁCIO, 2011).

Entidade Administração de Sistema: gerencia a rotina operacional do arquivo como um todo. Suas funções são: solicitar e negociar acordos de submissão com produtores; auditar as submissões para garantir que estejam dentro dos padrões do arquivo; gerenciar e configuração de *hardware* e *software* do sistema; monitorar e melhorar as operações de arquivo e desenvolver inventários sobre a migração/atualização do conteúdo do arquivo; criar e manter padrões de arquivo e políticas, fornecendo suporte ao cliente bem como atender solicitações pendentes (GRÁCIO, 2011).

Entidade Planejamento e Preservação: monitora o ambiente OAIS e fornece recomendações que garantam o acesso à informação armazenada a longo prazo à Comunidade Alvo, mesmo que o ambiente computacional original tenha se tornado obsoleto. Fazem parte de suas funções: avaliação dos conteúdos dos arquivos; recomendações periódicas de estratégias de migração; desenvolvimento de recomendações para padrões e políticas do arquivo; monitoramento das mudanças no ambiente tecnológico e nas demandas; desenvolvimento de planos detalhados de migração; protótipos de *software* e planos de teste para atingir as metas de migração da entidade Administração do Sistema (GRÁCIO, 2011).

Entidade Acesso: atende as necessidades dos consumidores por meio de serviços de recebimento de solicitações; aplicação de controles que limitem o acesso principalmente à informação protegida; coordenação da execução de solicitações, para que sejam bem sucedidas; geração de respostas como os Pacotes de Disseminação da Informação e entregar as respostas aos consumidores (GRÁCIO, 2011).

Partindo da premissa de que os repositórios digitais confiáveis têm que estar em conformidade com o ambiente OAIS, as bibliotecas da Universidade de Cornell e do *Massachusetts Institute of Technology* (MIT) reproduziram as relações entre os atributos dos repositórios digitais confiáveis e ressaltaram que o atributo “estar em conformidade com o OAIS” é um atributo inerente. Dessa maneira, todos os outros atributos estão submetidos a ele, conforme Figura 8.

**Figura 8** - Modelo Cornell para atributos de repositório digital confiável



**Fonte:** Cornell University (2014)

Na relação entre os atributos de um repositório digital confiável, representados no modelo de Cornell, identifica-se o destaque dado no âmbito organizacional, posicionando a tecnologia no contexto informacional. Tal posicionamento evidencia que a tecnologia deverá adequar-se ao contexto e às necessidades dos programas de preservação digital.

O modelo também aponta uma fronteira para os arquivos digitais, para os atributos dos repositórios digitais confiáveis, visto que uma organização pode manter mais que um domínio de repositórios, os quais poderão ser coordenados pela

organização, ou então, várias organizações poderão se unir para administrar um repositório, como acontece quando se tem um consórcio (MCGOVERN, 2007).

Já para o quesito de responsabilidade, o documento *Trusted Digital Repositories: Attributes and Responsibilities: An RGL-OLCL Report* (2002), sugere:

- Negociar e aceitar informação adequada dos produtores de informação e dos detentores de direitos. (*Copyright*, privacidade; acesso atual e futuro; metadados técnicos e bibliográficos; teste de autenticidade; documentação para o arquivamento permanente).
- Ter o controle suficiente da informação. (Análise do conteúdo, propriedades significativas, formatos aceitáveis, migrações; nível de preservação para cada classe de documento; verificação de metadados; Identificação persistente; pacote de armazenamento; verificação de autenticidade e integridade; armazenamento (centralizado, distribuído ou terceirizado).
- Determinar as comunidades-alvo. (Base de conhecimento e sua capacidade técnica).
- Assegurar que a informação a ser preservada seja compreensível para a comunidade-alvo de forma independente. (Uso de metadados técnicos, sua base de conhecimento e/ou mudança de tecnologia).
- Seguir políticas e procedimentos documentados. (Políticas para formação de coleções, controle de acesso para armazenamento, para definir a comunidade-alvo; vínculo entre políticas e procedimentos).
- Tornar a informação preservada disponível para a comunidade alvo. (Descoberta de recursos; autenticidade; restrições legais; política de preços; suporte ao usuário).
- Defender o uso de boas práticas na criação de recursos digitais (Padronização).

Banat-Berger, Duploux e Huc (2009) identificam essas reponsabilidades como as do arquivo em seu ambiente físico, porém acrescentam os aspectos ligados aos riscos

derivados da perda de inteligibilidade da informação eletrônica e à falta de domínio de conteúdos estáveis num ambiente estável.

Ao se tratar dos requisitos de certificação e confiança, o RGL/OCLC afirma que as instituições do patrimônio, isto é, que os arquivos, as bibliotecas e os museus já são instituições reconhecidamente confiáveis pelo seu público-alvo, os quais, ao longo de sua história, têm preservado uma grande quantidade de registros de toda natureza. Porém, ao trabalhar com informações digitais, que são mais instáveis e menos tangíveis que outros tipos de matérias, o textual, por exemplo, quesitos como confiança e credibilidade são mais complexos de ser mensurados e provados.

Na perspectiva de Sayão (2010, p. 82),

Adicionar confiança aos repositórios digitais implica no estabelecimento da presunção de que um dado repositório digital é o que diz ser e que a informação armazenada lá está segura por um longo prazo.

Para a certificação do acesso confiável em um repositório digital, assegurando assim o cumprimento de sua missão e, por conseguinte, sua confiança e credibilidade, foi criado um grupo de trabalho com pessoas de diferentes origens institucionais e geográficas. O grupo tinha também a intenção de apresentar o trabalho ao processo de normalização administrado pela Organização Internacional para Normalização (ISO). A *Trask Force on Digital Certification*, patrocinada pelo *National Archives and Records Administration* (NARA) e a RGL. Esse grupo definiu os elementos certificáveis que um repositório digital deveria possuir, e desenvolveu uma proposta com a determinação de organismos, políticas e procedimentos apropriados para a certificação de um repositório digital (LAVOIE, 2004).

Ainda buscando o aprimoramento na certificação, depois de um convite à comunidade de interesse, foi publicado em 2007 o *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC).

Com base na TRAC, foi publicada no ano de 2012 a ISO 16363:2012, uma norma que se propõe fornecer ferramentas para avaliar a confiabilidade de repositórios digitais e pode ser utilizada como base para certificação de tais repositórios.

Thomaz (2007, p. 84) discorre sobre certificação e afirma:

A certificação tornou-se um componente-chave para repositórios digitais contemporâneos. [...] usamos a certificação como nosso mecanismo e instrumento de medida. Isso possibilita que os repositórios se recuperem e caminhem, obtendo negócios, construam e comprovem as boas práticas.

A autora expõe que as práticas de certificação, no passado, eram feitas de modo informal e implícito, no entanto, com os arquivos digitais, faz-se necessário que tais práticas sejam formais e explícitas (THOMAZ, 2007).

No cenário internacional, tem-se a ISO 16363:2012 para avaliação e certificação dos Repositórios Digitais Confiáveis. No Brasil, a Resolução 39/2014 do CONARQ estabelece Diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

### **4.3 Repositórios arquivísticos digitais confiáveis**

A partir do uso das Tecnologias de Informação e Comunicação (TIC), houve um crescimento exponencial tanto no volume quanto na variedade dos dados registrados, como já demonstramos anteriormente. Frente a essa nova realidade, ocorreu um crescimento exponencial no volume dos documentos arquivísticos (LOPES, 1997; SOUSA, 2007, 2008).

Para Hedstrom (1998, p. 191, tradução nossa), “Na atualidade, nossa capacidade de criar, acumular e armazenar materiais digitais excede em muito a nossa capacidade de preservá-los”. Nesse contexto, temos a urgência de preservação dos documentos digitais que foram e estão sendo produzidos e armazenados, utilizando-se das tecnologias disponíveis e acessíveis.

Acirram-se, então, as discussões sobre as TIC no âmbito da Arquivologia. Bellotto (2004, p. 305), ao descrever sobre as TIC, faz a seguinte afirmação:

A informática está definitivamente incorporada aos arquivos, seja na gestão ou na disseminação da informação de documentos tradicionais, seja na organização e descrição de documentos em suportes isolados

concretos, seja nos documentos virtuais, integrantes de banco de dados e dos sistemas de comunicação.

Face às novas práticas em todos os setores possibilitados pelas TIC, documentos arquivísticos estão sendo produzidos e armazenados unicamente em formato digital (ROCHA et al., 2004; 2005; INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS, 2007). No que tange às vantagens do documento arquivístico digital, devemos considerar a facilidade de acesso, de acessibilidade e a economia de espaço físico. Porém, segundo o Conselho Nacional de Arquivos (2012, p. 1),

Os documentos arquivísticos digitais apresentam dificuldades adicionais para a 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.

Diante do posicionamento do CONARQ, podemos verificar que os documentos arquivísticos digitais requerem tratamento diferenciado, pois possuem características próprias para que seja comprovada sua autenticidade.

O *Digital Preservation in Archives: Overview of Current Research and Practices* apresenta o que segue:

Para os arquivos públicos ou privados, a prestação de serviços “tradicionais”, como o acesso contínuo e a disponibilização de documentos autênticos, tornou-se mais complicada com o uso da tecnologia digital. Por isso, os arquivos necessitam desenvolver novos serviços digitais (NATIONAL ARCHIVES OF SWEDEN, 2005, p. 2, tradução nossa).

No documento, descreve, ainda, que a criação de novos serviços deve considerar os diferentes interesses dos usuários, caracterizando-os em: usuários de arquivos e sociedade em geral, definindo-os como:

Os usuários dos arquivos possuem expectativas de acesso ao documento arquivístico. Logo, esse acesso deve ser eletrônico, rápido e preciso. A sociedade, em geral, precisa que os documentos sejam mantidos para as futuras gerações como prova, visto que os registros

digitais fazem parte da memória da sociedade (NATIONAL ARCHIVES OF SWEDEN, 2005, p. 2, tradução nossa).

Assim, para que sejam tratados em sua especificidade, os documentos arquivísticos digitais deverão estar em um ambiente confiável, onde seja possível monitorar as ações sobre os documentos, bem como abranger seus respectivos componentes digitais.

No ano de 2014, o Conselho Nacional de Arquivos, atento a todas as questões levantadas a respeito da confiabilidade dos Repositórios Digitais, tanto em nível internacional quanto em nacional, publica as diretrizes para a implementação de repositórios digitais confiáveis, na forma de Resolução 39, do CONARQ, que tem a missão de apresentar orientações sobre preservação, gerenciamento e acesso contínuo e em longo prazo aos documentos arquivísticos digitais autênticos.

## **5 DIRETRIZES NACIONAIS PARA REPOSITÓRIOS DIGITAIS CONFIÁVEIS**

Neste capítulo apresenta-se a análise das diretrizes propostas pela CONARQ - Resolução 39 e pela Norma ISO 16363:2012. Com isso, objetiva-se identificar orientações de medição de confiabilidade ou certificação de um Repositório Arquivístico Digital o que é de capital importância quando se dá ênfase ao acesso à informação e aos documentos do domínio arquivístico.

### **5.1 Resolução 39 do CONARQ**

A Resolução 39, datada de 29 de abril de 2014, estabelece diretrizes para a implementação de repositórios confiáveis para a transferência e recolhimento de documentos arquivísticos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR).

O SINAR “[...] tem como finalidade implementar a política nacional de arquivos públicos e privados, visando à gestão, à preservação e ao acesso aos documentos de arquivo” (BRASIL, 2002) e tem como integrantes:

- O Arquivo Nacional;
- Os arquivos do Poder Executivo Federal;
- Os arquivos do Poder Legislativo Federal;
- Os arquivos do Poder Judiciário Federal;
- Os arquivos estaduais dos Poderes Executivo, Legislativo e Judiciário;
- Os arquivos municipais dos Poderes Executivo, Legislativo e Judiciário.

Pessoas físicas e jurídicas de direito privado, detentoras de arquivo, mediante acordo ou ajuste com um órgão central, podem ser integrantes do SINAR.

As Diretrizes para Implementação de Repositórios Digitais Confiáveis de Documentos Arquivísticos foram elaboradas por uma equipe constituída por dezessete membros da Câmara Técnica de Documentos Eletrônicos do CONARQ (CTDE), pertencentes a diferentes instituições arquivísticas de diferentes localidades do Brasil.

As diretrizes são baseadas no modelo *Open Archival Information System* (1999), no relatório da *Research Library Group* (RLG) e da *Online Computer Library Center* (OCLC) - *Trusted Digital Repositories Attributes and Responsibilities* (2002) e no documento *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC) (2007) apresentados anteriormente.

Na apresentação das diretrizes, ao tratar do aumento da produção dos documentos arquivísticos em formatos digitais, há a seguinte consideração:

A produção crescente de documentos arquivísticos em formato digital desafia as organizações produtoras e as instituições de preservação na busca de soluções para a preservação e o acesso de longo prazo. Os documentos digitais sofrem diversas ameaças decorrentes da fragilidade inerente aos objetos digitais, da facilidade de adulteração e da rápida obsolescência tecnológica (CONSELHO NACIONAL DE ARQUIVOS, 2014b, p. 4).

Nota-se que, assim como no cenário mundial, essa é uma preocupação emergente no Brasil onde se buscam meios para a salvaguarda dos documentos arquivísticos em formato digital. A resolução explicita tal preocupação na descrição do objetivo de:

Indicar parâmetros para repositórios arquivísticos digitais confiáveis de forma a garantir a integridade, a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos de tempo ou até mesmo permanente. (CONSELHO NACIONAL DE ARQUIVOS, 2014b, p. 5).

No dia 04 de setembro de 2015, a Câmara Técnica de Documentos Eletrônicos, por meio da Resolução nº 43, altera a redação da Resolução nº 39, de 29 de abril de 2014, ajustando o texto: onde se lia “Diretrizes para Implementação de Repositórios Digitais Confiáveis de Documentos Arquivísticos”, lê-se “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq”.

Mudança essa bastante pertinente, visto que repositórios arquivísticos se diferenciam dos demais repositórios pela especificidade de seus materiais e pelo cumprimento de requisitos que obrigatoriamente assegurem o armazenamento e o acesso em longo ou permanente prazo.

Vale destacar que a modificação de 2014, na redação das diretrizes, ocorreu somente na nomenclatura. A redação foi modificada para Repositórios Arquivísticos Digitais Confiáveis e acrescentada a sigla RDC-Arq.

Os Repositórios Arquivísticos Digitais são compostos essencialmente de fontes primárias de informações (cartas, processos, registros) produzidas diretamente por um indivíduo ou organização, ao invés de fontes secundárias como as encontradas em bibliotecas (livro, periódicos etc.). Os arquivos custodiam registros únicos que não podem ser encontrados ou consultados em outro local a não ser nos arquivos (RAMALHO, 2007).

As diretrizes são divididas em três partes: Apresentação; Principais Requisitos e Padrões e Normas de Referência.

Na apresentação, tem-se a introdução do documento com algumas definições de termos do universo arquivístico que proporcionarão ao arquivista clareza no entendimento das diretrizes.

A segunda parte das diretrizes é composta pela apresentação dos principais requisitos para a criação de um Repositório Arquivístico Digital Confiável RDC-Arq. Segundo as orientações brasileiras, estão assim estabelecidas:

A instituição responsável pelo RDC-Arq deve:

- Ter responsabilidade pelo repositório, no que diz respeito à sua implantação e manutenção, bem como sua criação deverá ser partilhada por profissionais de arquivo e de Tecnologia da Informação para que possam ser cumpridos os requisitos tecnológicos e o tratamento arquivístico.
- Fazer o tratamento arquivístico pautado nas normas arquivísticas.

O RDC-Arq deve:

- Ser independente.
- Possibilitar a interoperabilidade com outros repositórios e sistemas informatizados que tratem de documentos arquivísticos.

Para que sejam cumpridos os requisitos, a fim de que o repositório digital seja considerado confiável, o CONARQ pautou-se na ISO 16.363:2012, conforme apontamentos na resolução. Tal norma será apresentada no tópico 5.2 deste capítulo.

Os requisitos apresentados nas diretrizes da resolução 39 do CONARQ estão organizados em três conjuntos: infraestrutura organizacional; gerenciamento do documento digital e tecnologia, estrutura técnica e segurança.

O primeiro conjunto de requisitos, Infraestrutura Organizacional, diz respeito ao ambiente em que o RDC-Arq será criado, e aos requisitos de: governança e viabilidade organizacional; estrutura organizacional e de pessoal; transparência de procedimento e arcabouço político; sustentabilidade financeira e Contratos, licenças e passivos.

O segundo conjunto, Gerenciamento do Documento Digital, deverá estar obrigatoriamente de acordo com o modelo OAIS, que estabelece a formação de pacotes de informação que envolve documentos digitais e seus metadados. Os pacotes de informação são: pacote de informação para submissão (*submission information package* – SIP); pacote de informação para arquivamento (*archival information package* – AIP) e pacote de informação para disseminação (*dissemination information package* – DIP).

O terceiro conjunto de requisitos, Tecnologia, Infraestrutura Técnica e Segurança, refere-se às melhores práticas pertinentes às áreas de gestão de dados e segurança, que devem ser atendidas por um repositório digital confiável. Os requisitos desse conjunto não estabelecem *hardware* e/ou *software*. Dentre as práticas apontadas estão: Infraestrutura do Sistema; Tecnologias Apropriadas e Segurança.

A terceira parte das diretrizes é composta das recomendações sobre os Padrões e Normas de Referências, isto é, são apresentados os documentos de referência que deverão ser utilizados para a construção dos RDC-Arq. Tais documentos irão definir os modelos ou ainda orientar a certificação de repositórios confiáveis; definirão os metadados que poderão ser utilizados em conformidade com o propósito do repositório e a codificação em *eXtensible Markup Language* (XML).

Nessa parte das diretrizes, os Padrões e Normas de Referência definidos são:

1. Modelo de referência OAIS.
2. Relatório da *Research Library Group* (RLG) e da *Online Computer Library Center* (OCLC) – Repositórios digitais confiáveis: atributos e responsabilidades.
3. Certificação e auditoria de repositórios confiáveis: critérios e *checklist* (TRAC).
4. Requisitos técnicos para entidades de auditoria e certificação de organizações candidatas a serem repositórios digitais confiáveis.
5. Metadados de preservação (*Preservation Metadata: Implementation Strategies - PREMIS*).
6. Norma Geral Internacional de Descrição Arquivística - ISAD(G).
7. Norma Brasileira de Descrição Arquivística (NOBRADE).
8. Metadados do e-ARQ Brasil.
9. Protocolo para coleta de metadados (*Open Archives Initiative - Protocol for Metadata Harvesting - OAI-PMH*).
10. Padrão de codificação e transmissão de metadados (*Metadata Encoding & Transmission Standard - METS*).
11. Descrição arquivística codificada (*Encoded Archival Description - EAD*).

Algumas dessas indicações são ferramentas que integram os instrumentos de trabalho do arquivista, sendo elas: Norma Geral Internacional de Descrição Arquivística – ISAD(G), Norma Brasileira de Descrição Arquivística (NOBRADE), Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias (ISAAR-CPF), Norma Internacional para Descrição de Funções (ISDF), Norma Internacional para Descrição de instituições com Acervo Arquivístico (ISDIAH), Dicionário Brasileiro de Terminologia Arquivística (DBATE), princípios de acesso aos arquivos, entre outras que demandam um trabalho dedicado de capacitação voltado para o entendimento das TIC no escopo do trabalho arquivístico para a construção fundamental de RDC-Arq.

Nesse momento, cabe um alerta sobre alguns apontamentos rapidamente citados na Resolução do CONARQ para a instalação dos Repositórios Arquivísticos Digitais Confiáveis RDC-Arq. Conforme relatam as normas nacional e internacional vigente, as interfaces dos repositórios podem potencializar e aumentar sua capacidade

de satisfazer as necessidades informacionais de seus usuários ao conectar seus serviços e coleções à comunidade. Nessa premissa, procurou-se, no texto da resolução, informações referentes aos termos: Acessibilidade; Comunidade Alvo; Curadoria Digital; Interface; Preservação; *Software*; Usabilidade e Usuário dentro da perspectiva de atendimento ao usuário. Esses termos também serão buscados no interior da norma ISO para a certificação de confiabilidade em repositório, sobre a qual passaremos a discorrer no próximo item. O resultado sobre a busca do termo será apresentado na seção 5.3.

## **5.2 *Space data and information transfer systems -- Audit and certification of trustworthy digital - ISO 16363:2012***

Segundo Houghton (2015), em dias atuais quase todos os documentos que criamos, é um objeto digital. Provavelmente, nem tudo deve ser mantido para sempre, porém, materiais de valor acadêmico ou histórico devem ser mantidos para as futuras gerações, dessa feita, preservar objetos digitais é mais desafiador que manter itens de papel.

Com a rápida obsolescência de *hardware* e a substituição de *software* presenciamos a deterioração das mídias de armazenamento o que tornou urgente a criação de ferramentas e padrões para preservação dos meios digitais.

Nesse contexto, os repositórios digitais nos últimos anos têm tido consideráveis avanços no que tange à criação de padrões e ferramentas, visando à preservação de objetos digitais, tendo em vista o crescente interesse na auditoria e na certificação dos repositórios digitais diante da necessidade de os usuários confiarem em sua segurança. Assim, o padrão *Trustworthy Repositories Audit and Certification: Criteria and Checklist* (TRAC) foi o mais aceito para que se avaliassem a confiabilidade dos repositórios digitais.

Originalmente a TRAC foi desenvolvida pelo *Research Libraries Group* e *National Archives and Records Administration* e transformou-se em *Certification of Trustworthy Digital Repositories: Recommended practice CCSDS 652.0-M-1 (Consultative Committee for Space Data Systems)*, tendo se formalizado na *International Organization for Standardization* (ISO) 16363 em 2012. Por essa razão, a ISO se apresenta com a

mesma configuração do *Audit and Certification of trustworthy Digital Repositories - Magenta Book*, (como CCSDS 652, 0-M-1, setembro de 2011).

O escopo do referencial normativo prescrito pela ISO 16363:2012 é ser uma ferramenta que viabiliza a auditoria, a avaliação e a certificação dos repositórios digitais. A norma aponta, ainda, a documentação básica necessária, para que seja possível o cumprimento do processo de auditoria, bem como os requisitos para os auditores, balizando dessa maneira, o processo de certificação.

A ISO também estabelece metodologias adequadas que irão determinar a consistência e a sustentabilidade nos repositórios digitais. É recomendado o *Checklist* para que seja possível fazer a auditoria e a certificação, organiza as métricas ou critérios da infraestrutura organizacional.

Geralmente os critérios são bem abrangentes, embora alguns tenham explicações insuficientes ou ausentes podem gerar diferentes interpretações. É importante ressaltar que nem todos os critérios serão aplicáveis a todos os repositórios.

A norma contém cento e cinco critérios que abrangem três áreas: Infraestrutura organizacional; Gerenciamento de objetos digitais e Infraestrutura e gestão de riscos de segurança.

O *Checklist* inclui elementos como: governança; estrutura organizacional; mandato ou finalidades; âmbito; funções e responsabilidades; enquadramento da política; sistema de financiamento; questões financeiras incluindo ativos; contratos licenças e passivos e transparência (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2011).

As métricas normativas que estão relacionadas com a Infraestrutura Organizacional fazem a descrição da arquitetura técnica, processos e recursos necessários para que um repositório digital seja sustentável. Os critérios são divididos em (CONSULTATIVE..., 2011, tradução nossa):

- Governança e viabilidade organizacional;
- Estrutura organizacional e de pessoal;
- Responsabilidade processual e preservações no âmbito da política;
- Sustentabilidade financeira;

- Contratos licenças e ativos.

As normas relacionadas à Gestão de objetos digitais avaliam a responsabilidade de gestão dos objetos digitais de um repositório, incluindo os aspectos organizacionais e as técnicas relacionadas com tal responsabilidade como: funções do repositório, processos e procedimentos para a ingestão, gerenciamento, preservação e acesso aos objetos digitais.

Para que essa função possa ser cumprida, são apresentados seis elementos baseados na funcionalidade dos arquivos o que permitirá o agrupamento de acordo com as entidades funcionais do modelo de referência OAIS.

- Ingestão: aquisição de conteúdo;
- Ingerir: criação do *AIP*;
- Plano de preservação;
- Preservação *AIP*;
- Gestão da informação;
- Gerenciamento de acesso.

À gestão de objetos digitais, caberá analisar o processo de recepção e gestão de objetos digitais do repositório, ou seja, a forma como esse incorpora a informação digital assim como a criação da gestão dos Pacotes de Informação de Arquivo (*AIP*). Também essa gestão abarcará o planejamento da preservação e a maneira como os *AIP* são preservados, observando ainda os componentes de gestão de informação do serviço e a gestão de acessos.

A seção denominada Gestão de Risco da Infraestrutura e de Segurança está ligada às infraestruturas e às tecnologias no âmbito da gestão de risco da infraestrutura técnica, tratando a Segurança também na perspectiva da Gestão de Risco, constatação da utilidade da cultura de avaliação de risco e garantindo o funcionamento e o serviço de confiança (CONSULTATIVE..., 2011, tradução nossa).

- Gestão de risco da infraestrutura técnica;

- Gestão de riscos de segurança.

Toda preocupação com a auditoria para a certificação de confiabilidade de um Repositório Digital se justifica, quando percebemos a importância dessas ações em nossos dias em que o documento digital é produzido em grande escala. Assim as interfaces dos repositórios possibilitam não somente o acesso rápido e confiável, como também por meio de boas práticas, conectam seus serviços e coleções às comunidades usuárias.

Conforme apontado na seção anterior, os termos: *Accessibility*; *Designated Community*; *Digital Curation*; *Interface*; *Preservation/Preserved*; *Software*; *Usability* e *User(s)*, também serão buscados no interior da norma ISO para a certificação de confiabilidade em repositório, sobre a qual passaremos a discorrer no próximo item. O resultado sobre a busca do termo será apresentado na seção 5.3.

### **5.3 Categorização do termo acesso na Norma ISO 16363 e na Resolução 39 do CONARQ**

Sendo função básica dos arquivos disponibilizarem as informações que estão sob sua custódia no acervo documental para o acesso, Silva (2002, p. 40) afirma que o arquivo é “[...] um sistema bidimensional e nunca unidimensional. Nele se projeta com maior ou menor expressão a entidade produtora/receptora de informação [...]” o que confirma que esse sistema primordialmente necessita disponibilizar os documentos e facilitar o acesso a eles. Nesse contexto, ao explorar os documentos utilizados neste estudo, observou-se que a expressão “acesso” era recorrente em diversos pontos do documento.

No intuito de identificar cada parte do documento que continha a expressão acesso/Access, optou-se por disponibilizá-lo nas categorias:

- Introdução - composta dos itens: sumário; apresentação; introdução; objetivo do documento e definições.
- Principais Requisitos para Repositórios Digitais Confiáveis – composta dos itens: Visão geral dos critérios de auditoria e certificação: repositório

digital confiável; Principais requisitos de um RDC-Arq; Princípios de preservação digital; independência dos repositórios.

- Infraestrutura organizacional – composta dos itens: Governança e viabilidade organizacional; transparência de procedimentos e arcabouço político/Regulamentação de responsabilidades e políticas de preservação; sustentabilidade financeira; contratos, licenças e passivos.
- Gerenciamento do documento digital – composta dos itens: Ingestão: aquisição do conteúdo; Admissão/Criação do AIP/Admissão: criação do pacote de arquivamento; gerenciamento da informação; gestão do acesso/gerenciamento do acesso.
- Infraestrutura e segurança na gestão dos riscos - composta dos itens: técnicas de gestão de riscos e infraestrutura; gestão de riscos de segurança.
- Referencial teórico metodológico.

Nas categorias, procurou-se explorar o documento no sentido de identificar a expressão acesso. Para uma melhor visualização das categorias e do percentual da expressão acesso nos textos da norma ISO 16363:12 e da Resolução 39 do CONARQ, apresentamos a seguir a Figura 9.

**Figura 9** - Categorização do termo Acesso: ISO 16363:2012 e Resolução 39 do CONARQ



**Fonte:** Elaborado pela autora

Seguindo a ordem do texto da norma e da resolução 39, a primeira categoria para o termo acesso foi: Introdução. Nessa categoria, o termo é citado 75 vezes na Norma ISO 16363:2012 e 37 vezes na Recomendação 39 do CONARQ, assim a incidência de citação do termo em tal categoria, representa 8% do total das citações na norma ISO e 29,72% na Introdução da Resolução 39, do total de citações do referido termo. Como a Resolução é voltada para o domínio arquivístico, faz-se necessária a disponibilização de informações e documentos para a comunidade. Podemos constatar a preocupação no que tange ao acesso às informações arquivísticas.

Na categoria Principais Requisitos para um Repositório Digital Confiável, a norma ISO cita o termo acesso apenas uma vez, no item Um repositório digital confiável o que representa 1,34% do total, já na Resolução o termo é citado sete vezes da seguinte maneira: cinco referências ao termo se dão no contexto dos principais requisitos de um RDC-Arq, uma citação no item Princípios de preservação digital e duas

citações no item referente à Independência dos repositórios, perfazendo o total de 18,92% de citações nessa categoria.

A categoria Infraestrutura Organizacional é parte do rol de Requisitos propostos tanto pela norma ISO, quanto pela Resolução do CONARQ em que são apontados os requisitos de um repositório deverá cumprir para que seja considerado confiável. Nessa categoria, há a menção do termo acesso 23 vezes na ISO, com o percentual de 30,66%, distribuídos da seguinte maneira: 5 citações no contexto da Governança e viabilidade organizacional; 10 citações no que diz respeito à Responsabilidade processual e política de preservação; uma menção do termo ao discorrer sobre Sustentabilidade Financeira e sete inclusões do termo ao se tratar de Contratos, licenças e passivo. A Resolução faz referência ao termo 2 vezes , uma ao tratar da Governança e viabilidade organizacional e outra no tocante à Transparência de procedimentos e arcabouço político. Essa categoria representa na Resolução 5,41% de citações do termo.

A categoria Gerenciamento do objeto também é uma seção que traz as recomendações para a certificação de um repositório digital. Essa categoria tem como um de seus itens - Gestão do acesso, na norma ISO e Gerenciamento de acesso na Resolução 39. Devido à especificidade desse item, nele o termo acesso é mais encontrado, sendo que, na ISO no item Ingestão e aquisição do conteúdo, o termo é citado uma vez, no item Admissão: criação do AIP o termo é sete vezes citado e no item Gestão de acesso o termo é 21 vezes citado, perfazendo o total de 29 citações com o percentual de 38,66% do total. Na Resolução 39, o termo é citado 14 vezes com um percentual de citação de 37,84%, sendo que sua maior incidência está no item Gerenciamento de acesso, 11 vezes, Admissão: criação do pacote de arquivamento, uma vez e no item Gerenciamento da informação é citado uma vez. Podemos verificar que esse item abarca o maior percentual das citações do termo e sua importância, visto que há um item específico nas duas recomendações no que se refere ao Acesso.

A terceira e última categoria que faz parte do rol das recomendações necessárias para que um repositório digital possa ser considerado confiável, diz respeito à Infraestrutura e segurança na gestão de riscos. Nessa categoria, não encontramos nenhuma citação do termo em questão na Resolução 39, porém, na ISO,

essa categoria é responsável por um percentual de 20% do total de citações, sendo que onze citações se fazem presentes no item Técnicas de gestão de riscos de infraestrutura e 4 são pertinentes ao item Gestão de riscos de segurança.

Na categoria Referencial teórico e metodológico, a ISO contém uma citação do termo pela *British Standard Institution*, num percentual de 1,34% de citação, já a Resolução 39, a qual foi fundamentada na norma ISO 16363, tem 3 citações do termo. Assim essa categoria tem o percentual de 8,11% das citações no todo.

Diante do exposto, podemos perceber a preocupação das duas instituições quanto ao acesso, visto que é uma ação importante para o êxito e cumprimento dos objetivos de um repositório digital, quando ele disponibiliza suas informações e documentos a sua comunidade alvo com o intuito de satisfazer suas necessidades informacionais, tendo como foco a informação confiável.

Após a categorização do termo acesso, procurou-se identificar ações e elementos que viabilizem o acesso de toda comunidade que necessite de uma informação arquivística, sejam usuários, especialistas ou não. Por isso, buscamos na norma ISO 16363:2012 e na Recomendação 39 do CONARQ, os termos: *Acessibilidade/Accessibility*; *Comunidade Alvo/Designated Community*; *Curadoria Digital/Digital Curation*; *Interface*; *Preservação/Preservation*; *Preservada/ Preserved*; *Usabilidade/Usability*; *Usuário(s)/User(s)* que se encontram nas seções um, dois e três que é o local onde os documentos elencam os requisitos necessários que um repositório Digital deverá contemplar para ser considerado confiável e, por conseguinte, obter a certificação. Os termos foram escolhidos por serem partes importantes na perspectiva de acesso às informações e aos documentos arquivísticos. Para tanto, elegemos as seguintes categorias dentro dos Requisitos para um repositório digital confiável:

- **Infraestrutura organizacional** – composta dos itens: Governança e viabilidade organizacional; Estrutura organizacional de pessoal; Regulamentação de responsabilidades e política de preservação; Transparência de procedimentos e arcabouço político e Contratos, licenças e passivos.

- **Gerenciamento do documento digital** – composta dos itens: Gerenciamento de informação; Admissão: criação do AIP/ Admissão: criação do pacote de arquivamento; Gestão da informação/Gerenciamento da informação; Ingestão: aquisição do conteúdo; Admissão/Criação do AIP/Admissão: criação do pacote de arquivamento; Preservação/Planejamento da preservação; Preservação do AIP/ Armazenamento e preservação/manutenção do AIP gerenciamento da informação; gestão do acesso/gerenciamento do acesso.
- **Infraestrutura e segurança na gestão dos riscos** - composta dos itens: técnicas de gestão de riscos e infraestrutura e segurança.

Para essa busca, foram desconsiderados da norma ISO: os textos de apoio, os exemplos de reunião de requisitos e as discussões (que se encontram junto a cada subitem). Na resolução 39, foram desconsiderados os parágrafos explicativos (localizados abaixo de alguns itens e subitens). O resultado dessa busca está demonstrado no Quadro 3, a seguir, com a disponibilização dos termos em ordem alfabética:

**Quadro 3** - Categorização de termos em relação aos Requisitos para RDC-Arq: ISO 16363:2012 e Resolução 39 do CONARQ

Termo	Categoria	Requisito	ISO	Res. 39
Acessibilidade/ Accessibility			-	-
Comunidade Alvo/ Designated Community	Infraestrutura organizacional:	Regulamentação de responsabilidades e política de preservação/Transparência de procedimentos e arcabouço político	2	2
	Gerenciamento do documento digital	Gerenciamento de informação	-	1
		Admissão: criação do AIP/ Admissão: criação do pacote de arquivamento	3	2
		Gestão da informação/ Gerenciamento da informação	-	1
	Infraestrutura e segurança na gestão dos riscos	Técnicas de gestão de riscos e infraestrutura/ Infraestrutura de Sistema	1	1

Termo	Categoria	Requisito	ISO	Res. 39
Curadoria Digital/ Digital Curation			-	-
Interface			-	-
Preservação – Preservada/ Preservation - Preserved	Infraestrutura organizacional:	Governança e viabilidade organizacional	3	1
		Estrutura organizacional de pessoal	1	
		Regulamentações de responsabilidades e políticas de preservação	5	-
		Transparência de procedimentos e arcabouço político	-	3
		Contratos, licenças e passivos	3	-
	Gerenciamento do objeto Digital	Ingestão: aquisição do conteúdo	4	2
		Admissão: Criação do AIP/Admissão: criação do pacote de arquivamento	4	6
		Preservação/ Planejamento da preservação	5	4
		Preservação do AIP/ Armazenamento e preservação/manutenção do AIP	3	6
		Infraestrutura e segurança na gestão dos riscos	Técnicas de gestão de riscos e infraestrutura	2
Segurança	1		0	
Software	Infraestrutura organizacional:	Regulamentações de responsabilidades e políticas de preservação	1	1
	Infraestrutura e segurança na gestão dos riscos	Técnicas de gestão de riscos de infraestrutura	6	6
Usabilidade/ Usability			-	-
Usuários/User	Infraestrutura organizacional:	Transparência de procedimentos e arcabouço político	-	1
	Gerenciamento do objeto Digital	Gerenciamento da informação	-	1
		Gestão de acesso	-	9
	Infraestrutura e segurança na gestão dos riscos	Infraestrutura de sistema	1	1

**Fonte:** Elaborado pela autora

Conforme demonstrado no quadro, o termo *acessibilidade/accessibility* não se encontra nem na norma ISO, nem nas recomendações da Resolução 39 do CONARQ. Para implementação de um RDC-Arq, o termo foi escolhido porque entendemos que, ao promover a acessibilidade a partir de diferentes sistemas e equipamentos, é viabilizado o acesso a toda comunidade.

Vale ressaltar que, apesar de o termo não ser citado, percebemos que há preocupação com o ato de tornar acessível o conteúdo quando, no item Gerenciamento do Objeto Digital, a norma ISO faz a seguinte ressalva: “Repositório deve ter um processo documentado para testar compreensibilidade para as suas comunidades designadas das Informações do conteúdo das AIP na sua criação” (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012), já a Resolução 39 é mais específica e pontua que o repositório deve: “Ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais)” (CONSELHO NACIONAL DE ARQUIVOS, 2014).

O termo *Comunidade Alvo/Designated Community*, que diz respeito ao público a quem o repositório deve atender, é contemplado nas três seções de recomendações, isto é, seis (6) vezes na norma ISO e sete (7) vezes na Resolução.

Ao buscarmos o termo Curadoria Digital, constatamos que ele somente aparece uma vez na Norma ISO como nota de rodapé e não foi indicado na Resolução 39. Sua busca se deu por ser um conceito relativamente novo que abarca a preservação digital, a criação de novos modelos de custódia de dados e informações digitais, de gestão de conteúdo e do uso e reuso das informações. Na perspectiva de acesso, Márdero Arellano (2004, p. 15), ao discorrer sobre a preservação dos documentos, especialmente os digitais, pontua: “A aplicação de estratégias de preservação para documentos digitais é uma prioridade, pois sem elas não existiria nenhuma garantia de acesso, confiabilidade e integridade dos documentos a longo prazo”.

Ainda que o termo Curadoria não seja citado, é possível verificar termos e ações que fazem parte do processo da Curadoria Digital como: objetos digitais; representação da informação; ação de preservação; acesso; recebimento entre outros.

Pesquisadores, estudiosos, pessoal do administrativo e o cidadão comum conectam-se aos arquivos através de interfaces, assim, como se configura como a porta de acesso ao repositório. Buscamos nos documentos o termo Interface e constatamos que ele não é mencionado nem na Norma ISO nem na resolução 39.

Os termos *Preservação/Preservation – Preservada/Preserved* são apontados 31 vezes na Norma e 22 vezes na Resolução, assim eles se configuram como os termos

mais utilizados pelos documentos dentre os que estamos buscando. Na categoria Infraestrutura organizacional, o termo é contemplado com 38,71% na ISO e 18,19% na Resolução 39. A categoria Gerenciamento do objeto digital contempla o termo em 51,61% na norma ISO e em 81,82% na Resolução 39. Na categoria Infraestrutura e segurança na gestão dos riscos, o termo é contemplado em 9,68% na Norma ISO, mas na Resolução 39, não se encontra presente. A quantidade de inserções do termo preservação denota a preocupação com a preservação dos documentos, dados e informações custodiadas pelos repositórios digitais, porém a preservação poderia ser parte no processo de Curadoria Digital.

O termo *Software* é mencionado sete (7) vezes nos dois documentos, nas mesmas categorias e itens, sendo que 14,29% se encontram no item Infraestrutura organizacional, requisito Regulamentação de responsabilidades e políticas de preservação e 87,29% diz respeito ao item Infraestrutura e segurança na gestão dos riscos no requisito Técnicas de gestão de riscos de infraestrutura. O RDC-Arq fará a escolha do *software* que melhor atenda a suas necessidades.

O termo Usabilidade/*Usability* não é citado nem na Norma ISO, nem na Resolução 39.

O termo Usuário(s)/*User(s)* apesar de estar somente em um (1) subitem na norma ISO, constatamos que ele é recorrente no texto de apoio, nos exemplos da reunião dos requisitos e nas discussões que se encontram junto a cada subitem o que demonstra que, apesar de não citado, há uma preocupação com o usuário na Norma ISO.

Na Recomendação 39, o termo usuário é indicado doze (12) vezes, sendo que 83,34% se referem à categoria Gerenciamento do objeto digital no item Gestão de acessos aparece em 75% do total de citações, e 8,33% estão no item Gerenciamento da Informação. A categoria Infraestrutura organizacional Infraestrutura organizacional o item transparência de procedimento e arcabouço político é responsável por 8,3% com o mesmo percentual da categoria Infraestrutura e segurança na gestão dos riscos, requisito Infraestrutura do sistema.

Com a categorização dos temas, verificou-se que se faz necessária a descrição de ações de maneira mais pontual no que tange à legislação arquivística e de acesso à

informação, ao uso de Ciclo de Vida dos Documentos proposto pela Curadoria Digital, e às ações que efetivem a acessibilidade e a usabilidade, para que as necessidades informacionais de um maior número de cidadãos sejam atendidas.

#### **5.4 Requisitos da ISO 16363:2012 e da Resolução 39 do CONARQ**

Nesse momento, a análise dos requisitos indicados pela Resolução 39 e pela Norma ISO 16363:2012 é de importância capital, pois, a partir dela, será possível identificar os elementos fundamentais para a construção de repositórios arquivísticos digitais que garantam as características necessárias para o tratamento arquivístico dos documentos e que sejam repositórios confiáveis, como especifica a resolução e como certifica a norma.

A ISO 16363:2012 é a norma que permite a certificação de confiança em nível internacional para repositórios digitais de organizações públicas ou privadas. A partir da criação dessa norma, tornou-se possível mensurar os objetivos do repositório e assim verificar se ele é confiável, independente do tipo de material digital.

Já a Resolução 39 do CONARQ, faz a recomendação aos órgãos e integrantes do SINAR para que sejam adotadas Diretrizes para a implementação de repositórios digitais confiáveis de documentos arquivísticos no Brasil. Vale ressaltar que os requisitos da Resolução 39 tiveram como base a norma ISO 16363:2012 (CONSELHO NACIONAL DE ARQUIVOS, 2015, p. 12).

Diante desse cenário, buscamos os conceitos para os termos norma e diretrizes e encontramos as seguintes definições:

Segundo o Dicionário de Filosofia, Norma é:

Regra ou critério de juízo. A Norma também pode ser construída por um caso concreto, um modelo e um exemplo; mas o caso concreto, o modelo ou o exemplo só valem como Normas se puderem ser utilizados como critérios de juízo dos outros casos, ou das coisas as quais o exemplo ou o modelo referem (ABBAGNANO, 1998, p. 716).

Já o Vocabulário Jurídico, mais enfático, traz a seguinte definição:

Derivado do latim *norma*, oriundo do grego *gnorimos* (esquadria, esquadro), dentro do seu sentido literal, é tomado na linguagem jurídica como regra, modelo, paradigma, forma ou tudo que se estabelece em lei ou regulamento para servir de pauta ou padrão (SILVA, 1967, p. 1067).

O Novo Dicionário Aurélio de Língua Portuguesa define norma como: “Aquilo que se estabelece como base ou medida para a realização ou a avaliação de alguma coisa.” (FERREIRA, 2009, p. 1408).

Nesse contexto, podemos concluir que a Norma ISO 16363:2012 fixa padrões que garantem a confiabilidade dos Repositórios Digitais Confiáveis.

Para o termo *diretriz*, o Novo Dicionário Aurélio da Língua Portuguesa traz como definição: “Conjunto de instrução ou indicações para se tratar ou levar a termo um plano, uma ação” (FERREIRA, 2004, p. 1050).

O dicionário Jurídico define *diretriz* como: “[...] esboço em linhas gerais de um plano, projeto etc. diretiva, norma de procedimento, conduta etc.; diretiva [...]” (MALTA; LEFÈVRE, 1987, p. 611).

*Diretriz* no dicionário Houaiss da língua portuguesa (HOUAISS, 2004, p. 796) é definida como: “Que dirige, orientação, rumo”.

Assim, as diretrizes propostas pelo CONARQ orientam os repositórios arquivísticos digitais, para que possam ser reconhecidos como confiáveis.

Podemos verificar, a partir das definições dos termos, que a ISO diz respeito aos requisitos que o repositório deve cumprir para obtenção da certificação, visto que são utilizadas como critérios e juízos, enquanto que a Resolução recomenda elementos que, se o repositório atender, esse estará em conformidade com as premissas, para ser considerado um repositório arquivístico digital confiável.

Tendo como referência essas indicações internacional e nacional, a seguir demonstraremos no Quadro 4, os requisitos da Norma ISO 16.363:2012 que são contemplados nas recomendações da Resolução 39, no que diz respeito à Organização e Infraestrutura, dispostos na terceira seção (ISO) e II.2.1 (Resolução).

**Quadro 4** - Análise demonstrativa, itens compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 3 - Organização e Infraestrutura

ISO 16363:2012	RESOLUÇÃO 39
<b>3 Organização e Infraestrutura</b>	<b>II.2.1 Infraestrutura organizacional</b>
<b>3.1 Governança e viabilidade organizacional</b>	<b>a. Governança e viabilidade organizacional</b>
3.1.1 O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, a gestão e acesso à informação digital por longo prazo.	O repositório tem como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. Essa missão é claramente identificada por todos os interessados no repositório e envolve: mandato legal, contexto organizacional e requisitos regulatórios.
3.1.2.1 O repositório deve ter um plano adequado de sucessão, planos de contingência e/ou acordos judiciais, no caso de o repositório parar sua atividade ou a instituição governamental, ou financiamento mudar substancialmente o seu âmbito.	O repositório tem um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos, para garantir a continuidade do serviço, no caso de o repositório parar de operar ou de a instituição responsável e/ou financiadora mudar seu escopo.
<b>3.2 Estrutura organizacional e de pessoal</b>	<b>b. Estrutura organizacional e de pessoal</b>
3.2.1 O repositório deve identificar e estabelecer as funções que necessita realizar e deverá nomear pessoas com qualificações e experiência adequadas para cumprir esses deveres.	O repositório tem uma equipe dotada de qualificação e formação necessárias, e em número suficiente, para garantir todos os serviços e funcionalidades pertinentes ao repositório. Além disso, deve manter um programa de desenvolvimento profissional contínuo.
3.2.1.2 O repositório deve ter um número adequado de pessoas em sua equipe, para apoiar todas as funções e serviços.	
3.2.1.3 O repositório deve colocar em prática um programa de desenvolvimento profissional ativo que forneça a qualificação da equipe competências e oportunidades de desenvolvimento.	
<b>3.3 Regulamentações de responsabilidades e políticas de preservação</b>	<b>c. Transparência de procedimentos e arcabouço político</b>
3.3.1 O repositório deve ter definido a sua base de conhecimento, sua comunidade de associado(s) e deve ter essas definições acessíveis.	Definir a comunidade alvo e sua base de conhecimento.
3.3.2 O repositório deve ter políticas de preservação, para garantir que seu Plano Estratégico de preservação seja cumprido.	Possuir políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados.
3.3.2.1 O repositório deve ter mecanismos de revisão, atualização e desenvolvimento contínuo das suas políticas de preservação, à medida que o repositório cresce, e a tecnologia e a comunidade evoluem.	Possuir políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem.
3.3.3 O repositório deverá ter sua história documentada, bem como as alterações de operações e procedimentos de <i>software</i> e <i>hardware</i> .	Fazer o registro histórico das mudanças de procedimentos, de <i>software</i> e <i>hardware</i> .
<b>3.3 Regulamentações de responsabilidades e políticas de preservação</b>	<b>c. Transparência de procedimentos e arcabouço político:</b>
3.3.5 O repositório deve definir, coletar, rastrear e fornecer medidas integridade da informação.	Estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia.
3.3.6 O repositório deve comprometer com um calendário regular de autoavaliação e de certificação externa.	Estar comprometido em realizar regularmente uma autoavaliação de seu funcionamento e renovar sua certificação;
<b>3.4 Sustentabilidade Financeira</b>	<b>d. Sustentabilidade financeira</b>

ISO 16363:2012	Resolução 39
<b>3 Organização e Infra estrutura</b>	<b>II.2.1 Infraestrutura organizacional</b>
3.4.1 O repositório deve dispor de sistemas de planejamento de negócios de curto e longo prazo, para que seja mantido ao longo do tempo.	Demonstração da capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, sejam por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros.
<b>3.4 Sustentabilidade Financeira</b>	<b>d. Sustentabilidade financeira</b>
3.4.2 O repositório deve ter práticas e procedimentos que sejam transparentes, em conformidade com as normas e práticas contábeis relevantes e auditados por terceiros, de acordo com os requisitos legais territoriais financeiros.	Transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere.
	Revisão e ajustes anuais.
3.4.3 O repositório deve ter um compromisso contínuo, para analisar e informar sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).	Compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos.
<b>3.5 Contratos, licenças e passivos.</b>	<b>e. Contratos, licenças e passivos</b>
3.5.1 O repositório deve ter e manter contratos adequados ou contratos de depósito para materiais digitais que ele gerencia, preserva e/ou para o qual fornece acesso.	Os contratos, licenças e passivos firmados pelo repositório devem ser claros e mensuráveis; delinear papéis, responsabilidades, prazos e condições e ser facilmente acessíveis ou disponíveis aos interessados. Esses contratos, licenças e passivos podem envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. Esses mesmos instrumentos devem especificar todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial no que diz respeito à propriedade intelectual e a restrições de uso.
3.5.1.1 O repositório devem ter contratos ou contratos de depósito que especificam e transferiram todos os direitos de preservação necessários. Esses direitos transferidos serão documentados.	
3.5.1.2 O repositório deve ter especificado todos os aspectos relevantes de aquisição, manutenção, acesso e retirada em acordos escritos com os depositantes e outras partes relevantes.	

Fonte: Elaborado pela autora

Após análise da norma ISO 16363:2012 e da Resolução 39 do CONARQ sobre organização e infraestrutura de repositórios arquivísticos, fazemos os seguintes apontamentos:

Na organização de conjuntos de requisitos, tem-se a apresentação de três seções.

A primeira seção de requisitos é dividida em cinco itens em que tanto a ISO quanto a Resolução 39 utilizam a mesma nomenclatura: Infraestrutura Organizacional.

A primeira subdivisão 3.1: Governança e viabilidade organizacional, a norma ISO o subdivide em cinco subitens, já a Resolução 39 o subdivide em dois subitens, contemplando dois assuntos tratados na ISO.

Na segunda subdivisão 3.2: Estrutura organizacional e de pessoal, a norma ISO estabelece no item 3.2, quatro subitens, a Resolução 39 por sua vez, traz apenas um subitem que contemplam os assuntos tratados nos itens: 3.2.1, 3.2.1.2 e 3.1.1.3.

Na terceira subdivisão 3.3, a ISO utiliza o título Regulamentação de responsabilidades e políticas de preservação, já a Resolução 39 utiliza a nomenclatura Transparência de procedimentos e arcabouço político. A ISO apresenta para esse item sete subitens. A Resolução 39 o divide em nove subitens, sendo que seis tratam de assuntos relacionados aos da ISO.

Na quarta subdivisão 3.4: Sustentabilidade financeira, a ISO, para esse item, apresenta três subitens e a Resolução apresenta quatro subitens em que três discorrem sobre o mesmo assunto da ISO.

Na quinta e última subdivisão 3.5: Contratos, licenças e passivos, a Norma ISO apresenta seis subitens, enquanto a Resolução 39 apresenta apenas um subitem que engloba três subitens da ISO.

Após o apontamento dos itens que são contemplados pela ISO e pela Resolução 39 do Conarq, no Quadro 5 é possível verificar os subitens da sessão 3 que são mencionados nas recomendações ISO 16.363 e não o são na Resolução 39 ou vice-versa.

**Quadro 5** - Análise demonstrativa, itens não compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 3 - Organização e Infraestrutura

<b>ISO 16363:2012</b>	<b>RESOLUÇÃO 39</b>
<b>3 Organização e Infraestrutura</b>	<b>II.2.1 Infraestrutura organizacional</b>
<b>3.1 Governança e viabilidade organizacional</b>	<b>a. Governança e viabilidade organizacional</b>
3.1.2 O repositório deve ter um Plano Estratégico de Preservação que defina a abordagem do repositório no apoio sua missão em longo prazo.	
3.1.2.2 O repositório deve controlar seu ambiente organizacional para determinar quando executar o seu plano de sucessão, planos de contingência e/ou acordos judiciais.	
3.1.3 O repositório deve ter uma política para o recolhimento do documento, especificando o tipo de informação que irá preservar, manter, gerenciar e fornecer acesso.	
<b>3.2 Estrutura organizacional e de pessoal</b>	<b>3.2 Estrutura organizacional e de pessoal</b>

<b>ISO 16363:2012</b>	<b>RESOLUÇÃO 39</b>
<b>3 Organização e Infraestrutura</b>	<b>II.2.1 Infraestrutura organizacional</b>
3.2.1.1 O repositório deve identificar e estabelecer os deveres que precisa executar.	
<b>3.3 Regulamentações de responsabilidades e políticas de preservação</b>	<b>c. Transparência de procedimentos e arcabouço político</b>
	Documentar permissões legais – por meio de acordos de custódia, normas de procedimentos e outros – que isentem de responsabilidade, no caso de alteração passível de ocorrer em estratégias de preservação digital.
	Demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, buscando atendê-las.
<b>3.3 Regulamentações de responsabilidades e políticas de preservação</b>	<b>c. Transparência de procedimentos e arcabouço político</b>
<b>ISO 16363:2012</b>	<b>RESOLUÇÃO 39</b>
3.3.4 O repositório deve comprometer-se a transparência e responsabilidade em todas as ações de apoio à exploração e gestão do repositório que afetam a preservação de conteúdos digitais ao longo do tempo.	
<b>3.4 Sustentabilidade Financeira</b>	<b>d. Sustentabilidade Financeira</b>
	Revisão e ajustes anuais.
<b>3.5 Contratos, licenças e passivos.</b>	<b>e. Contratos, licenças e passivos</b>
3.5.1.3 O repositório deve ter políticas que indiquem quando ele aceita a responsabilidade de preservação de conteúdo de cada conjunto de objetos de dados apresentada.	
3.5.1.4 O repositório deve ter políticas no lugar, para lidar com a responsabilidade e os desafios à propriedade aos direitos.	
3.5.2 O repositório deve rastrear e gerenciar direitos de propriedade intelectual e as restrições à utilização de conteúdo do repositório como exigido pelo contrato de depósito, contrato ou licença.	

**Fonte:** Elaborado pela autora

Após a análise da seção 3, podemos verificar que os itens 3.1.2, 3.1.2.2 e 3.1.3 (Governança e viabilidade organizacional), o subitem 3.2.1.1, (Estrutura organizacional e de pessoal), o item 3.3.4 (Regulamentação de responsabilidades e políticas de preservação) e os itens 3.5.1.3, 3.5.1.4 e 3.5.1.5 (Contratos, licenças e passivos) da norma ISO, fazem referência à política do repositório, assim, não são apontadas na Recomendação, visto que, como a resolução é dirigida para repositórios de instituições arquivísticas, subentende-se que essas já devem possuir políticas próprias.

Os três subitens parte do item Regulamentação de responsabilidades e políticas de preservação, apontados pela Resolução 39, dizem respeito a assuntos específicos para o tratamento de documentos que são custodiados pelos arquivos. Por essa especificidade não são contemplados pela ISO.

A quarta subdivisão 3.4 (Sustentabilidade financeira) que diz respeito à revisão e ajustes anuais de preços é apontado na Resolução 39, podemos inferir que, devido à situação econômica do país, faz-se necessário tal elemento.

Para a visualização da Seção 4 da ISO e II.2.2 da Resolução 39 em que é tratado o Gerenciamento do Objeto digital (ISO) e Gerenciamento do documento digital (Resolução), o Quadro 6 aponta os requisitos recomendados pela ISO 16.363 e pela Resolução 39.

**Quadro 6** - Análise demonstrativa, itens compatíveis pela ISO 16363:2012 e pela Resolução 39  
CONARQ: Seção 4 - Gerenciamento do Objeto Digital

ISO 16363:2012	Resolução 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
<b>4.1 Ingestão: aquisição de conteúdo</b>	<b>a. Admissão: captura de documentos digitais</b>
4.1.2 O repositório deve especificar claramente a informação que precisa ser associada com informação de conteúdo específico no momento do seu depósito.	Especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão.
4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais.	Ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência.
4.1.5 O repositório deve ter um processo de ingerir que verifica cada <i>SIP</i> para integralidade e exatidão.	Ter procedimentos para verificar a integridade do <i>SIP</i> o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana.
4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.	Ter o controle físico (controle completo de <i>bits</i> ) dos documentos transmitidos com cada <i>SIP</i> , a fim de preservá-los.
4.1.7 O repositório deve fornecer ao produtor /depositante respostas adequadas em pontos acordados durante os processos de ingestão.	Fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo processo da admissão.
4.1.8 O repositório deve ter registros das ações e processos de administração que são relevantes para aquisição de conteúdo.	Ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação.

ISO 16363:2012	Resolução 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
<b>4.2 Admissão: Criação da AIP</b>	<b>b. Admissão: criação do pacote de arquivamento</b>
4.2.1 O repositório deve ter para cada <i>AIP</i> ou classe de <i>AIP</i> preservados pelo repositório uma definição associada que é adequada para analisar o <i>AIP</i> e estar apto para as necessidades de preservação em longo prazo.	Descrever minuciosamente as diferentes classes de informação e como os <i>AIPs</i> são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes (por exemplo, a imagem <i>TIFF</i> que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessária à imagem <i>TIFF</i> que é apresentada ao olho humano).
4.2.1.1 O repositório deve ser capaz de identificar qual a definição se aplica ao qual <i>AIP</i> .	Descrever cada classe de informação (texto estruturado, imagem matricial, banco de dados, imagem em movimento e outras) a ser preservada pelo repositório, e como ela está implementada – essa descrição deve apontar as componentes chaves do <i>AIP</i> : o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixibilidade, proveniência e contexto), e ainda como esses componentes se relacionam.
4.2.1.2 O repositório deve ter uma definição de cada <i>AIP</i> que é adequado para a preservação a longo prazo, permitindo a identificação e análise de todos os componentes requeridos dentro que <i>AIP</i> .	
<b>4.2 Admissão: Criação da AIP</b>	<b>b. Admissão: criação do pacote de arquivamento</b>
4.2.2 O repositório deve ter uma descrição de como os <i>AIPs</i> são construídos a partir <i>SIP</i> .	Descrever como os <i>AIPs</i> são construídos a partir dos <i>SIPs</i> , ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do <i>AIP</i> .
4.2.3 O repositório deve documentar a disposição final de todos os <i>SIP</i> .	Ser capaz de demonstrar se os <i>SIPs</i> , foram aceitos e transformados em um <i>AIPs</i> integralmente ou em parte, ou ainda se foram recusados.
4.2.3.1 O repositório deve seguir os procedimentos documentados se um <i>SIP</i> não está incorporado a um <i>AIP</i> ou descartado e deve indicar por que o <i>SIP</i> não foi incorporado ou descartado.	No caso de o documento já possuir um identificador único, a ele atribuído no <i>SIP</i> , o repositório deverá mantê-lo no <i>AIP</i> , ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao <i>SIP</i> .
4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos persistentes para todos os <i>AIPs</i> .	Atribuir aos <i>AIPs</i> , identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por ex.: <i>Handle System</i> , DOI, URN, PURL).
4.2.4.1 O repositório deve identificar exclusivamente cada <i>AIP</i> dentro do repositório.	
4.2.4.1.1 O repositório terá identificadores exclusivos.	

ISO 16363:2012	Resolução 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
4.2.4.1.2 O repositório deverá ceder e manter identificadores persistentes do <i>AIP</i> e seus componentes, de modo a ser exclusivo dentro do contexto do repositório.	
4.2.5 Os repositórios devem ter acesso a ferramentas e recursos necessários para fornecer informações representante autorizado para todos os objetos digitais que ele contém.	Ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivo (ex.: <i>PRONOM</i> – base de dados com registro de formatos mantida pelo arquivo nacional do Reino Unido <sup>2</sup> ) e registros de outras informações de representação
4.2.5.1 O repositório deve ter ferramentas ou métodos para identificar o tipo de todos os objetos apresentados como dados de arquivo.	
4.2.5.2 O repositório deve ter ferramentas ou métodos para determinar quais representações da informações são necessárias para fazer cada objeto de dados compreensível para sua comunidade alvo.	
4.2.5.3 O repositório deve ter acesso à representação da informação necessária.	
4.2.5.4 O repositório deve ter ferramentas ou métodos para garantir que as representações da informação sejam requisitos persistentes e associado aos objetos de dados relevantes.	
4.2.6 O repositório deve ter processos documentados para a aquisição da Preservação da Descrição da Informações (PDI) para informação de conteúdo associado e adquirir PDI de acordo com os processos documentados.	Registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas anteriormente.
<b>4.2 Admissão: Criação da AIP</b>	<b>b. Admissão: criação do pacote de arquivamento</b>
4.2.6.1 O repositório deve ter processos documentados para a aquisição de PDI.	Registrar metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros.
4.2.7 O repositório deve assegurar que as informações de conteúdo do <i>AIP</i> são compreensíveis para a sua Comunidade alvo no momento da criação do <i>AIP</i> .	Ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais).
4.2.7.1 Repositório deve ter um processo documentado para testar compreensibilidade para as suas comunidades designadas das Informações do conteúdo das <i>AIP</i> na sua criação.	
4.2.7.2 O repositório deve executar o processo de teste para cada classe de Informações do conteúdo das <i>AIP</i> .	

<sup>2</sup> Disponível em: <http://nationalarchives.gov.uk/PRONOM/>

ISO 16363:2012	Resolução 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
4.2.7.3 Se falhar o teste de compreensibilidade, o repositório devem pôr as informações de conteúdo da <i>AIP</i> até o nível necessário para compreensão.	Ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais).
4.2.8 O repositório deve verificar cada <i>AIP</i> para a integralidade e exatidão no ponto em que é criado.	Verificar a completude e a correção de cada <i>AIP</i> no momento em que é gerado, isto é, no momento em que o <i>SIP</i> é convertido em <i>AIP</i> .
4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade do repositório de recolha / conteúdo.	Ter um mecanismo independente para verificar a integridade do conjunto do seu acervo, ou seja, verificar que todos os documentos previstos foram, de fato, admitidos no repositório justificando possíveis lacunas.
4.2.10 O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para a criação de <i>AIP</i> .	Documentar todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do <i>AIP</i> .
<b>4.3 Preservação</b>	<b>c. Planejamento da preservação</b>
4.3.1 O repositório deve ter documentado estratégias de preservação relevantes para as suas participações.	Estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos.
4.3.2.1 O repositório deve ter mecanismos para o monitoramento e a notificação quando a informação sobre a representação dos documentos for inadequada para seu público alvo.	Mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável (ex.: um formato de arquivo que esteja entrando em desuso, um suporte que esteja no final de sua vida útil).
4.3.3 O repositório deve ter mecanismos para mudar seus planos de preservação como resultado das suas atividades de monitorização.	Mecanismos de mudanças do plano de preservação como resultado do monitoramento
4.3.4 O repositório deve apresentar provas da eficácia das suas atividades de preservação.	Fornecimento de evidências sobre a eficácia do plano de preservação.
<b>4.5 Gestão da Informação</b>	<b>e. Gerenciamento de informação</b>
<b>4.4 Preservação do <i>AIP</i></b>	<b>d. Armazenamento e preservação / manutenção do <i>AIP</i></b>
4.4.1 O repositório deve ter especificações para saber como os <i>AIP</i> são armazenados até o nível de <i>Bit</i> .	Utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;
4.4.1.1 O repositório deve preservar as informações de conteúdo do <i>AIP</i> .	Atender minimamente a dois aspectos da preservação digital – os cuidados com armazenamento (controle dos suportes, dos formatos e da localização de cópias) e a eventual necessidade de migração (atualização de suportes e conversão de formatos);

ISO 16363:2012	Resolução 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
4.4.1.2 O repositório deve monitorar ativamente a integridade do <i>AIP</i> .	Monitoramento constante da integridade dos <i>AIPs</i> , por meio do registro de metadados de fixidade e de <i>logs</i> de checagem dessa integridade (por exemplo, <i>checksum</i> );
4.4.2 O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos <i>AIP</i> .	Preservação do documento digital (informação de conteúdo do <i>AIP</i> ) originalmente admitido no repositório e daquele resultante da última migração;
4.4.2.1 O repositório deve ter procedimentos para todas as ações tomadas em <i>AIP</i> .	Registro de todas as ações de preservação realizadas nos <i>AIPs</i> .
4.4.2.2 O repositório deve ser capaz de demonstrar que as ações tomadas em <i>AIP</i> foram compatíveis com a especificação dessas ações.	
4.5.1 O repositório deve especificar os requisitos mínimos de informação para permitir ao público alvo descobrir e identificar o material de seu interesse.	Metadados mínimos que permitam a busca e localização dos documentos – esses metadados devem ser identificadores conhecidos pela comunidade-alvo de usuários (ex.: número de matrícula do servidor público, título de livro numa biblioteca, número de processo).
4.5.2 O repositório deve capturar ou criar informações mínimas descritivas que garantam sua associação com o <i>AIP</i> .	Captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao <i>AIP</i> correspondente.
4.5.3 O repositório deverá manter ligação bi direcional entre cada <i>AIP</i> e sua informação descritiva.	Integridade referencial entre os <i>AIPs</i> e sua informação descritiva (metadados), ou seja, todo <i>AIP</i> deve ter uma informação descritiva, e toda informação descritiva deve apontar para um <i>AIP</i> .
4.5.3.1 O repositório deve manter as associações entre seus <i>AIP</i> e sua informação descritiva ao longo do tempo.	
<b>4.6 Gestão do acesso.</b>	<b>f. Gerenciamento de acesso</b>
4.6.1 O repositório deve cumprir políticas de acesso.	Divulgação, para a comunidade de usuários, das opções disponíveis de acesso aos documentos e de entrega dos mesmos;
4.6.1.1 O repositório deve registrar e analisar todas as falhas de gerenciamento de acesso e anomalias.	Implementação de uma política de registro dos acessos ocorridos que esteja de acordo com as necessidades de controle desses acessos, tanto da parte do repositório como dos produtores dos documentos nele admitidos;

**Fonte:** Elaborado pela autora

A Seção 4 aponta os requisitos no que diz respeito ao Gerenciamento do Objeto Digital em repositórios arquivísticos. É a seção, que contempla o maior número de requisitos na Norma ISO e de elementos na Resolução 39. Para essa seção a Norma utiliza a nomenclatura: Gerenciamento de Objetos Digitais, e a Resolução 39 utiliza nomenclatura Gerenciamento de Documentos Digitais. A seção é dividida em seis itens com nomenclaturas diferentes conforme Quadro 7 a seguir.

**Quadro 7** - Nomenclaturas utilizadas na Seção - Gerenciamento do Objeto Digital

Item	ISO 16363:2012	Item	Resolução 39 CONARQ
4.1	Admissão: aquisição de conteúdo	A	Admissão: captura de documentos digitais
4.2	Admissão: criação do <i>AIP</i>	B	Admissão: criação do pacote de arquivamento
4.3	Preservação	C	Planejamento da Preservação
4.4	Preservação do <i>AIP</i>	D	Armazenamento e preservação/manutenção do <i>AIP</i>
4.5	Gestão da Informação	E	Gerenciamento de informação
4.6	Gestão do acesso	F	Gerenciamento de acesso

**Fonte:** Elaborado pela autora

A primeira subdivisão 4.1 que diz respeito à admissão dos documentos no repositório, a Norma ISO o subdivide em dez subitens, já a Resolução 39 o subdivide em oito subitens, dos quais seis são assuntos tratados na ISO.

A segunda subdivisão 4.2 onde são contemplados os subitens relativos ao Pacote de informação para arquivamento, a norma ISO a subdivide em 28 subitens, e a Resolução 39 faz a subdivisão do item em treze subitens. Dessa feita, contemplando vinte e quatro assuntos tratados pela ISO.

Nesse ponto, as duas recomendações, em seus subitens, apontam a preocupação com o acesso do usuário.

Na terceira subdivisão 4.3 (Preservação), a Norma ISO subdivide o item Preservação em seis subitens, e a Resolução 39 subdivide o item Planejamento e preservação em quatro subitens, contemplando quatro subitens da ISO.

Na quarta subdivisão 4.4: Armazenamento e preservação/manutenção do *AIP*, os cinco subitens da ISO são contemplados na Resolução, porém a ISO os aponta com maior número de detalhes, as ações que deverão ser feitas.

Na quinta subdivisão 4.5: Gerenciamento da informação, tanto a ISO quanto a Resolução 39 apontam quatro subdivisões, porém dois subitens da ISO, como estão escritos mais detalhadamente, são abrangidos por um subitem da Resolução 39.

A sexta e última subdivisão 4.6: Gerenciamento de acesso, da segunda seção de requisitos, a ISO a subdivide em três subitens, enquanto que a Resolução 39 a subdivide em nove subitens.

No Quadro 8, demonstraremos os subitens da sessão 4 que são mencionados na Norma ISO 16.363 e não o são Resolução 39 ou vice-versa.

**Quadro 8** - Análise demonstrativa, itens não compatíveis pela Norma ISO 16363:2012 e pela Resolução 39 CONARQ:Seção 4 - Gerenciamento do Objeto Digital

ISO 16363:2012	RESOLUÇÃO 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
<b>4.1 Ingestões: aquisição de conteúdo</b>	<b>a. Admissão: captura de documentos digitais</b>
4.1.1 O repositório deve identificar as informações de conteúdo e as propriedades de informação que o repositório preservar.	
4.1.1.1 O repositório deve ter procedimento(s) para identificar as propriedades de informações que irão preservar.	
4.1.1.2 O repositório deve ter um registro da informação de conteúdo e as propriedades de informação que irá preservar.	
	Identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, <i>layout</i> , tabela de cor, resolução da imagem, canais de som etc.).
4.1.3 O repositório deve ter as especificações adequadas que permitam o reconhecimento e a análise do <i>SIP</i> .	
	Demonstrar em que momento a responsabilidade pela preservação do documento submetido ( <i>SIP</i> ) é formalmente aceita pelo repositório.
<b>4.2 Admissão: Criação da AIP</b>	<b>b Admissão: criação do pacote de arquivamento</b>
4.2.4.1.3 A documentação deve descrever todos os processos utilizados para alterações a esses identificadores.	
4.2.4.1.4 O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais para duplicações.	
4.2.4.1.5 O sistema de identificadores deve ser adequado para caber atuais e previsíveis necessidades futuras do repositório como números de objetos.	
4.2.4.2 O repositório deve ter um sistema de serviços de ligação/resolução de confiança, a fim de encontrar o objeto identificado exclusivamente, independentemente da sua localização física.	
<b>4.3 Preservação</b>	<b>c. Planejamento da preservação</b>

ISO 16363:2012	RESOLUÇÃO 39
<b>4. Gerenciamento do Objeto Digital</b>	<b>II.2.2 – Gerenciamento do documento digital</b>
4.3.2 O repositório deve ter mecanismos em vigor para monitorar a preservação do meio ambiente.	
4.3.3.1 O repositório deve ter mecanismos para criar, identificar ou recolher qualquer representação da informação necessária.	
<b>4.6 Gestão do acesso.</b>	<b>4.6 Gestão do acesso.</b>
4.6.2 O repositório devem seguir as políticas e procedimentos que permitam a difusão de objetos digitais que são rastreáveis aos originais, com provas que sustentem a sua autenticidade.	
	Concessão de acesso a cada <i>AIP</i> , para os usuários autorizados e da forma devida (ex.: autorização de “somente leitura”, ou acesso a um número limitado de itens por período), em conformidade com o acordo estabelecido entre o repositório e o produtor/depositante.
	Documentação e implementação de políticas de acesso (identificação e autenticação de usuários), em conformidade com os acordos estabelecidos entre o repositório e o produtor/depositante – essas políticas de acesso podem variar, desde a isenção da necessidade de identificação de usuário até o controle rígido da identificação e autenticação do usuário.
	Registro de falhas de controle de acesso (como, por exemplo, um acesso indevidamente negado) e uso desse registro para avaliar eventuais falhas no sistema de segurança.
	Demonstração de que o processo que gera o <i>DIP</i> atende completamente à requisição do usuário (ex.: se o usuário pediu um conjunto de documentos, receberá o conjunto completo; se ele pediu um documento, receberá apenas esse único documento).
	Demonstração de que o processo que gera o <i>DIP</i> está correto em relação ao pedido do usuário (ex.: se o repositório oferece imagens nos formatos JPG e PNG, o usuário deve receber, dentre esses, o formato que solicitou).
	Demonstração de que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição.
	Garantia da autenticidade dos <i>DIPs</i> , por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o <i>DIP</i> e o objeto original – para isso, um repositório deve ser capaz de demonstrar o processo de construção do <i>DIP</i> a partir de um <i>AIP</i> .

Fonte: Elaborado pela autora

Conforme ocorrência do quadro anterior, os subitens 4.1.1, 4.1.1.1, 4.1.1.2 e 4.1.3 (Ingestão: aquisição do conteúdo), os subitens 4.2.4.1.3, 4.2.4.1.4, 4.2.4.5 e 4.2.4.2 do item (Admissão: criação do pacote de arquivamento), 4.3.2 e 4.3.3.1 (Preservação) e 4.6.2 (Gestão do acesso), a resolução não os contempla devido a tais subitens serem relativos às políticas do repositório. Os 10 subitens acrescentados pela Resolução 39 ocorrem pela especificidade, visto que, se trata de documentos arquivísticos que estão subordinados à Lei de Acesso à Informação, aponta como o acesso deverá ser atendido pelo RDC-Arq.

No Quadro 9, estão demonstrados os requisitos recomendados pela Resolução 39 e pela ISO 16363 em sua seção 5.

**Quadro 9** - Análise demonstrativa, itens compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 5 - Infraestrutura e Segurança na Gestão de Riscos

ISO 16363:2012	Resolução 39
<b>5 Infraestrutura e segurança na gestão de riscos.</b>	<b>II.2.3 – Tecnologia, infraestrutura técnica e segurança</b>
<b>5.1 TÉCNICAS DE GESTÃO DE RISCO DE INFRAESTRUTURA.</b>	<b>b. Tecnologias apropriadas</b>
5.1.1.1.1O repositório deve possuir tecnologias de hardware adequadas aos serviços que oferece às suas comunidades alvo.	O repositório deve adotar uma tecnologia de <i>hardware</i> e <i>software</i> apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.
5.1.1.1.2 O repositório deve dispor de procedimentos para monitorar e receber notificações quando são necessárias mudanças de tecnologia de <i>hardware</i> .	
5.1.1.1.3 O repositório deve dispor de procedimentos para avaliar quando as mudanças são necessárias para <i>hardware</i> atual.	
5.1.1.1.5 O repositório terá tecnologias de <i>software</i> adequadas aos serviços que presta a sua comunidade alvo.	
5.1.1.1.6 O repositório deve dispor de procedimentos para monitorar e receber notificações quando são necessárias mudanças de <i>software</i> .	
5.1.1.1.7 O repositório deve dispor de procedimentos para avaliar quando as mudanças são necessárias para <i>software</i> atual.	
5.1.1.1.8 O repositório deve ter procedimentos, compromisso e financiamento para substituir <i>software</i> quando a avaliação indica a necessidade de fazê-lo.	
<b>5.1 TÉCNICAS DE GESTÃO DE RISCO DE INFRAESTRUTURA.</b>	
5.1.1.3 O repositório deve ter mecanismos eficazes para detectar a corrupção ou perda.	Mecanismos efetivos para a detecção de corrupção ou perda de <i>bits</i> .

ISO 16363:2012	Resolução 39
<b>5 Infraestrutura e segurança na gestão de riscos.</b>	<b>II.2.3 – Tecnologia, infraestrutura técnica e segurança</b>
5.1.1.3.1 O repositório deve registrar e reportar a sua administração todos os casos de corrupção ou perda de dados, e deverão ser tomadas medidas para reparo / substituição de dados corrompidos ou perdidos.	Relato dos incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados.
5.1.1.4 O repositório deve ter um processo para gravar e reagir à disponibilidade de novas atualizações de segurança baseados na avaliação do risco benefício.	Previsão de procedimentos de atualização de suporte ( <i>refreshing</i> ) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de <i>hardware</i> .
5.1.1.5 O repositório deve definir processos para mídia de armazenamento e / ou alteração de <i>hardware</i> (ex.: <i>refreshing</i> , migração).	
5.1.1.6 O repositório deve identificar e documentar processos críticos que afetem sua capacidade de cumprir com as suas responsabilidades obrigatórias.	Documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias.
5.1.1.1.6 O repositório deve dispor de procedimentos para monitorar e receber notificações quando são necessárias mudanças de <i>software</i> .	Adequação dos processos, do <i>hardware</i> e do <i>software</i> do sistema de <i>backup</i> às necessidades do repositório.
5.1.2 O repositório deve gerir o número e a localização das cópias de todos os objetos digitais.	Gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas.
<b>5.2 Gestão de riscos de Segurança</b>	<b>c. Segurança</b>
5.1.2.1 O repositório deve ter mecanismos para garantir várias cópias de objetos digitais sincronizados.	Mecanismos para garantir o sincronismo entre as cópias de um mesmo documento, ou seja, garantir que as mudanças intencionais feitas em uma cópia sejam propagadas para todas as outras.
5.2.1 O repositório deve manter uma análise sistemática dos fatores de risco de segurança associados com os dados, o sistema, o pessoal e as instalações físicas.	Análise sistemática de dados, sistemas, pessoas e instalação física.
5.2.2 O repositório deve ter implementado controles para tratar adequadamente cada um dos riscos de segurança definidos.	Adoção de procedimentos de controle para tratar adequadamente as necessidades de segurança.
5.2.3 A equipe repositório deve ter delineado funções, responsabilidades e autorizações relacionadas com a implementação de mudanças dentro do sistema.	Delineamento de papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema.
5.2.4 O repositório deve ter adequada preparação para desastres escritos e plano(s) de recuperação, incluindo pelo menos um <i>backup off-site</i> de todas as informações preservadas, juntamente com uma cópia fora do local dos plano (s) de recuperação.	Plano de prevenção de desastres e de reparação, que inclua, ao menos, um <i>backup, off-site</i> , de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.

Fonte: Elaborado pela autora

A terceira e última seção (seção 5) de requisitos diz respeito à gestão de riscos em nível de infraestrutura e segurança e está segmentada em duas subdivisões (5.1 e 5.2), enquanto as Diretrizes da Resolução 39 estabelecem três subdivisões (a, b e c). Conforme apontamento da Resolução, ela não faz a prescrição de *hardware* e *software*,

apenas descreve as melhores práticas pertinentes à gestão de dados e segurança que devem ser atendidas pelo RDC-Arq.

A primeira subdivisão da seção 5 da ISO, 5.1: Técnicas de gestão de risco de infraestrutura, é subdividida em vinte subitens. Destes subitens, quinze estão relacionados a 8 subitens das duas primeiras subdivisões (a e b) da Resolução 39 da seguinte forma: os subitens 5.1.1.1.1, 5.1.1.1.2, 5.1.1.1.3, 5.1.1.1.5, 5.1.1.1.6, 5.1.1.1.7.e 5.1.1.1.8 (pertinentes ao item Técnicas e gestão de riscos de infraestruturas) são contemplados pela Resolução 39 em seu único item de “b”- Tecnologias apropriadas; os subitens 5.1.1.4 e 5.1.1.5 são contemplados por um dos itens de “a” - Infraestrutura de sistema ; e os demais subitens da seção 5 fazem o relacionamento um por um com outros itens de “a”.

A segunda subdivisão da ISO diz respeito à Segurança, mesma nomenclatura apontada pela Resolução 39 em sua terceira subdivisão.

Nesta subdivisão (5.2), as duas recomendações apontam quatro subdivisões, havendo correspondência entre elas.

No Quadro 10, demonstraremos os subitens da sessão 5 que são mencionados na Norma 16.363 e não o são na Resolução 39 ou vice-versa.

**Quadro 10** - Análise demonstrativa, itens não compatíveis pela ISO 16363:2012 e pela Resolução 39 CONARQ: Seção 5 - Infraestrutura e Segurança na Gestão de Riscos

ISO 16363:2012	RESOLUÇÃO 39
5 infraestrutura e segurança na gestão de riscos.	II.2.3 – Tecnologia, infraestrutura técnica e segurança
5.1 TÉCNICAS DE GESTÃO DE RISCO DE INFRAESTRUTURA.	a. Infraestrutura de sistema
5.1.1 O repositório deve identificar e gerir os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema.	
5.1.1.1 O repositório deve empregar tecnologias de notificação de monitoramento de sistemas relacionado ao tempo (obsolescência).	

ISO 16363:2012	RESOLUÇÃO 39
<b>5 infraestrutura e segurança na gestão de riscos.</b>	<b>II.2.3 – Tecnologia, infraestrutura técnica e segurança</b>
5.1.1.1.4 O repositório deve ter procedimentos, compromisso e financiamento para substituir <i>hardware</i> quando a avaliação indica a necessidade de fazê-lo.	
5.1.1.2 O repositório terá suporte de <i>hardware</i> e <i>software</i> adequado para a funcionalidade de <i>backup</i> suficiente para preservar o conteúdo do repositório e acompanhamento de funções de repositório.	
5.1.1.6.1 O repositório deve ter um processo de gestão de mudança documentado que identifica alterações em processos críticos que potencialmente afetam a capacidade do repositório para cumprir com as suas responsabilidades obrigatórias.	
5.1.1.6.2 O repositório deve ter um processo para testar e avaliar o efeito das mudanças nos processos críticos do repositório.	
	Funcionamento do repositório com base num sistema operacional e outros <i>softwares</i> de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários.
	Previsão de procedimentos para testar o efeito de mudanças críticas no sistema.
	Ponderação entre os riscos e os benefícios nas decisões de atualização de <i>software</i> de segurança.

**Fonte:** Elaborado pela autora

A análise da seção 5 confirma a análise das seções três e quatro, que após serem cotejados com a Resolução 39, os itens das duas diretrizes não são completamente compatíveis, confirmando que as diretrizes da ISO fazem referência às políticas que o repositório deve ter. A Resolução, por sua vez, como é dirigida a repositórios arquivísticos que já possuem políticas próprias, direciona suas recomendações para a preservação dos documentos do domínio arquivístico.

Após o cotejamento das recomendações propostas pela norma ISO 16363:2012 que certifica Repositórios Digitais Confiáveis e das recomendações da Resolução 39 do CONARQ que oferece uma lista de requisitos para que um Repositório Arquivístico seja considerado Confiável e que possa ser certificado, apresenta-se no capítulo 6, a seguir, um conjunto de atividades (*Checklist*) que auxiliará o Arquivista na avaliação de confiabilidade de Repositório Arquivístico Digital Confiável que poderá resultar em sua certificação.

## **6 RECOMENDAÇÕES PARA A CONSTRUÇÃO DE RDC-ARQ, CONSIDERANDO AS DIRETRIZES DA NORMA ISO 16363:2012 E A RESOLUÇÃO 39 DO CONARQ BASEADAS NO ACESSO À INFORMAÇÃO**

Baseados na premissa de que os ambientes informacionais dos arquivos permanentes tratam, custodiam, preservam e propiciam o acesso às informações e aos documentos, para que repositórios digitais existam e tenham a característica de confiabilidade, faz-se imprescindível manter a integralidade, a proveniência e a preservação dos documentos. Caso contrário, os recursos arquivísticos deixariam de ser elemento ou prova de algum evento ocorrido, e, por conseguinte, não seriam confiáveis.

A Norma ISO 16363 (2012, p. 14, tradução nossa) aponta, em sua justificativa de criação, que: “[...] as alegações de confiabilidade são fáceis de fazer, mas até o momento, difíceis de justificar ou objetivamente provar. Então, estabelecer critérios mais claros detalhando o que é um repositório confiável ou não se tornou vital”.

Assim, a participação do arquivista na construção de um Repositório Digital assegurará a manutenção das características do recurso arquivístico, mesmo com as mudanças ocorridas nos suportes, no acesso, na agilização do processo de descrição e de transferência da informação, criados a partir do uso das tecnologias que potencializam o acesso e a disseminação da informação.

Nesse contexto, considerando a Lei de Acesso à Informação, a preocupação está na construção de Repositórios Arquivísticos Digitais Confiáveis, que mantenham as características do recurso para serem elementos de prova, ofereçam acesso remoto, gerenciem conteúdo, preservem, utilizem metadados como parte do processo da Curadoria Digital, visando à preservação, à recuperação, à segurança e à confiabilidade, considerando que o ambiente arquivístico contém especificidades quanto ao grau de sigilo e acesso.

A partir da análise exploratória da Norma ISO 16363:2012, que faz a certificação de Repositórios Digitais, da Resolução 39 do Conarq, que faz recomendações para que um Repositório Arquivístico Digital Confiável, da legislação vigente no Brasil e dos estudos de Camargo (2010), no Quadro 11, a seguir apresentam-se recomendações

que auxiliam o Arquivista no pedido de certificação ou na medição de confiabilidade de um RDC-Arq.

As recomendações que estão em cor azul foram adicionadas às Diretrizes propostas pela ISO 16363:2012 e pelo CONARQ, visto que este estudo tem como proposta o acesso à informação. Assim, dizem respeito ao conhecimento por parte do arquivista, às leis referentes a arquivos e acesso vigentes no país, à Curadoria Digital, tema explorado no corpo do trabalho, à Acessibilidade e à Usabilidade.

**Quadro 11** - Recomendações de *checklist* para medição e/ou certificação de confiabilidade para RDC-Arq com ênfase no Acesso à Informação

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
ORGANIZAÇÃO E INFRAESTRUTURA	1. Política de Arquivo	1.1	Estar em conformidade com a lei em vigência que dispõe sobre a política nacional de arquivos e privados e dá outras providências, hoje Lei n. 8.159 (BRASIL, 1991).		
		1.2	Estar em conformidade com a Lei de Acesso à Informação Lei 12.527 (BRASIL, 2012).		
	2. Governança e viabilidade Organizacional	2.1	Ter uma declaração de missão que reflita um compromisso com a preservação, a gestão e acesso à informação digital por longo prazo (ISO, 2012).		
		2.2	Ter como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. Essa missão é claramente identificada por todos os interessados no repositório e envolve: mandato legal, contexto organizacional e requisitos regulatórios (CONARQ, 2014).		
		2.3	Ter um Plano Estratégico de Preservação que defina a abordagem do repositório no apoio a sua missão em longo prazo (ISO, 2012).		
		2.4	Ter um plano adequado de sucessão, planos de contingência e/ou acordos judiciais, no caso de o repositório parar sua atividade ou a instituição governamental, ou financiamento mudar substancialmente o seu âmbito (ISO, 2012).		
		2.5	Ter um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos para garantir a continuidade do serviço, no caso de o repositório parar de operar ou de a instituição responsável e/ou financiadora mudar seu escopo (CONARQ, 2014).		
		2.6	Controlar seu ambiente organizacional para determinar quando executar o seu plano de sucessão, planos de contingência e/ou acordos judiciais (ISO, 2012).		
		2.7	Ter uma política para o recolhimento do documento, especificando o tipo de informação que irá preservar, manter, gerenciar e fornecer acesso (ISO, 2012).		
	3. Estrutura Organizacional	3.1	Identificar e estabelecer as funções que necessita realizar e nomear pessoas com qualificações e experiência adequadas para cumprir esses deveres. (ISO, 2012)		
		3.2	Ter uma equipe dotada de qualificação e formação necessárias e em número suficiente, para garantir todos os serviços e funcionalidades pertinentes ao repositório. Além disso, manter um programa de desenvolvimento profissional contínuo (CONARQ, 2014).		
		3.3	Identificar e estabelecer os deveres que precisa executar (ISO, 2012).		
		3.4	Ter um número adequado de pessoas em sua equipe, para apoiar todas as funções e serviços (ISO, 2012).		
		3.5	Colocar em prática um programa de desenvolvimento profissional ativo que forneça a qualificação da equipe, competências e oportunidades de desenvolvimento (ISO, 2012).		
	4. Regulamentação de Responsabilidades políticas de preservação	4.1	Definir a sua base de conhecimento, sua Comunidade-Alvo e ter essas definições acessíveis (ISO, 2012; CONARQ, 2014).		
		4.2	Ter políticas de preservação, para garantir que seu Plano Estratégico de Preservação será cumprido (ISO, 2012).		
4.3		Possuir políticas e definições, acessíveis publicamente que demonstrem como os requisitos do serviço de preservação serão contemplados (CONARQ, 2014).			

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
ORGANIZAÇÃO E INFRAESTRUTURA	4. Regulamentação de Responsabilidades políticas de preservação	4.4	Possuir mecanismos de revisão, atualização e desenvolvimento contínuo de suas políticas de preservação, à medida que o repositório cresce, e a tecnologia e, as práticas da comunidade evoluem (ISO, 2012; CONARQ, 2014).		
		4.5	Documentar permissões legais – por meio de acordos de custódia, normas de procedimentos e outros – que isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital (CONARQ, 2014).		
		4.6	Ter sua história documentada, bem como as alterações de operações e procedimentos de <i>software</i> e <i>hardware</i> (ISO, 2012).		
		4.7	Fazer o registro histórico de mudanças de procedimentos e de <i>software</i> e <i>hardware</i> (CONARQ, 2014).		
		4.8	Comprometer-se com a transparência e com a responsabilidade em todas as ações de apoio à exploração e gestão do repositório que afetem a preservação de conteúdos digitais ao longo do tempo (ISO, 2012).		
		4.9	Relacionar o registro histórico acima referido, com suas estratégias de preservação digital e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais (CONARQ, 2014).		
		4.10	Demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, buscando atendê-las (CONARQ, 2014).		
		4.11	Comprometer-se em definir, coletar, rastrear e fornecer medidas para a integridade da informação (ISO, 2012).		
		4.12	Estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia (CONARQ, 2014).		
		4.13	Possuir com um calendário para fazer regularmente a autoavaliação de seu funcionamento e renovar sua certificação externa (ISO, 2012).		
	4.14	<a href="#">Adotar a Curadoria Digital como um processo para o ciclo de vida dos documentos em que a preservação seja parte desse processo.</a>			
	5. Sustentabilidade Financeira	5.1	Dispor de sistemas de planejamento de negócios de curto e longo prazo, para que seja mantido ao longo do tempo (ISO, 2012).		
		5.2	Demonstrar a capacidade de obter recursos financeiros estáveis e contínuos para sustentar, por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros (CONARQ, 2014).		
		5.3	Possuir práticas e procedimentos que sejam transparentes (em conformidade com as normas e práticas contábeis relevantes) e auditados por terceiros de acordo com os requisitos legais territoriais financeiros (ISO, 2012).		
		5.4	Ter transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere (CONARQ, 2014).		
		5.5	Realizar revisão e ajustes anuais (CONARQ, 2014).		
		5.6	Ter um compromisso contínuo para analisar e informar sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos) (ISO, 2012).		
5.7		Comprometer-se com os ciclos de planejamento, com o equilíbrio dos riscos, benefícios, investimentos e gastos (CONARQ, 2014).			

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
ORGANIZAÇÃO E INFRAESTRUTURA	6. Contratos, licenças e passivos	6.1	Ter e manter contratos adequados ou contratos de depósito para materiais digitais que ele gereencie e/ou preserve para o qual forneça acesso (ISO, 2012).		
		6.2	Possuir os contratos de depósito que especifiquem todos os direitos de preservação necessários, transferindo-os e documentando-os (ISO, 2012).		
		6.3	Ter especificados todos os aspectos relevantes de aquisição, manutenção, acesso e retirada em acordos escritos com os depositantes e outras partes relevantes (ISO, 2012).		
		6.4	Ter seus contratos, licenças e passivos firmados pelo repositório claros e mensuráveis; delinear papéis, responsabilidades, prazos e condições e ser facilmente acessíveis ou disponíveis aos interessados. Esses contratos, licenças e passivos podem envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. Esses mesmos instrumentos devem especificar todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial, no que diz respeito à propriedade intelectual e a restrições de uso (CONARQ, 2014).		
		6.5	Ter registrado as políticas que indiquem, quando ele aceita a responsabilidade de preservação de conteúdo de cada conjunto de objetos, de dados apresentados (ISO, 2012).		
		6.6	Ter políticas para lidar com a responsabilidade e os desafios à propriedade e aos direitos (ISO, 2012).		
		6.7	O repositório deve rastrear e gerenciar direitos de propriedade intelectual e as restrições à utilização de conteúdo do repositório como exigido pelo contrato de depósito, contrato ou licença (ISO, 2012).		
	7. Acessibilidade	7.1	Fornecer alternativas de não-texto de modo que possa ser mudado para outro tipo como braile, discurso ou símbolos. (CAMARGO, 2010).		
		7.2	Fornecer alternativas sincronizadas para multimídia (CAMARGO, 2010).		
		7.3	Criar várias maneiras de apresentação do índice (CAMARGO, 2010).		
		7.4	Utilizar toda a funcionalidade disponível do teclado (CAMARGO, 2010).		
		7.5	Oferecer opção de modificação de tamanho de fonte (CAMARGO, 2010).		
		7.6	Oferecer opção de modificação de fundo de página (CAMARGO, 2010).		
	8. Usabilidade	8.1	Exibir o nome do Repositório e/ou logotipo ou slogan (CAMARGO, 2010).		
		8.2	Incluir um link da homepage para uma Seção “Sobre Nós” (CAMARGO, 2010).		
		8.3	Incluir um link “Fale Conosco” (CAMARGO, 2010).		
		8.4	Empregar padrões e estilo com consistência (CAMARGO, 2010).		
		8.5	Disponibilizar para os usuários uma caixa de busca (CAMARGO, 2010).		
		8.6	Usar texto com muito contraste e cores de pano de fundo (CAMARGO, 2010).		
		8.7	Evitar rolagem horizontal (CAMARGO, 2010).		

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
ORGANIZAÇÃO E INFRAESTRUTURA	8. Usabilidade	8.8	Usar raramente menus suspensos (CAMARGO, 2010).		
		8.9	Informar se o <i>website</i> ficar paralisado ou não estiver funcionando (CAMARGO, 2010).		
		8.10	Reduzir o tempo das respostas (CAMARGO, 2010).		
		8.11	Oferecer cursor com comportamento padronizado (CAMARGO, 2010).		
		8.12	Dar enfoque no conteúdo (CAMARGO, 2010).		
		8.13	Possibilitar retorno à página principal (CAMARGO, 2010).		
		8.14	Possibilitar o acesso às informações por meio de poucos comandos (CAMARGO, 2010).		
		8.15	Utilizar mensagens de erro com vocabulário neutro (CAMARGO, 2010).		
		8.16	Evitar caracteres especiais e adequar à fonte em relação ao assunto (CAMARGO, 2010)		
GERENCIAMENTO DO DOCUMENTO DIGITAL	9. Recepção: aquisição de conteúdo	9.1	Identificar as informações de conteúdo e as propriedades de informação que o repositório preservar (ISO, 2012).		
		9.2	Ter um procedimento(s) para identificar as propriedades de informações que irá preservar (ISO, 2012).		
		9.3	Ter um registro da informação de conteúdo e as propriedades de informação que irá preservar (ISO, 2012).		
		9.4	Identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, <i>layout</i> , tabela de cor, resolução da imagem, canais de som etc.) (CONARQ, 2014).		
		9.5	Especificar claramente a informação que precisa ser associado com informação de conteúdo específico no momento do seu depósito (ISO, 2012).		
		9.6	Especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão (CONARQ, 2014).		
		9.7	O repositório deve ter as especificações adequadas que permitam o reconhecimento e a análise do <i>SIP</i> (ISO, 2012).		
		9.8	O repositório deve ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais (ISO, 2012).		
		9.9	Ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência (CONARQ, 2014).		
		9.10	Ter um processo de ingerir que verifique cada <i>SIP</i> para integralidade e exatidão (ISO, 2012).		
		9.11	Ter procedimentos para verificar a integridade do <i>SIP</i> o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana (CONARQ, 2014).		
		9.12	O repositório deve ter controle suficiente sobre os Objetos Digitais para preservá-los (ISO, 2012; CONARQ 2014).		
		9.13	Fornecer ao produtor/depositante respostas adequadas em pontos acordados durante os processos de recepção (ISO, 2012)		
		9.14	Fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo processo da admissão (CONARQ, 2014).		
		9.15	Ter registros das ações e processos de administração que sejam relevantes para aquisição de conteúdo (ISO, 2012).		

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
GERENCIAMENTO DO DOCUMENTO DIGITAL	9. Recepção: aquisição de conteúdo	9.16	Ter registros de todas as ações e processos administrativos que ocorram durante o processo de admissão e sejam relevantes para a preservação (CONARQ, 2014).		
		9.17	Demonstrar em que momento a responsabilidade pela preservação do documento submetido ( <i>SIP</i> ) é formalmente aceita pelo repositório (CONARQ, 2014).		
	10. Admissão: criação do pacote de arquivamento	10.1	Ter para cada <i>AIP</i> ou classe de <i>AIP</i> preservados pelo repositório uma definição associada que seja adequada para analisar o <i>AIP</i> e estar apto para as necessidades de preservação em longo prazo (ISO, 2012).		
		10.2	Descrever minuciosamente as diferentes classes de informação e como os <i>AIPs</i> são implementados nos casos em que a especificidade dessas classes exija ações de preservação diferentes (por exemplo, a imagem <i>TIFF</i> que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessárias à imagem <i>TIFF</i> que é apresentada ao olho humano) (CONARQ, 2014).		
		10.3	Ser capaz de identificar qual definição se aplica a qual <i>AIP</i> (ISO, 2012).		
		10.4	Ter uma definição de cada <i>AIP</i> que seja adequada para a preservação a longo prazo, permitindo a identificação e análise de todos os componentes requeridos dentro do <i>AIP</i> (ISO, 2012).		
		10.5	Descrever cada classe de informação (texto estruturado, imagem matricial, banco de dados, imagem em movimento e outras) a ser preservada pelo repositório, e como ela está implementada. Essa descrição deve apontar as componentes chaves do <i>AIP</i> : o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixibilidade, proveniência e contexto), e ainda como esses componentes se relacionam (CONARQ, 2014).		
		10.6	O repositório deve ter uma descrição de como os <i>AIPs</i> são construídos a partir <i>SIP</i> (ISO, 2012).		
		10.7	Descrever como os <i>AIPs</i> são construídos a partir dos <i>SIPs</i> , ou seja, apontar todas as transformações pelas quais passarão os documentos, os metadados submetidos e os metadados a serem adicionados no momento da formação do <i>AIP</i> (CONARQ, 2014).		
		10.8	Documentar a disposição final de todos os <i>SIP</i> (ISO, 2012).		
		10.9	Ser capaz de demonstrar se os <i>SIPs</i> foram aceitos e transformados em <i>AIPs</i> integralmente ou em parte, ou ainda se foram recusados (CONARQ, 2014).		
		10.10	Seguir os procedimentos documentados (se um <i>SIP</i> não está incorporado num <i>AIP</i> ou descartado) e deve indicar por que o <i>SIP</i> não foi incorporado ou descartado (ISO, 2012).		
		10.11	No caso de o documento já possuir um identificador único a ele atribuído no <i>SIP</i> , o repositório deverá mantê-lo no <i>AIP</i> , ou criar outro identificador que deverá ser associado, de maneira persistente, ao <i>SIP</i> (CONARQ, 2014).		
		10.12	Ter e usar uma convenção que gere identificadores únicos persistentes para todos os <i>AIPs</i> (ISO, 2012).		
		10.13	Identificar exclusivamente cada <i>AIP</i> dentro do repositório (ISO, 2012).		
10.14	Possuir identificadores exclusivos (ISO, 2012).				
10.15	Ceder e manter identificadores persistentes do <i>AIP</i> e seus componentes, de modo a ser exclusivo dentro do contexto do repositório (ISO, 2012).				

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
GERENCIAMENTO DO DOCUMENTO DIGITAL	10. Admissão: criação do pacote de arquivamento	10.16	Atribuir aos <i>AIPs</i> identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por ex.: <i>Handle System</i> , DOI, URN, PURL) ( CONARQ, 2014).		
		10.17	A documentação deve descrever todos os processos utilizados para alterações nesses identificadores (ISO, 2012).		
		10.18	O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais para duplicações (ISO, 2012).		
		10.19	O sistema de identificadores deve ser adequado para conter atuais e previsíveis necessidades futuras do repositório, como números de objetos (ISO, 2012).		
		10.20	O repositório deve ter um sistema de serviços de ligação/resolução de confiança, a fim de encontrar o objeto identificado como exclusivo, independentemente da sua localização física (ISO, 2012).		
		10.21	O repositório deve ter acesso a ferramentas e recursos necessários para fornecer informações ao Representante autorizado sobre todos os objetos digitais que ele contém (ISO, 2012).		
		10.22	O repositório deve ter ferramentas ou métodos para identificar o tipo de todos os objetos apresentados como dados de arquivo (ISO, 2012).		
		10.23	O repositório deve ter ferramentas ou métodos para determinar quais representações das informações são necessárias para fazer todo o dado compreensível para sua comunidade-alvo (ISO, 2012).		
		10.24	O repositório deve ter acesso à representação da informação necessária (ISO, 2012).		
		10.25	O repositório deve ter ferramentas ou métodos para garantir que as representações das informações sejam requisitos persistentes e associados aos objetos de dados relevantes (ISO, 2012).		
		10.26	Ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivo (ex.: <i>PRONOM</i> – base de dados com registro de formatos, mantida pelo arquivo nacional do Reino Unido) e registros de outras informações de representação (CONARQ, 2012).		
		10.27	O repositório deve ter processos documentados para a aquisição da Preservação da Descrição da Informação (PDI) para informação de conteúdos associados e adquirir PDI de acordo com os processos documentados (ISO, 2012).		
		10.28	Registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas anteriormente (CONARQ, 2012).		
		10.29	O repositório deve ter processos documentados para a aquisição de PDI (ISO, 2012).		
		10.30	Registrar metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros (CONARQ, 2012).		
		10.31	Assegurar que as informações de conteúdo do <i>AIP</i> sejam compreensíveis para a sua Comunidade-alvo no momento da criação do <i>AIP</i> (ISO, 2012).		
10.32	Ter um processo documentado para testar compreensibilidade de suas comunidades designadas das Informações do conteúdo dos <i>AIP</i> na sua criação (ISO, 2012).				
10.33	Executar o processo de teste para cada classe de Informações do conteúdo dos <i>AIP</i> (ISO, 2012).				
10.34	Se falhar o teste de compreensibilidade, o repositório deve pôr as informações de conteúdo do <i>AIP</i> até o nível necessário para compreensão (ISO, 2012).				

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
GERENCIAMENTO DO DOCUMENTO DIGITAL	10. Admissão: criação do pacote de arquivamento	10.35	Ter procedimentos para testar se os documentos são compreensíveis pela comunidade-alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais) (CONARQ, 2012).		
		10.36	Verificar cada AIP para a integralidade e exatidão no ponto em que é criado (ISO, 2012).		
		10.37	Verificar a completude e a correção de cada AIP no momento em que é gerado, isto é, no momento em que o SIP é convertido em AIP (CONARQ, 2012).		
		10.38	Fornecer um mecanismo independente para verificar a integridade do repositório de recolha/conteúdo (ISO, 2012).		
		10.39	Ter um mecanismo independente para verificar a integridade do conjunto do seu acervo, ou seja, verificar que todos os documentos previstos foram, de fato, admitidos no repositório justificando possíveis lacunas (CONARQ, 2012).		
		10.40	Ter registros contemporâneos de ações e processos de administração que sejam relevantes para a criação do AIP (ISO, 2012).		
		10.41	Documentar todas as ações relevantes à preservação dos documentos que estão relacionadas à criação do AIP (CONARQ, 2012).		
	11. Preservação	11.1	Documentar estratégias de preservação relevantes para as suas participações (ISO, 2012).		
		11.2	Preservar estratégias bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos (CONARQ, 2012).		
		11.3	Ter mecanismos em vigor para monitorar a preservação do meio (ISO, 2012).		
		11.4	Ter mecanismos para o monitoramento e a notificação quando a informação sobre a representação dos documentos for inadequada para seu público alvo (ISO, 2012).		
		11.5	Ter mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável (ex.: um formato de arquivo que esteja entrando em desuso, um suporte que esteja no final de sua vida útil) (CONARQ, 2012).		
		11.6	Ter mecanismos para mudar seus planos de preservação como resultado das suas atividades de monitorização (ISO, 2012).		
		11.7	Ter mecanismos de mudanças do plano de preservação como resultado do monitoramento (CONARQ, 2012).		
		11.8	Ter mecanismos para criar, identificar ou recolher qualquer representação da informação necessária (ISO, 2012).		
		11.9	Apresentar provas de eficácia das suas atividades de preservação (ISO, 2012).		
		11.10	Fornecer evidências sobre a eficácia do plano de preservação (CONARQ, 2012).		
	12. Preservação do AIP	12.1	Ter especificações para saber como os AIP são armazenadas até o nível de bit (ISO, 2012).		
		12.2	Utilizar as estratégias previstas no planejamento da preservação que podem ser várias e devem ser registradas nos metadados de preservação (CONARQ, 2012).		
		12.3	O repositório deve preservar as informações de conteúdo da AIP (ISO, 2012).		
		12.4	Atender minimamente a dois aspectos da preservação digital – os cuidados com armazenamento (controle dos suportes, dos formatos e da localização de cópias) e a eventual necessidade de migração (atualização de suportes e conversão de formatos) (CONARQ, 2012).		
		12.5	O repositório deve monitorar ativamente a integridade do AIP (ISO, 2012).		

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
GERENCIAMENTO DO DOCUMENTO DIGITAL	12. Preservação do AIP	12.6	Monitorar constantemente a integridade dos AIPs por meio do registro de metadados de fixidade e de logs de checagem dessa integridade (por exemplo, <i>checksum</i> ) (CONARQ, 2012).		
		12.7	O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIP (ISO, 2012).		
		12.8	Preservar o documento digital (informação de conteúdo do AIP) originalmente admitido no repositório e daquele resultante da última migração (CONARQ, 2012).		
		12.9	Ter procedimentos para todas as ações tomadas em AIP (ISO, 2012).		
		12.10	Ser capaz de demonstrar que as ações tomadas em AIP foram compatíveis com a especificação dessas ações (ISO, 2012).		
		12.11	Registrar todas as ações de preservação realizadas nos AIPs (CONARQ, 2012).		
	13. Gestão da Informação	13.1	Especificar os requisitos mínimos de informação para permitir ao público alvo descobrir e identificar o material de seu interesse (ISO, 2012).		
		13.2	Ter metadados mínimos que permitam a busca e localização dos documentos e sejam identificadores conhecidos pela comunidade-alvo de usuários (ex.: número de matrícula do servidor público, título de livro numa biblioteca, número de processo) (CONARQ, 2012).		
		13.3	Fazer a captura ou criar informações mínimas descritivas e garantir que ele esteja associado com o AIP (ISO, 2012).		
		13.4	Fazer a captura ou criação de metadados mínimos pelo repositório durante o processo de admissão e associação desses metadados ao AIP correspondente (CONARQ, 2012).		
		13.5	Manter ligação bidirecional entre cada AIP e sua informação descritiva (ISO, 2012).		
		13.6	O repositório deve manter as associações entre seus AIP e sua informação descritiva ao longo do tempo (ISO, 2012).		
		13.7	Integridade referencial entre os AIPs e sua informação descritiva (metadados), ou seja, todo AIP deve ter uma informação descritiva, e toda informação descritiva deve apontar para um AIP (CONARQ, 2012).		
		13.8	Manter a integridade referencial, mesmo no caso de quebra temporária da relação entre AIP e seus metadados descritivos. Nesse caso, o repositório deve ser capaz de restaurar a relação rompida (CONARQ, 2012).		
	14. Gestão do Acesso	14.1	O repositório deve cumprir políticas de acesso (ISO, 2012).		
		14.2	Divulgar para a comunidade de usuários as opções disponíveis de acesso aos documentos e de entrega dos mesmos (CONARQ, 2012).		
		14.3	Registrar e analisar todas as falhas de gerenciamento de acesso e anomalias (ISO, 2012).		
		14.4	Implementar uma política de registro dos acessos ocorridos que esteja de acordo com as necessidades de controle desses acessos, tanto da parte do repositório como dos produtores dos documentos nele admitidos (CONARQ, 2012).		
14.5		Seguir políticas e procedimentos que permitam a difusão de objetos digitais que sejam rastreáveis aos originais com provas que sustentem a sua autenticidade (ISO, 2012).			
14.6		Conceder acesso a cada AIP para os usuários autorizados e da forma devida (ex.: autorização de "somente leitura", ou acesso a um número limitado de itens por período), em conformidade com o acordo estabelecido entre o repositório e o produtor/depositante (CONARQ, 2012).			

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
GERENCIAMENTO DO DOCUMENTO DIGITAL	14. Gestão do Acesso	14.7	Documentar e implementar políticas de acesso (identificação e autenticação de usuários), em conformidade com os acordos estabelecidos entre o repositório e o produtor/depositante. Essas políticas de acesso podem variar desde a isenção da necessidade de identificação de usuário até o controle rígido da identificação e autenticação do usuário (CONARQ, 2012).		
		14.8	Registrar de falhas no controle de acesso (como, por exemplo, um acesso indevidamente negado) e uso desse registro para avaliar eventuais falhas no sistema de segurança (CONARQ, 2012).		
		14.9	Demonstrar que o processo que gera o <i>DIP</i> atende completamente à requisição do usuário (ex.: se o usuário pediu um conjunto de documentos, receberá o conjunto completo; se ele pediu um documento, receberá apenas esse único documento) (CONARQ, 2012).		
		14.10	Demonstrar que o processo que gera o <i>DIP</i> está correto em relação ao pedido do usuário (ex.: se o repositório oferece imagens nos formatos JPG e PNG, o usuário deve receber, dentre esses, o formato que solicitou) (CONARQ, 2012).		
		14.11	Demonstrar que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição (CONARQ, 2012).		
		14.12	Garantir a autenticidade dos <i>DIPs</i> por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o <i>DIP</i> e o objeto original. Para isso, um repositório deve ser capaz de demonstrar o processo de construção do <i>DIP</i> a partir de um <i>AIP</i> (CONARQ, 2012).		
INFRAESTRUTURA E SEGURANÇA NA GESTÃO DE RISCOS	15. Técnicas de gestão de risco e infraestrutura	15.1	Identificar e gerir os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema (ISO, 2012).		
		15.2	O repositório deve empregar tecnologias de notificação de monitoramento de sistemas relacionadas ao tempo (obsolescência) (ISO, 2012).		
		15.3	Disponer de procedimentos para monitorar e receber notificações quando forem necessárias mudanças de tecnologia de <i>hardware</i> (ISO, 2012).		
		15.4	Disponer de procedimentos para avaliar quando as mudanças forem necessárias para <i>hardware</i> atual (ISO, 2012).		
		15.5	Adotar uma tecnologia de <i>hardware</i> e <i>software</i> apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada (CONARQ, 2012).		
		15.6	Ter procedimentos, compromisso e financiamento para substituir <i>hardware</i> quando a avaliação indicar a necessidade de fazê-lo (ISO, 2012).		
		15.7	Ter tecnologias de <i>software</i> adequadas aos serviços que presta a sua comunidade-alvo (ISO, 2012).		
		15.8	Disponer de procedimentos para monitorar e receber notificações quando são necessárias mudanças de <i>software</i> (ISO, 2012).		
		15.9	Disponer de procedimentos para avaliar quando as mudanças são necessárias para <i>software</i> atual (ISO, 2012).		
		15.10	Ter procedimentos, compromisso e financiamento para substituir <i>software</i> quando a avaliação indicar a necessidade de fazê-lo (ISO, 2012).		
		15.11	Ter suporte de <i>hardware</i> e <i>software</i> adequado para a funcionalidade de <i>backup</i> suficiente para preservar o conteúdo do repositório e acompanhamento de funções de repositório (ISO, 2012).		

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
INFRAESTRUTURA E SEGURANÇA NA GESTÃO DE RISCOS	15. Técnicas de gestão de risco e infraestrutura	15.12	Ter mecanismos efetivos para a detecção de corrupção ou perda de <i>bits</i> (CONARQ, 2012).		
		15.13	Registrar e reportar a sua administração todos os casos de corrupção ou perda de dados, e, deverão ser tomadas medidas para reparo/substituição de dados corrompidos ou perdidos (ISO, 2012).		
		15.14	Relatar os incidentes de corrupção ou perda de dados eventualmente ocorridos e adotar medidas para reparação ou substituição desses mesmos dados (CONARQ, 2012).		
		15.15	Ter um processo para gravar e reagir à disponibilidade de novas atualizações de segurança baseado na avaliação do risco/benefício (ISO, 2012).		
		15.16	Definir processos para mídia de armazenamento e / ou alteração de <i>hardware</i> (ex: <i>refreshing</i> , migração) (ISO, 2012).		
		15.17	Ter previsão de procedimentos de atualização de suporte ( <i>refreshing</i> ) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de <i>hardware</i> (CONARQ, 2012).		
		15.18	Identificar e documentar processos críticos que afetem sua capacidade de cumprir com as suas responsabilidades obrigatórias (ISO, 2012).		
		15.19	Documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias (CONARQ, 2012).		
		15.20	O repositório deve dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças de <i>software</i> (ISO, 2012).		
		15.21	Adequar os processos do <i>hardware</i> e do <i>software</i> do sistema de <i>backup</i> às necessidades do repositório (CONARQ, 2012).		
		15.22	Ter um processo de gestão de mudança documentado que identifique alterações em processos críticos que potencialmente afetem a capacidade de o repositório cumprir suas responsabilidades obrigatórias (ISO, 2012).		
		15.23	Ter um processo para testar e avaliar o efeito das mudanças nos processos críticos do repositório.		
		15.24	O repositório deve gerir o número e a localização das cópias de todos os objetos digitais (ISO, 2012).		
		15.25	Gerenciar o número de cópias de todos os documentos mantidos no repositório e a localização de cada uma delas (CONARQ, 2012).		
		15.26	Ter mecanismos para garantir várias cópias de objetos digitais sincronizados (ISO, 2012).		
		15.27	Ter mecanismos para garantir o sincronismo entre as cópias de um mesmo documento, ou seja, garantir que as mudanças intencionais feitas em uma cópia sejam propagadas para todas as outras (CONARQ, 2012).		
		15.28	Ter seu funcionamento com base num sistema operacional e outros <i>softwares</i> de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários (CONARQ, 2012).		
15.29	Ter previsão de procedimentos para testar o efeito de mudanças críticas no sistema (CONARQ, 2012).				
15.30	Fazer a ponderação entre riscos e benefícios nas decisões de atualização de <i>software</i> de segurança (CONARQ, 2012).				

Seção	Tópico	Item	Descrição do item para verificação	Sim	Não
INFRAESTRUTURA E SEGURANÇA NA GESTÃO DE RISCOS	16. Tecnologias apropriadas	16.1	Ter adotado uma tecnologia de <i>hardware</i> e <i>software</i> apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada (CONARQ, 2012).		
	17. Gestão de Riscos - Segurança	17.1	Manter uma análise sistemática dos fatores de risco de segurança associados com os dados, os sistemas, o pessoal e as instalações físicas (ISO, 2012).		
		17.2	Fazer a análise sistemática de dados, sistemas, pessoas e instalação física (CONARQ, 2012).		
		17.3	Implementar controles para tratar adequadamente cada um dos riscos de segurança definidos (ISO, 2012).		
		17.4	Adotar procedimentos de controle para tratar adequadamente as necessidades de segurança (CONARQ, 2012).		
		17.5	A equipe repositório deve delinear funções, responsabilidades e autorizações relacionadas com a implementação de mudanças dentro do sistema (ISO, 2012).		
		17.6	Delinear papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema (CONARQ, 2012).		
		17.7	Ter adequada preparação para desastres escritos e plano(s) de recuperação, incluindo, pelo menos, um backup off-site de todas as informações preservadas, juntamente com uma cópia fora do local do plano (s) de recuperação (ISO, 2012).		
		17.8	Possuir plano de prevenção de desastres e de reparação que inclua, ao menos, um <i>backup off site</i> de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação (CONARQ, 2012).		

Fonte: Elaborado pela autora

A análise da Norma ISO 16363:2012 e das Recomendações 39 do CONARQ, gerou orientações que auxiliarão os arquivistas no que diz respeito a melhores práticas no que tange à confiabilidade dos Repositórios Arquivísticos Digitais, tanto para sua certificação, como para a medição de confiabilidade, quesito capital para um repositório do domínio arquivístico brasileiro.

Como nossa ênfase está no acesso à informação, as recomendações propostas são dirigidas aos arquivistas. Após a análise exploratória das normas, foi feita a categorização e o cotejamento entre os dois documentos após esse processo, conforme explicitado no capítulo cinco, foi proposta a ampliação de três tópicos e vinte e cinco itens, objetivando o acesso de um maior número de usuários às informações custodiadas e disponibilizadas pelos Repositórios Arquivísticos Digitais Confiáveis RDC-Arq.

Para melhor visualização dos tópicos e dos itens inseridos na seção: Organização e Infraestrutura, eles estão escritos nas recomendações de checklist para medição e/ou certificação de confiabilidade para RDC-Arq com ênfase no acesso à Informação em cor azul.

O primeiro tópico inserido é denominado Política de Arquivo – número 1 - na seção: Organização e Infraestrutura. Como estamos trabalhando com arquivos permanentes, é fundamental que o arquivista tenha conhecimento das leis vigentes no Brasil assim, o tópico 1 é acompanhado das recomendações dos itens: 1.1 Estar em conformidade com a lei em vigência que dispõe sobre a política nacional dos arquivos públicos e privados, que no dia de hoje é Lei Nº 8.159, de 8 de janeiro de 1991, e do item: 2.2 Estar em conformidade com a da Lei Nº 12.527, Lei de Acesso à Informação, que regulamenta o direito constitucional de acesso às informações públicas.

Já no tópico quatro - Regulamentação de responsabilidades políticas de preservação – da seção organização e infraestrutura, é feita a recomendação do item 4.17, em que o RDC-Arq deve: Adotar a Curadoria Digital como um processo para o ciclo de vida dos documentos, e que a preservação seja parte desse processo.

Isso porque entendemos que o modelo do Ciclo de Vida proposto pela *Digital Curation Centre* subsidia as atividades realizadas pelo arquivista, visto que foi idealizado a partir de consultas com profissionais e especialistas, em todas as fases de

seu ciclo, o que garante uma sequência lógica desde o recebimento do documento, sua avaliação, seleção ou descarte dos dados, seguido de arquivamento e de ações subsequentes como a preservação, o armazenamento, o acesso, até a transformação ou reavaliação dos dados.

Todo processo de curadoria permite que os curadores identifiquem potenciais pontos fracos nas políticas do repositório ou ainda *gaps* na cadeia de arquivo, além de identificar as preocupações com a comunidade que poderiam fazer parte das rotinas de trabalho, bem como identificar outros interessados como fonte ou utilizadores.

Como citado anteriormente, ao se fazer arquivamento dos dados, não apenas se preservam esses dados, como se agregam valores a eles, pois ao arquivar o dado, visando sua preservação, poderá ser feita a adição de metadados administrativos, que descreverá a cadeia curadora possibilitará a transformação dos dados para outro formato e ainda permitirá que eles sejam colocados num contexto mais amplo, como também, para sua gestão, serão adicionadas anotações ou então serão desenvolvidos relacionamentos com outros conjuntos de dados.

Na seção quatro da Norma ISO 16363:2012 e da Resolução 39 do CONARQ, que tratam do Gerenciamento do Objeto/Documento Digital, o requisito acessibilidade é mencionado de modo superficial. Recomenda-se na Norma ISO, em seu item 4.2 Admissão: criação do pacote de arquivamento, subitem 4.2.7 “O repositório deve assegurar que as informações de conteúdo da *AIP* são compreensíveis para a sua comunidade-alvo no momento da criação da *AIP*”.

Do mesmo modo, a Resolução 39 do CONARQ, faz a seguinte referência à questão da acessibilidade: “Ter procedimentos para testar se os documentos são compreensíveis pela comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais)”.

Entendemos que a criação de um tópico que apresente recomendações mais específicas e precisas auxiliará o arquivista na criação de Repositório Arquivístico Digital Confiável ampliando o atendimento a diferentes comunidades-alvo.

Diante do exposto, para o desenvolvimento de um ambiente informacional digital devem ser considerados os diferentes cenários em que o usuário poderá acessá-lo, tais como situações em que o usuário tem dificuldades para ler, ouvir, ou compreender o

conteúdo que se apresenta no *site* do repositório digital, ou ainda em casos que o usuário faz uso de dispositivos que apresentam interfaces não convencionais. Outro fato a ser considerado é que o usuário poderá utilizar *browsers* ou sistemas operacionais diferentes como também poderá ter restrições no que se refere à velocidade de conexão com a Internet (FREIRE; FONTES, 2004)

Fundamentada nas análises da Norma ISO 16363:2012 e da Resolução 39 do CONARQ, apresentamos a inserção dos tópicos Acessibilidade e Usabilidade, com o intuito de que as barreiras de acesso possam ser minimizadas.

A inserção do tópico Acessibilidade - de número sete - é seguido da adição de seis itens, os quais elencamos a seguir: 7.1 Fornecer alternativas de não texto de modo que possa ser mudado para outro tipo de braile, discurso ou símbolos; 7.2 Fornecer alternativas sincronizadas para multimídia; 7.3 Criar várias maneiras de apresentação do índice; 7.4 Utilizar toda a funcionalidade que está disponível no teclado; 7.5 oferecer opção de modificação de tamanho de fonte e 7.6 Oferecer opção de modificação de fundo de página, para a certificação de confiabilidade de um Repositório Arquivístico Digital.

A partir de uma acessibilidade ótima, podemos ter também usabilidade que, segundo Silvino e Abrahão (2003, p. 13) “[...] é aferida pelos critérios ergonômicos e de funcionalidade e indica o grau de facilidade que a página oferece ao ser acessada”. Dentre os problemas mais recorrentes, no que tange à usabilidade, estão: interação usuário sistema ineficiente, dificuldade em acessar a informação desejada, interfaces complicadas e não intuitivas.

A inserção do tópico Usabilidade – de número 8 - é reiterada pela adição de 16 itens que facilitarão a interação do usuário com a interface de um Repositório Arquivístico Digital Confiável, descritos a seguir: 8.1 Exibir o nome do repositório e/ou logotipo ou slogan; 8.2 incluir um *link* da *homepage* para uma seção “Sobre Nós”; 8.3 Incluir um *link* “Fale Conosco”; 8.4 Empregar padrões e estilo com consistência; 8.5 Disponibilizar para os usuários uma caixa de busca; 8.6 Usar texto com muito contraste e cores de pano de fundo; 8.7 Evitar rolagem horizontal; 8.8 Usar raramente menus suspensos; 8.9 Informar se o *website* ficar paralisado ou não estiver funcionando; 8.10 Reduzir o tempo das respostas; 8.11 Oferecer cursor com comportamento padronizado;

8.12 Dar enfoque no conteúdo; 8.13 Possibilitar retorno à página principal; 8.14 Possibilitar o acesso às informações por meio de poucos comandos; 8.15 Utilizar mensagens de erro com vocabulário neutro e 8.16 Evitar caracteres especiais e adequar a fonte em relação ao assunto.

Buscamos, com a inserção do tópico usabilidade e dos 16 itens, aumentar a usabilidade do ambiente digital e, por conseguinte, a qualidade da ambiência, visto que, a usabilidade é que indica o grau de facilidade que uma página da *Web* oferece ao ser acessada. Dessa maneira, mais usuários terão acesso aos documentos custodiados pelos Repositórios Arquivísticos Digitais Confiáveis, uma vez que encontrarão páginas intuitivas, acessíveis e fluidas para satisfazer suas necessidades informacionais.

Nesse momento, vale destacar que ferramentas estão disponíveis na *Web* com a proposta de avaliar a acessibilidade, como é o caso da ferramenta DaSilva<sup>3</sup> o primeiro avaliador de acessibilidade em português para *Websites* e o avaliador de usabilidade e desempenho de *Websites ErgoList*<sup>4</sup>.

---

<sup>3</sup> Disponível em: <<http://www.dasilva.org.br/>>

<sup>4</sup> Disponível em: <<http://labiutil.inf.ufsc.br/ergolist/>>

## 7 CONSIDERAÇÕES FINAIS

As Instituições Arquivísticas são as guardiãs dos registros dos atos de instituições ou famílias que foram registrados por pessoas físicas, assim, são ambientes de guarda e custódia dos documentos que são tratados como objeto central de diferentes áreas. Além de uma prova do tempo, uma consequência proveniente de um ato ou função que pode influenciar ou determinar relações sociais ou até mesmo a vida de pessoas.

Em virtude das novas demandas da sociedade, Instituições Arquivísticas estão sendo desafiadas a constantes atualizações no uso das Tecnologias de Informação e Comunicação, pois os ambientes digitais que abarcam a produção de documentos gerados em excepcional quantidade e em diferentes suportes exigem o crescimento de Arquivos Digitais com acervos híbridos e confiáveis, bem como a otimização de seus serviços.

Borko (1968), ao discorrer sobre a Ciência da Informação, à qual a Arquivologia está relacionada, pontua que é a disciplina que investiga as propriedades e o comportamento da informação, as forças que governam o fluxo da informação e os meios de processamento da informação para a sua ótima acessibilidade e usabilidade.

Nessa perspectiva, os Repositórios Arquivísticos Digitais se configuram como ambientes que promovem a mediação cultural e o acesso à informação. Assim, podemos constatar o quanto as Tecnologias de Informação e Comunicação (TIC) e a ambiência digital geram medidas eficazes para que os documentos digitais sejam disponibilizados, encontrados, utilizados e reutilizados, tornando conhecidas as riquezas culturais e assegurada sua conservação.

O direito à informação bem como o acesso à informação confiável é uma premissa para Repositórios Arquivísticos Digitais. Nesse cenário, analisar o conjunto de atributos essenciais para a implantação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq), a partir das diretrizes da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*) e da Resolução 39 do CONARQ “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq” para criação de um conjunto de

recomendações para a certificação de Repositórios Arquivísticos Confiáveis se constituiu como o escopo deste trabalho.

Assim, os objetivos apresentados na pesquisa foram atendidos. Porém, para que isso fosse possível, foi montado um arcabouço com o objetivo geral, peculiar a todos os capítulos da tese. Já os objetivos específicos foram atendidos por meio de estudos realizados e estruturados em discussões a cada capítulo.

Pudemos observar que os estudos dos Repositórios Arquivísticos Digitais Confiáveis ainda são poucos na vertente da certificação e do estudo da experiência do usuário, pois as discussões, na área da Ciência da Informação, são mais frequentes no que se refere à Curadoria Digital e à utilização de *software*.

Dessa maneira, o primeiro objetivo específico, **Descrever o papel do arquivista como Usuário Chave, na construção de RDC-Arq**, foi atendido pelos capítulos 2 e 3. No capítulo 2, foi desenvolvida a fundamentação teórica dos termos: documento, documento arquivístico, Documento Digital e Curadoria Digital. No capítulo 3, o trabalho do arquivista foi contextualizado. O direito à informação e a legislação referenciou o acesso como direito fundamental de todo cidadão e o papel do arquivista como parte integrante na construção de Repositórios Arquivísticos Digitais Confiáveis.

Além disso, no Capítulo 3, a Lei de Acesso à Informação foi contextualizada no cenário Internacional e Nacional a partir da criação da LAI nº 12.527 que foi regulamentada e passou a vigorar em novembro 2012. Ressalta-se que a partir dessa data, acentuou-se o debate sobre boas práticas arquivísticas para a otimização e ampliação do acesso à informação, dando maior visibilidade ao arquivista como profissional da informação que assegurará o acesso à informação, e que, diante das tecnologias presentes, seu papel na sociedade necessita ser redesenhado para que possa atender seu público-alvo de maneira eficiente.

Também foram considerados, no capítulo, os principais conceitos sobre o profissional arquivista à frente de arquivos que se revelaram como sistemas de informações complexos, localizados na ambiência digital e com acervos híbridos, pois custodiam documentos analógicos, digitais e nascidos digitais. Portanto urgem serem confiáveis, garantindo a preservação em longo prazo e o acesso, conforme

determinado por lei, à sua comunidade-alvo, composta por cidadãos que querem satisfazer suas necessidades informacionais de maneira fácil, rápida e segura.

Nesse contexto, o Arquivista deve assumir o papel de Usuário-Chave diante de uma equipe multidisciplinar na criação de sistemas informacionais onde serão criados os Repositórios. Para que o Arquivista possibilite e/ou facilite o acesso às informações arquivísticas frente à nova demanda, apresentamos o quadro com a sistematização das ações que esse profissional deve considerar, além do tratamento documental que já é feito.

O segundo objetivo específico, **identificar as diretrizes da Resolução 39 – “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq” e da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*), com foco na certificação de RDC-Arq**, foi respondido pelos capítulos 4 e 5. No capítulo 4, foi desenvolvida a fundamentação teórica sobre os Repositórios Digitais, Repositórios Digitais Confiáveis e Repositórios Arquivísticos Digitais Confiáveis. Já no capítulo 5, a análise dos requisitos indicados pela Norma ISO e pela Resolução 39 permitiu a identificação dos elementos necessários para a construção de Repositórios Digitais Confiáveis. Vale apontar que a Norma ISO faz a certificação de qualquer Repositório Digital e a Resolução do CONARQ efetua a criação de um repositório, porém somente a ISO poderá certificá-lo.

O terceiro objetivo específico, **Categorizar as diretrizes da Resolução 39, “Diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis RDC-Arq” e da Norma ISO 16363:2012 (*Space data and information transfer systems -- Audit and certification of trustworthy digital repositories*), com foco na certificação de RDC-Arq**, e o quarto objetivo específico **Compatibilizar/Cotejar os requisitos indicados pela Norma ISO e pela Resolução do CONARQ**, foram respondidos pelo capítulo 5.

As diretrizes propostas pela Norma ISO e pela Resolução 39 do CONARQ foram sistematizadas em quadros, para uma melhor visualização do cotejamento entre as duas recomendações.

Também foram feitos quadros distintos para os itens convergentes e não convergentes dentro das categorias contempladas.

No procedimento deste estudo, pudemos verificar que a Norma ISO 16363:2012 apresenta maior granularidade o que a torna mais específica. Os itens da Norma ISO que não são contemplados na Resolução 39, dizem respeito às políticas que os repositórios devem possuir. No entanto, como a Resolução é direcionada aos Repositórios Arquivísticos Digitais, tais repositórios fazem parte do Sistema Nacional de Arquivos – SINAR - órgão que tem como uma de suas finalidades implementar a política nacional de arquivos públicos e privados. Destaque-se que os repositórios arquivísticos brasileiros da esfera pública já possuem políticas definidas.

As recomendações do CONARQ que não são contempladas pela Norma ISO, são específicas para Repositórios do domínio Arquivístico o que lhes confere especificidades documentais e cumprimento de requisitos que assegurem o armazenamento e o acesso por um longo ou permanente prazo, visto que custodiam registros únicos, isto é, fontes primárias de informação.

Sendo a função básica dos arquivos a disponibilização das informações que estão sob sua custódia para o acesso, e pelo fato de a ênfase deste estudo também estar no acesso às informações, o capítulo 5 traz a categorização do termo Acesso/Access nos textos da Norma ISO 16363:2012 e na Resolução 39 do CONARQ. A partir dessa categorização, verificou-se a preocupação das Diretrizes quanto ao acesso às informações.

Também foram identificadas e categorizadas as terminologias referentes a ações e elementos que viabilizam o acesso a um maior número de pessoas, ou seja, *Acessibilidade/Accessibility*; *Comunidade Alvo/Designated Community*; *Curadoria Digital/Digital Curation*; *Interface*; *Preservação/Preservation*; *Preservada/Preserved*; *Usabilidade/Usability*. *Usuário(s)/User(s)*. Para essa categorização, tomou-se como base os requisitos necessários que o Repositório Digital deverá contemplar para que seja considerado confiável.

Essa categorização serviu como subsídio para o cumprimento do quinto e último objetivo específico, **Sistematizar convergências para identificação dos requisitos com ênfase no acesso à informação em Repositórios Arquivísticos Digitais**

Confiáveis, que foi respondido no sexto capítulo. Nele apresentou-se um conjunto de informações (*Checklist*) dirigidas aos Arquivistas que atuam em Repositórios Digitais e desejam verificar os requisitos necessários para avaliação de confiabilidade do Repositório Digital ou ainda guiar o profissional da informação na coleta de requisitos para a certificação de confiabilidade do repositório.

Como a ênfase do trabalho se dá no acesso à informação, além dos requisitos sugeridos pela Norma ISO 16363:2012 e da Resolução 39 do CONARQ, foi adicionado a esse conjunto de informações um requisito pertinente à Legislação vigente no Brasil, um requisito pertinente à Curadoria Digital, visto que o DCC disponibiliza *Checklist* para cada fase do Ciclo de Vida dos Dados, apresentado no capítulo 4.

Foi incluído o item Acessibilidade com seis recomendações, para que o Repositório atinja um maior número de usuários. Nesse momento, faz-se importante ressaltar os apontamentos sobre o usuário feitos por Baranauskas e Mantoan (2001, p. 14), ao ponderarem sobre os aspectos da acessibilidade nas páginas da Web, consideram “[...] a variedade de contextos de interação que podem estar relacionadas a diferentes tipos e situações dos usuários com o sem deficiência [...]” e complementam que “Entre esses cidadãos encontram-se também a população idosa.” O que também é compartilhado por Winckler e Pimenta (2002, p. 2), quando pontuam que “[...] recomendações para acessibilidade não limita a utilização da interface apenas à pessoa com necessidades especiais”.

Também foi acrescentado o item Usabilidade com dezesseis requisitos, pois a interface é a porta de entrada para que as necessidades informacionais do público alvo sejam atendidas. Assim, faz-se necessária uma interface adequada ao sistema, bem como à satisfação do usuário.

A proposição das recomendações se encontra no Quadro 11.

Das 202 recomendações propostas, disponibilizou-se, no Apêndice 1, um subconjunto de 55 recomendações, denominadas de Recomendações Simplificadas para Certificação um Repositório Arquivístico Digital Confiável, que possibilitará ao Arquivista um *Checklist* para uma visão geral da confiabilidade de seu Repositório.

Assim, comprova-se a tese de que os requisitos que compõem a Norma ISO e a Resolução 39 do Conarq são elementos essenciais para a implantação de Repositórios

Arquivísticos Digitais Confiáveis (RDC-Arq) no que diz respeito ao uso e ao acesso à informação por conectar serviços e coleções visando às comunidades-alvo.

Também foi validada a hipótese dessa pesquisa, e, por meio da análise das normas ISO e Resolução 39, foram identificados os requisitos essenciais para a implantação de um Repositório Arquivístico Digital Confiável.

No final de nosso estudo, as verificações realizadas nos conduziram a reflexões sobre o papel dos Arquivistas, frente à demanda de criação de Repositórios Arquivísticos Digitais Confiáveis, ao trabalho em equipes multidisciplinares, ao conhecimento sobre o processo de Curadoria Digital e conseqüentemente com o Ciclo de Vida dos Dados. Sendo isso, uma imposição do mercado de trabalho, considerando que o ciberespaço rompe a distância física, temporal e as barreiras geográficas. O novo profissional da informação está capacitado para incorporar funções de responsável pela concepção, montagem e supervisão da apresentação e exposição de documentos confiáveis e também pelo catálogo nos meios digitais?

Tais indagações merecem atenção de profissionais da Ciência da Informação, uma vez que, a expertise do arquivista proporcionará e/ou facilitará o acesso de um grande número de pessoas às informações arquivísticas, pois os dados gerados estarão custodiadas nos acervos de Repositórios Arquivísticos Digitais. Haverá assim um ganho no conhecimento, pois dificilmente tais informações seriam acessadas por um número de pessoas que potencialmente é ampliado pelas TIC. Portanto é condição *sine qua non* que essas informações preservem sua integridade e confiabilidade.

A partir dessas delimitações, projetamos para novos trabalhos o acompanhamento da aplicação das recomendações para mensurar a confiabilidade nos repositórios arquivísticos digitais com ênfase no acesso, e o estudo dos currículos dos cursos de arquivologia no Brasil, com o intuito de verificar se o profissional está sendo formado para atender a demanda social na ambiência digital e assim validar as atividades elaboradas nesta pesquisa.

## REFERÊNCIAS

ABBAGNANO, Nicola. **Dicionário de Filosofia**. 2. ed. São Paulo: Martins Fontes, 1998.

ALVES, Ivone et al. **Dicionário de terminologia arquivística**. Lisboa: Instituto da Biblioteca Nacional e do Livro, 1993.

ALVES, Virginia Barbara Aguiar. Open archives: via verde ou via dourada. **Ponto de Acesso**, Salvador, v. 2, n. 2, p. 127-137, ago./set. 2008. Disponível em: <<https://portalseer.ufba.br/index.php/revistaici/article/view/1780>>. Acesso em: 13 jan. 2014.

ANDERS CHYDENIUS FOUNDATION. **The world's first freedom of information act: Anders Chydenius' legacy today**. Kokkola: Anders Chydenius Foundation, 2006.

ANNA, José Santa; CAMPOS, Suelen de Oliveira; CALMON, Maria Aparecida de Mesquita. Diferenças e semelhanças entre arquivos e bibliotecas: o profissional da informação em evidência. **Biblos**, Rio Grande, v. 29, n. 1, p. 95-113, 2015.

ARDENGHI, Régis Schneider. Direito à vida privada e direito à informação: colisão de direitos fundamentais. **Revista da ESMESC**, Santa Catarina, v. 19, n. 25, 2012. Disponível em: <<http://dx.doi.org/10.14295/revistadaesmesec.v19i25.57>>. Acesso em: 18 set. 2015.

ARQUIVO NACIONAL (BRASIL). **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005.

ASSOCIATION OF RESEARCH LIBRARIES. **To stand the test of time: long-term stewardship of digital data sets in science and engineering**. Arlington: National Science Foundation, 2006.

BANAT-BERGER, Françoise; DUPLOUY, Laurent; HUC, Claude. **L'archivage numérique à long terme: les débuts de la maturité**. Paris: La Documentation Française, 2009.

BANISAR, David. Freedom of information around the world 2006: a global survey of access to government information laws. [S.l.]: **Privacy International**, 2006.

BARANAUSKAS, Maria Cecilia Calani; MANTOAN, Maria Teresa Eglér. Acessibilidade em ambientes educacionais: para além das guidelines. **Educação Temática Digital**, Campinas, v. 2, n. 2, p. 13-22, 2001. Disponível em: <<http://dx.doi.org/10.20396/etd.v2i2.1068>>. Acesso em: 23 set. 2016.

BARROS, Dirlene Santos; NEVES, Dulce Amélia de Brito. Arquivo e memória: uma relação indissociável. **TransInformação**, Campinas, v. 21, n. 1, p. 55-61, jan./abr. 2009.

BEAGRIE, Neil. The Digital Curation Centre. **Learned Publishing**, v. 17, n. 1, p. 7-9, jan. 2004.

BELLOTTO, Heloísa Liberalli. Arquivologia: objetivos e objetos. **Arquivo**: boletim histórico e informativo, v. 10, n. 2, p. 81-83, 1989.

BELLOTTO, Heloísa Liberalli. Patrimônio documental e ação educativa nos arquivos. **Ciências & Letras**, Porto Alegre, n. 27, p. 151-166, jan./jun. 2000.

BELLOTTO, Heloísa Liberalli. **Como fazer análise diplomática e análise tipológica de documento de arquivo**. São Paulo: Arquivo do Estado, 2002.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes**: tratamento documental. 4. ed. Rio de Janeiro: Fundação Getúlio Vargas, 2004.

BELLOTTO, Heloísa Liberalli. **Arquivos**: estudos e reflexões. Belo Horizonte: Editora UFMG, 2014.

BORKO, Harold. Information Science: what is it? **American Documentation**, Washington, v. 19, n. 1, p. 3-5, 1968.

BRADLEY, Kevin; LEI, Junran; BLACKALL, Chris. **Towards an open source repository and preservation system**. Paris: UNESCO, 2007.

BRASIL. Congresso Nacional. Lei nº 5.296, de 2 de dezembro de 2004. Que estabelece normas gerais e critérios básicos para a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida, e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 3 dez. 2004. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2004/decreto/D5296.htm](http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/D5296.htm)>. Acesso em: 17 out. 2012.

BRASIL. Congresso Nacional. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 18 nov. 2011. Disponível em: <[https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm)>. Acesso em: 25 nov. 2012.

BRASIL. Constituição Federal (1988). **Constituição da República Federativa do Brasil**. Promulgada em 5 out. 1988. Brasília, DF, Senado Federal, 5 out. 1988.

BRASIL. Congresso Nacional. Decreto nº 4.073, de 3 de janeiro de 2002. Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 3 jan. 2002.

Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto/2002/d4073.htm](http://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm)>. Acesso em: 25 nov. 2012.

CAMARGO, Liriane Soares de Araújo de. **Metodologia de desenvolvimento de ambientes informacionais digitais a partir dos princípios da Arquitetura da Informação**. 2010. 287 f. Tese (Doutorado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2010.

CAMARGO, Liriane Soares de Araújo de; VIDOTTI, Silvana Aparecida Borsetti Gregório. Arquitetura da informação para repositórios científicos digitais. In: SAYÃO, Luís Fernando et al. (Org.). **Implantação e gestão de repositórios institucionais: políticas, memória, livre acesso e preservação**. Salvador: EDUFBA, 2009. p. 55-82.

CANAVAGGIO, Perrine; BALAFREJ, Alexandra. **Vers un droit d'accès a l'information publica au Maroc: etude comparative avec les normes et les meilleures pratiques dans le monde**. Maroc: UNESCO, 2011.

CARVALHO, Priscila Freitas de; CIANCONI, Regina de Barros. A gestão de informações arquivísticas sob a vigência da Lei de Acesso à Informação em ambiente universitário. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 16., 2015, João Pessoa. **Anais...** João Pessoa: UFPB, 2015.

CASTELLS, Manuel. Inovação, liberdade e poder na era da utopia tecnológica. In: MORAES, Dênis de (Org.). **Sociedade midiaticizada**. Rio de Janeiro: Mauad X, 2006. p. 225-231.

CASTILLO RUÍZ, José. Hacia una nueva definición de patrimonio histórico? In: **PH Boletín del Instituto Andaluz del Patrimonio Histórico**, Sevilla, v. 4, n. 16, p. 101-106, 1996.

CENTRE FOR LAW AND DEMOCRACY. **Global right to information rating**. 2016. Disponível em: <<http://www.rti-rating.org/>>. Acesso em: 28 set. 2016.

CHAGAS, Mário. Cultura, patrimônio e memória. In: CONGRESSO INTERNACIONAL DE ARQUIVOS, BIBLIOTECAS, CENTROS DE DOCUMENTAÇÃO E MUSEUS, 1., 2002, São Paulo. **Anais...** São Paulo: Imprensa Oficial do Estado, 2002. p. 135-150.

COELHO, Teixeira. **Dicionário crítico de política cultural: cultura e imaginário**. 2. ed. São Paulo: Iluminuras, 1999.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: CONARQ, 2012.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Glossário: documentos arquivísticos digitais**. Rio de Janeiro: CONARQ, 2014a. Disponível em:

<[http://www.conarq.gov.br/images/ctde/Glossario/2014ctdeglossario\\_v6\\_public.pdf](http://www.conarq.gov.br/images/ctde/Glossario/2014ctdeglossario_v6_public.pdf)>. Acesso em: 2 abr. 2014.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 39, de 29 de abril de 2014. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 30 abr. 2014b. Disponível em: <<http://www.conarq.arquivonacional.gov.br/legislacao/resolucoes-do-conarq/281-resolucao-n-39,-de-29-de-abril-de-2014.html>>. Acesso em: 3 jun. 2014.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 43, de 04 de setembro de 2015. **Diário Oficial da União**, Poder Executivo, Brasília, DF, 8 set. 2015. Disponível em: <<http://www.conarq.arquivonacional.gov.br/legislacao/resolucoes-do-conarq/335-resolucao-n-43,-de-04-de-setembro-de-2015.html>>. Acesso em: 15 set. 2015.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS. **Reference model for an Open Archival Information System (OAIS): recommended practice CCSDS 650.0-M-2**. Washington, DC: CCSDS, 2012. Disponível em: <<https://public.ccsds.org/pubs/650x0m2.pdf>>. Acesso em: 15 mar. 2016.

CONTROLADORIA GERAL DA UNIÃO (Brasil). **Relatório sobre a implementação da Lei nº 12.527: Lei de Acesso à Informação**. Brasília: Poder Executivo Federal, 2014.

COOK, Michael. Liberdade de informação: influência sobre a prática profissional em gestão de arquivos. **Acervo**, Rio de Janeiro, v. 24, n. 1, p. 245-256, jan./jun. 2011.

CORNELL UNIVERSITY. **Digital preservation management: implementing short-term strategies for long-term problems (digital preservation management workshops and tutorial)**. Cambridge, MA: MIT Libraries, 2014. Disponível em: <[http://www.dpworkshop.org/dpm-eng/eng\\_index.html](http://www.dpworkshop.org/dpm-eng/eng_index.html)>. Acesso em: 7 mar. 2016.

COSTA, Marco Antonio Ferreira da; COSTA, Maria de Fátima Barrozo da. **Metodologia da pesquisa: conceitos e técnicas**. Rio de Janeiro: Interciência, 2001.

CRUZ, Emília Barroso. **Manual de gestão de documentos**. Belo Horizonte: Secretaria de Estado de Cultura de Minas Gerais, 2013.

CRUZ MUNDET, José Ramón. **Manual de archivística**. 3. ed. Madrid: Fundación Germán Sánchez Rupérez, 1994.

DERRIDA, Jacques. **Mal de arquivo: uma impressão Freudiana**. Rio de Janeiro: Relume Dumará, 2001.

DIGITAL CURATION CENTRE. **DCC Curation Lifecycle Model**. 2008. Disponível em: <<http://www.dcc.ac.uk/resources/curation-lifecycle-model>>. Acesso em: 15 set. 2015.

DIGITAL CURATION CURRICULUM. **About DigCCurr I**. 2006. Disponível em: <<https://ils.unc.edu/digccurr/aboutI.html>>. Acesso em: 15 set. 2015.

DIGITAL PRESERVATION COALITION. **Digital Preservation Handbook**. 2008. Disponível em: <<http://www.dpconline.org/advice/preservationhandbook>>. Acesso em: 15 set. 2015.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação**. São Paulo: Revista dos Tribunais, 1990.

DURANTI, Luciana. Registros documentais contemporâneos como provas de ação. **Estudos Históricos**, v. 7, n. 13, p. 49-64, 1994.

EDMONDSON, Ray. **Memória do mundo**: diretrizes para salvaguarda do patrimônio documental. Paris: UNESCO, 2002.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário Aurélio da língua portuguesa**. Curitiba: Positivo, 2009.

FERREIRA, Miguel. **Introdução à preservação digital**: conceitos, estratégias e atuais consensos. Guimarães: Escola de Engenharia da Universidade do Minho, 2006.

FONSECA, Maria Cecília Londres. **O patrimônio em processo**: trajetória da política federal de preservação no Brasil. Rio de Janeiro: URFJ, 1997.

FONTAL MERILLAS, Olaia. **La educación patrimonial**: teoría y práctica para el aula, el museo e internet. Gijón: Trea, 2003.

FREEDOM INFO. **The access to information bill in Brazil**. 2013. Disponível em: <<http://www.freedominfo.org/regions/latin-america/brazil/>>. Acesso em: 18 ago. 2016.

GARBINATTO, Valeska. Ensino de história e patrimônio histórico: pontes para construção da memória e cidadania. **Ciências & Letras**, Porto Alegre, n. 27, p. 37-48, jan./jun. 2000.

GARCÍA BELSUNCE, César Augusto. Legislação sobre proteção do patrimônio documental e cultural. **Acervo**, Rio de Janeiro, v. 1, n. 1, p. 29-40, jan./jun. 1986.

GARRETT, John; WATERS, Donald. **Preserving digital information**: report of the task force on archiving of digital information. Washington, D.C.: Commission on Preservation and Access: Research Libraries Group, 1996.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

GONÇALEZ, Paula Regina Ventura Amorim. **Disseminação da informação nos websites das instituições de patrimônio público**: um enfoque nos arquivos permanentes. 2013. 144 f. Dissertação (Mestrado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2013.

GONÇALVES, José Reginaldo Santos. Monumentalidade e cotidiano: os patrimônios culturais como gênero do discurso. In: OLIVEIRA, Lúcia Lippi (Org.). **Cidade: história e desafios**. Rio de Janeiro: Fundação Getúlio Vargas, 2002. cap. 6.

GRÁCIO, José Carlos Abbud. **Preservação digital na gestão da informação**: um modelo processual para as instituições de ensino superior. 2011. 223 f. Tese (Doutorado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2011.

GUTIÉRREZ MUÑOZ, César. El documento archivístico. In: GUTIÉRREZ MUÑOZ, César. **Descripción de documentos archivísticos**. [Lima]: Instituto Riva-Agüero: Pontífica Universidad Católica del Perú, 1982.

HARVEY, Ross. **Digital curation**: a how-to-do-it manual. New York: Neal-Schuman Publishers, 2010.

HAYES, Helen. Digital repositories: helping universities and colleges. In: HAYES, Helen (Ed.). **JISC Briefing Paper**. England: [s.n.], 2005.

HEDSTROM, Margaret. Digital preservation: a time bomb for digital libraries. **Computer and the Humanities**, n. 31, p. 189-202, 1998. Disponível em: <<https://doi.org/10.1023/A:1000676723815>>. Acesso em: 1 fev. 2016.

HEERY, Rachel; ANDERSON, Sheila. **Digital repositories review**. [S.l.]: UKOLN: Arts and Humanities Data Service, 2005.

HEREDIA HERRERA, Antonia. **Archivística general**: teoría y práctica. 6. ed. Sevilla: Diputación Provincial de Sevilla, 1993.

HIGGINS, Sarah. The DCC Curation Lifecycle Model. **International Journal of Digital Curation**, v. 3, n. 1, p. 134-140, 2008. Disponível em: <<https://doi.org/10.2218/ijdc.v3i1.48>>. Acesso em: 12 jan. 2014.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro: Objetiva, 2001.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro: Objetiva, 2004.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro: Objetiva, 2007.

HOUGHTON, Bernadette. Trustworthiness: self-assessment of an Institutional Repository against ISO 16363-2012. **D-Lib Magazine**, Australia, v. 21, n. 3-4, mar./abr. 2015. Disponível em: <<https://doi.org/10.1045/march2015-houghton>>. Acesso em: 3 mar. 2016.

IACOVINO, Livia. Os arquivos como arsenais de responsabilidade. In: EASTWOOD, Terry; MACNEIL, Heather (Org.). **Correntes atuais do pensamento arquivístico**. Belo Horizonte: Editora UFMG, 2016. cap. 9.

INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL. **Patrimônio material**. 2014. Disponível em: <<http://portal.iphan.gov.br/pagina/detalhes/276>>. Acesso em: 15 set. 2015.

INSTITUTO PORTUGUÊS DE QUALIDADE. **Norma 4438-1**: Informação e documentação: gestão de documentos de arquivo. Lisboa, 2005.

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA. **Sobre os repositórios digitais**. [20--]. Disponível em: <<http://www.ibict.br/informacao-para-ciencia-tecnologia-e-inovacao%20/repositorios-digitais>>. Acesso em: 10 dez. 2014.

INTERNATIONAL COUNCIL ON ARCHIVES. **Declaração universal sobre arquivos**. 2010. Disponível em: <<http://www.ica.org/en/universal-declaration-archives>>. Acesso em: 30 jul. 2012.

INTERNATIONAL FEDERATION OF LIBRARY ASSOCIATIONS AND INSTITUTIONS. **Functional Requirements for Bibliographic Records**: final report. As amended and corrected through Feb. 2009. Munich: K.G. Saur Verlag, 1998.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363:2012**: Space data information transfer systems -- Audit and certification of trustworthy digital repositories. Genebra, 2012.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. **Diretrizes do produtor**: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. [S.l. : s.n.], [2007?]. Disponível em: <<http://www.conarq.arquivonacional.gov.br/publicacoes-ctde/27-diretrizes-do-produtor-e-do-preservador.html>>. Acesso em: 9 ago. 2014.

JARDIM, José Maria. **Sistemas e políticas públicas de arquivos no Brasil**. Niterói: EDUFF, 1995.

KÖCHE, José Carlos. **Fundamentos da metodologia científica**: teoria da ciência e prática da pesquisa. 21. ed. Petrópolis: Vozes, 2003.

KURAMOTO, Hélio. Informação científica: proposta de um novo modelo para o Brasil. **Ciência da Informação**, Brasília, v. 35, n. 2, p. 91-102, maio/ago. 2006.

LAGE, Maria Otília Pereira. **Abordar o patrimônio documental**: territórios, práticas e desafios. Guimarães: NEPS, 2002.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 4. ed. São Paulo: Atlas, 2001.

LAVOIE, Brian. **The Open Archival Information System (OAIS) reference model: introductory guide**. Dublin, Ohio: Digital Preservation Coalition, 2004.

LOPES, Luís Carlos. **A gestão da informação: as organizações, os arquivos e a informação aplicada**. Rio de Janeiro: Arquivo Público do Estado do Rio de Janeiro, 1997.

LYMAN, Peter. Archiving the world wide web. **Council on Library and Information Resources**, 2002. Disponível em: <<https://www.clir.org/pubs/reports/pub106/web.html>>. Acesso em: 27 maio 2015.

MALTA, Cristóvão Piragibe Tostes; LEFÈVRE, Júlia Brotero. **Dicionário jurídico**. 5. ed. Rio de Janeiro: Edições Trabalhistas. 1987.

MARCONDES, Carlos Henrique. Representação e economia da informação. **Ciência da Informação**, São Paulo, v. 30, n. 1, p. 61-70, jan./abr. 2001.

MARCONDES, Carlos Henrique; SAYÃO, Luís Fernando. Introdução: repositórios institucionais e livre acesso. In: SAYÃO, Luís Fernando et al. (Org.). **Implantação e gestão de repositórios institucionais: políticas, memória, livre acesso e preservação**. Salvador: EDUFBA, 2009. p. 9-21.

MARCONDES, Carlos Henrique et al. Ontologias como novas bases de conhecimento científico. **Perspectivas em Ciência da Informação**, v. 13, n. 3, p. 20-30, set./dez. 2008. Disponível em: <<http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/206>>. Acesso em: 17 jul. 2015.

MÁRDERO ARELLANO, Miguel Ángel. **Critérios para a preservação digital da informação científica**. 2008. 358 f. Tese (Doutorado em Ciência da Informação)- Universidade de Brasília, Brasília, 2008.

MÁRDERO ARELLANO, Miguel Ángel. Preservação de documentos digitais. **Ciência da Informação**, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004.

MASSON, Sílvia Mendes. Os repositórios digitais no âmbito da sociedade informacional. **Prisma.com**. Porto, n. 7, p. 105-152. 2008. Disponível em: <<http://revistas.ua.pt/index.php/prismacom/article/view/679>>. Acesso em: 10 mai. 2015.

MCGOVERN, Nancy. A digital decade: where have we been and where are we going in digital preservation? **RLG DigiNews**, v. 11, n. 1, abr. 2007. Disponível em: <<http://deepblue.lib.umich.edu/handle/2027.42/60441>>. Acesso em: 17 mar. 2015.

MENDEL, Toby. **Liberdade de informação: um estudo de direito comparado**. 2. ed. Brasília: UNESCO, 2009.

MUELLER, Suzana Pinheiro Machado. Formação profissional e educação continuada: que profissional devemos ser? In: SIMPÓSIO BRASIL-SUL DE INFORMAÇÃO, 1996, Londrina. **Anais...** Londrina: EDUEL, 1996. p. 253-272.

MUELLER, Suzana Pinheiro Machado; CARIBÉ, Rita de Cássia do Vale. Comunicação científica para o público leigo: história breve. **Informação & Informação**, Londrina, v. 15, n. esp. 1, p. 13-20, 2010. Disponível em: <[http://dx.doi.org/10.5433/1981-8920.2010v15n1\\_espp13](http://dx.doi.org/10.5433/1981-8920.2010v15n1_espp13)>. Acesso em: 14 fev. 2013.

MURGUIA, Eduardo Ismael. Percepções e aproximações do documento na historiografia, documentação e ciência da informação. **InCID: Revista de Ciência da Informação e Documentação**, Ribeirão Preto, v. 2, n. 2, p. 42-53, jul./dez. 2011. Disponível em: <<http://dx.doi.org/10.11606/issn.2178-2075.v2i2p42-53>>. Acesso em: 15 nov. 2014.

NATIONAL ARCHIVES OF SWEDEN. **Digital Preservation in archives**: overview of current Research and practices. [S.l.]: LDB-enheten, 2005. Disponível em: <[http://www.ltu.se/cms\\_fs/1.83844!/file/Digital%20Preservation %20in%20Archives.pdf](http://www.ltu.se/cms_fs/1.83844!/file/Digital%20Preservation%20in%20Archives.pdf)>. Acesso em: 22 abr. 2015.

NATIONAL LIBRARY OF AUSTRALIA. **Guidelines for the preservation of digital heritage**. [S.l.]: UNESCO, 2003. Disponível em: <<http://unesdoc.unesco.org/images/0013/001300/130071e.pdf>>. Acesso em: 23 set. 2015.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris: [s.n.], 2009.

OWEN, John Mackenzie. Preserving the digital heritage: roles and responsibilities for heritage repositories. In: LUSENET, Yola de; WINTERMANS, Vincent (Ed.). **Preserving the digital heritage: principles and policies**. The Hague: UNESCO, 2007.

RAMALHO, José Carlos. Repositórios digitais. In: TERTÚLIA EM INTELIGÊNCIA ARTIFICIAL, 3., 2007, Porto. **Apresentações...** Porto: Universidade do Minho, 2007.

RIBEIRO, Fernanda. Arquivos-memória-história: algumas notas para reflexão. **População e Sociedade**, Porto, n. 9, p. 19-21, 2002.

ROCHA, Claudia Lacombe et al. **Gestão arquivística de documentos eletrônicos**. Rio de Janeiro: Arquivo Nacional, 2004.

RONDINELLI, Rosely Curi. **O conceito do documento arquivístico frente à realidade digital**: uma revisitação necessária. 2011. 270 f. Tese (Doutorado em Ciência da Informação)-Universidade Federal Fluminense, Niterói, 2011.

RONDINELLI, Rosely Curi. **O documento arquivístico ante a realidade digital**: uma revisão conceitual necessária. Rio de Janeiro: Editora FGV, 2013.

ROSS, Seamus. Digital preservation, archival Science and methodological foundation for digital libraries. In: EUROPEAN CONFERENCE ON DIGITAL LIBRARIES, 11., 2007, Budapeste. **Anais...** Budapeste: Springer, 2007.

ROUSSEAU, Jean-Yves; COUTURE, Carol. **Os fundamentos da disciplina arquivística**. Lisboa: Publicações Dom Quixote, 1994.

SAGREDO FERNÁNDEZ, Félix; IZQUIERDO ARROYO, José María. Reflexiones sobre documento: palabra/objeto (I). **Boletín Millares Carlo**, n. 5, p. 161-197, 1982.

SANTOS, Cecilia Rodrigues. Novas fronteiras e novos pactos para o patrimônio cultural. **São Paulo em Perspectiva**, São Paulo, v.15, n. 2, p. 43-48, 2001.

SANTOS, Henrique Machado dos; FLORES, Daniel. Repositórios digitais confiáveis para documentos arquivísticos: ponderação sobre a preservação em longo prazo. **Perspectivas em Ciência da Informação**, v. 20, n. 2, p. 198-218, abr./jun. 2015. Disponível em: <<http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2341>>. Acesso em: 23 abr. 2016.

SANTOS, José Luiz dos. **O que é Cultura?** São Paulo: Brasiliense, 2006.

SANTOS, Plácida Leopoldina Ventura Amorim da Costa. As novas tecnologias na formação do profissional da informação. In: VALENTIM, Marta Lúcia Pomim (Org.). **A formação do profissional da informação**. São Paulo: Polis, 2002. p. 103-116.

SANTOS, Plácida Leopoldina Ventura Amorim da Costa; VIDOTTI, Silvana Aparecida Borsetti Gregório. Perspectivismo e tecnologias de informação e comunicação: acréscimos à Ciência da Informação? **DataGramaZero: Revista de Ciência da Informação**, v. 10, n. 3, p. 1-12, jun. 2009. Disponível em: <[http://www.dgz.org.br/jun09/Art\\_02.htm](http://www.dgz.org.br/jun09/Art_02.htm)>. Acesso em: 8 jul. 2009.

SANTOS, Thayse Natália Cantanhede. **Curadoria digital: o conceito no período de 2000 a 2013**. 2014. 165 f. Dissertação (Mestrado em Ciência da Informação)- Universidade Estadual de Brasília, Brasília, 2014.

SARACEVIC, Tefko. Interdisciplinary nature of Information Science. **Ciência da Informação**, Brasília. v. 24, n. 1, p. 36-41, 1997.

SARGENTINI, Vanice Maria Oliveira. Objetos da análise do discurso. In: SARGENTINI, Vanice Maria Oliveira; GREGOLIN, Maria do Rosário (Org.). **Análise do discurso: herança, método e objetos**. São Carlos: Claraluz, 2008. p. 103-113.

SAYÃO, Luís Fernando. Conservação dos documentos eletrônicos. In: MUSEU DE ASTRONOMIA E CIÊNCIAS AFINS. **Conservação de acervos**. Rio de Janeiro: MAST, 2007. v. 9, p. 181-204.

- SAYÃO, Luís Fernando. Repositórios digitais confiáveis para a preservação de periódicos eletrônicos científicos. **PontodeAcesso**, Salvador, v. 4, n. 3, p. 68-94, dez. 2010. Disponível em: <<https://portalseer.ufba.br/index.php/revistaici/article/view/4709>>. Acesso em: 2 mar. 2015.
- SAYÃO, Luís Fernando; SALES, Luana Farias. Curadoria digital: um novo patamar para preservação de dados digitais de pesquisa. **Informação & Sociedade: Estudos**, João Pessoa, v. 22, n. 3, p. 179-191, set./dez. 2012.
- SHELLENBERG, Theodore Roosevelt. **Arquivos modernos: princípios e técnicas**. 5. ed. Rio de Janeiro: FGV, 2004.
- SHERA, Jesse H.; CLEVELAND, Donald B. History and foundations of information science. **Annual Review of Information Science and Technology**, v. 12, p. 249-275, 1997.
- SIEBRA, Sandra de Albuquerque et al. Curadoria digital: além da questão da preservação digital. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 14., 2013, Rio de Janeiro. **Anais...** Rio de Janeiro: UFSC, 2013.
- SILVA, Armando Malheiro da. **Arquivística: teoria e prática de uma ciência da informação**. Porto: Afrontamento, 2002.
- SILVA, De Plácido e. **Vocabulário jurídico**. Rio de Janeiro: Forense, 1967.
- SOUSA, Renato Tarciso Barbosa de. A classificação como função matricial do que fazer arquivístico. In: SANTOS, Vanderlei Batista dos (Org.). **Arquivística: temas contemporâneos: classificação, preservação digital, gestão do conhecimento**. Brasília: SENAC, 2007. p. 79-163.
- SOUSA, Renato Tarciso Barbosa de. Em busca de um instrumental teórico-metodológico para a construção de instrumentos de classificação de documentos de arquivo. In: BARTALO, Linete; MORENO, Nadina Aparecida (Org.). **Gestão em arquivologia: abordagens múltiplas**. Londrina: EDUEL, 2008. p. 11-52.
- SVENONIUS, Elaine. **The intellectual foundation of information organization**. Cambridge: MIT Press, 2000.
- TESSITORE, Viviane. **Como implantar centros de documentação**. São Paulo: Arquivo do Estado, 2003.
- THOMAZ, Katia de Padua. Repositórios digitais confiáveis e certificação. **Arquivistica.net**, v. 3, n. 1, p. 80-89, jan./jun. 2007.

THOMAZ, Katia de Padua; SOARES, Antonio José. A preservação digital e o modelo de referência Open Archival Information System (OAIS). **DataGramZero: Revista em Ciência da Informação**, v. 5, n. 1, 2004. Disponível em: <[http://dgz.org.br/fev04/Art\\_01.htm](http://dgz.org.br/fev04/Art_01.htm)>. Acesso em: 15 ago. 2016.

TIBBO, Helen Ruth; HANK, Carolyn; LEE, Christopher A. Challenges, curricula, and competencies: researcher and practitioner perspectives for informing the development of a digital Curation curriculum. ARCHIVING, 2008, Berna. **Anais...** Berna: Society for Imaging Science and Technology, 2008.

VALENTIM, Marta Lígia Pomim. Formação: competências e habilidades do profissional da informação. In: VALENTIM, Marta Lígia Pomim (Org.). **A formação do profissional da informação**. São Paulo: Polis, 2002. p. 117-132.

VIANA, Gilberto Fladimar Rodrigues. **Os documentos arquivísticos digitais no sistema de informações SIE/UFSM**: da produção ao acesso. 2015. 139 f. Tese (Doutorado em Ciência da Informação)-Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2015.

SILVINO, Alexandre Magno Dias; ABRAHÃO, Júlia Issy. Navegabilidade e inclusão digital: usabilidade e competência. **RAE-eletrônica**, São Paulo, v. 2, n. 2, p. 1-17, jul./dez. 2003.

VIANA, Cassandra Lúcia de Maya; MÁRDERO ARELLANO, Miguel Ángel; SHINTAKU, Milton. Repositórios institucionais em ciência e tecnologia: uma experiência de customização do DSpace. In: SIMPÓSIO INTERNACIONAL DE BIBLIOTECAS DIGITAIS, 3., 2005, São Paulo. **Anais...** São Paulo: CRUESP, 2005.

VIVAS MORENO, Agustín. Factores socio-culturales para una historia de la archivística. **Investigación Bibliotecológica**, v. 18, n. 36, jan./jun. 2004.

WINCKLER, Marco; PIMENTA, Marcelo Soares. Avaliação de usabilidade de sites web. In: ESCOLA REGIONAL DE INFORMÁTICA, 2002, Porto Alegre. **Anais...** Porto Alegre: SBC, 2002.

YAMAOKA, Eloi Juniti. Ontologia para mapeamento da dependência tecnológica de objetos digitais no contexto da curadoria e preservação digital. **AtoZ**, Curitiba, v. 1, n. 2, p. 65-78, jan./dez. 2012.

ZANIRATO, Silvia Helena; RIBEIRO, Wagner Costa. Patrimônio cultural: a percepção da natureza como um bem não renovável. **Revista Brasileira de História**, São Paulo, v. 26, n. 51, p. 251-256, 2006.

## APÊNDICE A

<b>Recomendações simplificadas para medição e certificação de confiabilidade para Repositório Arquivístico Digital Confiável</b>		
<b>Descrição do item para verificação</b>	<b>Sim</b>	<b>Não</b>
1. Estar em conformidade com o modelo OAIS – <i>Open Archival Information System</i> (RCL/OCLC, 2002, p. 5).		
2. O Repositório deverá ter responsabilidade Administrativa (RCL/OCLC, 2002).		
3. O repositório deverá oferecer viabilidade Organizacional (RCL/OCLC, 2002).		
4. Possuir sustentabilidade Financeira (RCL/OCLC, 2002).		
5. Possuir adequação tecnológica e de procedimentos (RCL/OCLC, 2002).		
6. Ter segurança do Sistema (RCL/OCLC, 2002).		
7. Oferecer responsabilidade de procedimentos (RCL/OCLC, 2002).		
8. Estar em conformidade com a lei em vigência que dispõe sobre a política nacional de arquivos públicos e privados e da outras providências, hoje Lei n. 8.159 (BRASIL, 1991).		
9. Ter como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. (CONARQ, 2014)		
10. Ter um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos para garantir a continuidade do serviço. (CONARQ, 2014)		
11. Identificar e estabelecer as funções que necessita realizar e nomear pessoas com qualificações e experiência adequadas para cumprir esses deveres (ISO, 2012).		
12. Definir a comunidade alvo e sua base de conhecimento (CONARQ, 2014).		
13. Ter sua história documentada, bem como as alterações de operações e procedimentos de <i>software</i> e <i>hardware</i> (ISO, 2012).		
14. Comprometer-se com a transparência e responsabilidade em todas as ações de apoio à exploração e gestão do repositório que afetam a preservação de conteúdos digitais ao longo do tempo (ISO, 2012).		
15. Demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, buscando atendê-las (CONARQ, 2014).		
16. Comprometer-se com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia (CONARQ, 2014).		
17. Ter um calendário regular de auto avaliação e de certificação externa (ISO, 2012).		
18. Adotar a Curadoria Digital como um processo para o ciclo de vida dos documentos		
19. Dispor de sistemas de planejamento de negócios de curto e longo prazo, para que seja mantido ao longo do tempo (ISO, 2012).		
20. Os contratos, licenças e passivos firmados pelo repositório devem ser claros e mensuráveis; delinear papéis, responsabilidades, prazos e condições e ser facilmente acessíveis ou disponíveis aos interessados (CONARQ, 2014).		
21. Identificar as informações de conteúdo e as propriedades de informação que preservar (ISO, 2012).		
22. Especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão (CONARQ, 2014).		
23. Ter as especificações adequadas que permitam o reconhecimento e a análise do <i>SIP</i> (ISO, 2012).		
24. Ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência (CONARQ, 2014).		
25. Ter procedimentos para verificar a integridade do <i>SIP</i> , o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana (CONARQ, 2014).		
26. Ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e que são relevantes para a preservação (CONARQ, 2014).		
27. Demonstrar em que momento a responsabilidade pela preservação do documento submetido ( <i>SIP</i> ) é formalmente aceita pelo repositório (CONARQ, 2014).		
28. Descrever minuciosamente as diferentes classes de informação e como os <i>AIPs</i> são implementados nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes.		
29. Descrever como <i>AIPs</i> são construídos a partir <i>SIP</i> (ISO, 2012).		
30. Documentar a disposição final de todos os <i>SIP</i> (ISO, 2012).		
31. Atribuir aos <i>AIPs</i> identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por ex.: <i>Handle System</i> , DOI, URN, PURL) (CONARQ, 2014).		

<b>Recomendações simplificadas para medição e certificação de confiabilidade para Repositório Arquivístico Digital Confiável</b>		
<b>Descrição do item para verificação</b>	<b>Sim</b>	<b>Não</b>
32. Ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivo (CONARQ, 2012).		
33. Ter procedimentos para testar se os documentos são compreensíveis para comunidade alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (CONARQ, 2012).		
34. Verificar cada AIP para a integralidade e exatidão no ponto em que é criado (ISO, 2012).		
35. Promover a acessibilidade à informação armazenada (LIMA-MARQUES; MACEDO, 2006).		
36. Ter um mecanismo independente para verificar a integridade do conjunto do seu acervo (CONARQ, 2012).		
37. Documentar todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do AIP (CONARQ, 2012).		
38. Possuir estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado como, por exemplo, a normalização de formatos (CONARQ, 2012).		
39. Possuir mecanismos de mudanças do plano de preservação como resultado do monitoramento (CONARQ, 2012).		
40. Fornecer evidências sobre a eficácia do plano de preservação (CONARQ, 2012).		
41. Utilizar estratégias previstas no planejamento da preservação que podem ser várias e devem ser registradas nos metadados de preservação (CONARQ, 2012).		
42. Preservar o documento digital (informação de conteúdo do AIP) originalmente admitido no repositório e daquele resultante da última migração (CONARQ, 2012).		
43. Especificar os requisitos mínimos de informação para permitir ao público alvo descobrir e identificar o material de seu interesse (ISO, 2012).		
44. Captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão e associação desses metadados ao AIP correspondente (CONARQ, 2012).		
45. Manter Integridade referencial entre os AIPs e sua informação descritiva (metadados). (CONARQ, 2012).		
46. Divulgar para a comunidade de usuários as opções disponíveis de acesso aos documentos e de entrega dos mesmos (CONARQ, 2012).		
47. Dar a concessão de acesso a cada AIP para os usuários autorizados e da forma devida, em conformidade com o acordo estabelecido entre o repositório e o produtor/depositante (CONARQ, 2012).		
48. Ter documentação e implementação de políticas de acesso. Essas políticas de acesso podem variar desde a isenção da necessidade de identificação de usuário até o controle rígido da identificação e autenticação do usuário (CONARQ, 2012).		
49. Identificar e gerir os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema (ISO, 2012).		
50. Gerenciamento do número de cópias de todos os documentos mantidos no repositório e a localização de cada uma delas (CONARQ, 2012).		
51. Adotar uma tecnologia de <i>hardware</i> e <i>software</i> apropriada para os serviços que presta: procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada (CONARQ, 2012).		
52. Manter uma análise sistemática dos fatores de risco de segurança associados com os dados, sistemas, pessoal e instalações físicas (ISO, 2012).		
53. Adotar procedimentos de controle para tratar adequadamente as necessidades de segurança (CONARQ, 2012).		
54. Delinear papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema (CONARQ, 2012).		
55. Ter um plano de prevenção de desastres e de reparação que inclua, ao menos, um <i>backup, off site</i> , de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação (CONARQ, 2012).		

**Fonte:** Elaborado pela autora