UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO

FÁBIO LOPES DE ANDRADE

REPOSITÓRIOS DIGITAIS CONFIÁVEIS: AS TRANSFERÊNCIAS E A VERIFICAÇÃO DE COMPATIBILIDADE ENTRE MODELOS INTERNACIONAIS DE CRITÉRIOS DE PRESERVAÇÃO DIGITAL NO LONGO PRAZO E O RDC-ARQ

Belo Horizonte
2021

FÁBIO LOPES DE ANDRADE

REPOSITÓRIOS DIGITAIS CONFIÁVEIS: AS TRANSFERÊNCIAS E A VERIFICAÇÃO DE COMPATIBILIDADE ENTRE MODELOS INTERNACIONAIS DE CRITÉRIOS DE PRESERVAÇÃO DIGITAL NO LONGO PRAZO E O RDC-ARQ

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais para obtenção do grau de Mestre em Ciência da Informação.

Linha de Pesquisa: Políticas Públicas e Organização da Informação.

Orientadora: Dra. Cíntia Aparecida Chagas

BELO HORIZONTE

2021

A553r Andrade, Fábio Lopes de.

Repositórios digitais confiáveis [recurso eletrônico]: as transferências e a verificação de compatibilidade entre modelos internacionais de critérios de preservação digital no longo prazo e o rdc-arq / Fábio Lopes de Andrade. - 2021.

1 recurso eletrônico (531 f. : il., color): pdf.

Orientadora: Cíntia Aparecida Chagas.
Dissertação (Mestrado) – Universidade Federal de Minas Gerais, Escola de Ciência da Informação.
Referências: f. 174-183.
Apêndices: f. 194-526.
Exigências do sistema: Adobe Acrobat Reader.

1. Ciência da Informação – Teses. 2. Arquivos – Teses. 3. Preservação pela digitalização – Teses. I. Título. II. Arreguy, Cíntia Aparecida Chagas. III. Universidade Federal de Minas Gerais, Escola de Ciência da Informação.

CDU:651.5

Ficha catalográfica: Maianna Giselle de Paula CRB:2642
Biblioteca Profª Etelvina Lima, Escola de Ciência da Informação da UFMG.

UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO
CURSO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ATA DE DEFESA DE DISSERTAÇÃO

Às **09:00** horas do dia 20 de maio de 2021, por videoconferência, realizou-se a sessão pública para a defesa da Dissertação de FÁBIO LOPES DE ANDRADE. A presidência da sessão coube à Cíntia Aparecida Chagas, orientadora. Inicialmente, a presidente fez a apresentação da Comissão Examinadora assim constituída: Daniel Flores, UFSC, Welder Antônio Silva, ECI/UFMG e Cíntia Aparecida Chagas, ECI/UFMG, orientadora. Em seguida, o candidato fez a apresentação do trabalho que constitui sua **Dissertação de Mestrado**, intitulada: "*REPOSITÓRIOS DIGITAIS CONFIÁVEIS: A TRANSFERÊNCIAS E A VERIFICAÇÃO DE COMPATIBILIDADE ENTRE MODELOS INTERNACIONA CRITÉRIOS DE PRESERVAÇÃO DIGITAL NO LONGO PRAZO E O RDC-Arq*". Seguiu-se a arguição pelos examinadores e logo após, a Comissão reuniu-se, sem a presença do candidato e do público e decidiu considerar **aprovado** a **Dissertação de Mestrado**. O resultado final foi comunicado publicamente ao candidato pela presidente da Comissão. Nada mais havendo a tratar, a presidente encerrou a sessão e lavrou a presente ata que, depois de lida, se aprovada, será assinada pela Comissão Examinadora.

Belo Horizonte, 13 de maio de 2021.

Assinatura dos membros da banca examinadora:

Documento assinado eletronicamente por **Welder Antonio Silva**, **Professor do Magistério Superior**, em 24/05/2021, às 16:59, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Cintia Aparecida Chagas**, **Professora do Magistério Superior**, em 24/05/2021, às 17:21, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Daniel Flores**, **Usuário Externo**, em 25/05/2021, às 17:48, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0725052** e o código CRC **F31093BB**.

DEDICATÓRIA

Aos meus pais, Maria Eugênia e Waldir, e aos meus avós, Waldomiro e Regina, Anália e José Feres, dedico esta pesquisa. Suas vidas, um ciclo infinito de lutas e sacrifícios, proporcioaram-me este caminho, repleto oportunidades de aprendizado e de tranquilidade.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a minha orientadora, Drª. Cintia Aparecida Chagas, pela confiança, pela paciência, pela oportunidade de aprender e pela bondade em compartilhar seu tempo e seu vasto conhecimento no desenvolvimento desta pesquisa.

Agradeço aos mebros da Banca, Dr. Daniel Flores, Dr. Welder Antônio e Dr. Adalson Nascimento por aceitarem participar desta jornada e pelas orientações e incentivos quando de nossos encontros.

Agradeço aos Professores do Programa de Pós-Graduação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais pela generosidade em partilhar seus conhecimentos e experiências.

Agradeço aos Professores de Graduação do curso de Arquivologia, da Escola de Ciência da Informação da Universidade Federal de Minas Gerais: Drª. Ivana Parrela, Me. Marta Melgaço, Dr.Welder Silva, Me. Leandro Negreiros, Dr. Adalson, Dr. Renato Venâncio e Dr. Alessandro, pelo incentivo diário, desde a as primeiras aulas da primeira turma de graduação, ainda em 2009.

Agradeço à Drª. Eliane Rocha, pela amizade e pelo incentivo à continuidade nos estudos.

Agradeço à Professora Vera Furst, Coordenadora da 1ª Turma de Arquivologia da Escola de Ciência da Informação da UFMG e ao Servidor Guilherme Diniz, do Colegiado de Arquivologia, por empenharem-se tanto em minha conclusão de curso.

Agradeço à amiga Aline Medeiros, da Coordenação de Tecnologia da Informação do Ibram, pelo apoio e por seus apontamentos, essenciais para que esta jornada se iniciasse, ainda em 2018.

Agradeço aos amigos Dr. Jamerson Vieira e Marconi Jorge, da Procuradoria Federal Junto ao Ibram, pelo incentivo aos estudos, pelo apoio diante das adversidades e, acima de tudo, pelo exemplo de retidão de caráter e honestidade.

Às servidoras do Ibram Srª. Janete Conceição e Srª. Viviane Lacerda, meu sincero reconhecimento aos exemplos de ética e profissionalismo no exercício da função pública que as senhoras personificam.

Por fim, agradeço pelo apoio do institucional dos dirigentes Instituto Brasileiro de Museus, por acreditarem que esta pesquisa pode auxiliar na preservação de nossos acervos arquivísticos digitais.

RESUMO

Neste trabalho, objetivou-se analisar os critérios do Catalogue of Criteria for Trusted Digital Repositories (NESTOR), do Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) e Audit and Certification of Trustworthy Digital Repositories (ACTDR), comparando-os com os requisitos das Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq). Foram observadas as semelhanças e diferenças quanto aos agentes das ações de preservação, quanto às ações de preservação e quanto aos objetos digitais alvo dessas ações de preservação, elencadas em cada requisito, bem como se efetivam as ações de auditoria e certificação em cada um dos modelos de preservação digital. O intento foi elaborar um modelo conceitual híbrido, fruto das análises dos três modelos de requisitos supracitados, de forma a propor um formulário para autoavaliação de repositórios arquivísticos digitais confiáveis, adaptado ao contexto brasileiro e que possa subsidiar futuras atualizações do RDC-Arq. Ao mesmo tempo, investigou-se como proceder a transmissão de Pacotes de Submissão de Informação ao RDC-Arq, observando o Decreto nº 10.278/2020 e experiências internacionais de instituições arquivísticas e de preservação digital por longos períodos, com o intuito de desenvolver procedimentos aliados a tecnologias de software de código aberto e distribuídas gratuitamente, com a finalidade de prover Produtores e arquivos de instituições de ferramentas adequadas ao desafio da manutenção do valor legal dos documentos arquivísticos digitalizados em transmissões aos RDC-Arqs. A metodologia utilizada foi a revisão bibliográfica em pesquisas científicas voltadas para a preservação digital em longo prazo, notadamente, as citadas no RDC-Arq. Comparou-se, quantitativamente, e qualitativamente, os requisitos e critérios de modelos voltados à auditoria e certificação de repositórios digitais, em busca de similaridades e diferenças conceituais. Concluiu-se que o TRAC apresenta grande similaridade conceitual ao RDC-Arq, bem como já se dispõe de softwares para auxiliar os trabalhos de auditoria. O Catálogo NESTOR apresentou critérios de grande amplitude conceitual, mas que, em grande parte, não eram similares ao RDC-Arq. O ACTDR mostrou-se mais complexo e detalhado que o RDC-Arq, e é possível inferir que há relativa similaridade conceitual entre ambos. Quanto à transmissão de Pacotes de Submissão de Informação entre Produtores e instituições abarcadas pelo Decreto 10.278/2020, verificou-se que o referido Decreto deixou muitas lacunas quanto a especificidades técnicas e metodológicas para a efetivação do envio adequado de documentos digitalizados com valor legal. Por fim, sugeriu-se uma proposta de fluxo de ações, combinada com softwares adequados à manutenção da integridade, validação e busca de códigos maliciosos, que torna viável e segura a transmissão de documentos arquivísticos digitalizados.

Palavras-chave: *Catalogue of Criteria for Trusted Digital Repositories NESTOR.* Auditoria e Certificação de repositórios digitais confiáveis. Repositório Arquivístico Digital Confiável (RDC-Arq). *Audit and Certification of Trustworthy Digital Repositories (ACTDR). Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC).

ABSTRACT

This work aimed to analyze the criteria of the Catalogue of Criteria for Trusted Digital Repositories (NESTOR) of the Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) and the Audit and Certification of Trustworthy Digital Repositories (ACTDR). The criteria were compared with the requirements of the Guidelines for the Implementation of Reliable Digital Repositories (RDC-Arq), observing the similarities and differences regarding the agents of the preservation actions, the preservation actions, and the digital objects targeted by these preservation actions, listed in each requirement; as well as auditing and certification actions in each of the digital preservation models. The objective was to elaborate a hybrid conceptual model, fruit of the analysis of the three requirement models mentioned above, and propose a form for self-evaluation of reliable digital archival repositories, adapted to the Brazilian context, that can subsidize future RDC-Arq updates. At the same time, we investigated how to proceed with the transmission of Information Submission Packages to the RDC-Arq, observing Decree nº 10,278/2020 and international experiences of archival and digital preservation institutions for long periods, to propose appropriate technical procedures for digital archival preservation in the Brazilian context. The purpose was to develop procedures allied to open source software technologies distributed free of charge to provide Producers and archives of institutions reached by Decree 10,278/2020 with appropriate tools to maintain the legal value of digitized archival documents. The methodology used was the bibliographic review in scientific research aimed at long-term digital preservation, notably those cited in the RDC-Arq. We compared quantitatively and qualitatively the requirements and criteria of models aimed at auditing and certifying digital repositories in search of similarities and conceptual differences. In conclusion, TRAC shows a high conceptual similarity to the RDC-Arq and already has software available to assist the audit work. The NESTOR Catalog presented significant conceptual amplitude criteria but high non-similarity to the RDC-Arq. The ACTDR proved to be more complex and detailed than the RDC-Arq, and it is possible to see a relatively conceptual similarity between them. Decree 10.278/2020 left many gaps in technical and methodological specificities for the proper transmission of Information Submission Packages between Producers and institutions covered it. Finally, we suggest a proposal of action flow combined with appropriate software to maintain integrity, validation, and search for malicious codes, making the transmission of digital archival objects viable and secure.

Keywords: Catalogue of Criteria for Trusted Digital Repositories NESTOR. Audit and Certification of Trusted Digital Repositories. Trusted Digital Archive Repository (RDC-Arq). Audit and Certification of Reliable Digital Repositories (ACTDR) Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC).

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
ACTDR	Audit and Certification of Trustworthy Digital Repositories
AIP	Archival Information Package
ALCTS	Association for Library Collections & Technical Services
ARK	The Archival Resource Key
ASCII	American Standard Code for Information Interchange
AVG	Anti-Virus Guard
BnF	Bibliothèque nationale de France
BNSC	British National Space Centre
CCSDS	Consultative Committee for Space Data Systems
CEDARS	CURL Exemplars in Digital ARchiveS
CMM	Capability Maturity Model
CNES	Centre National d'Études Spatiales
CONARQ	Conselho Nacional de Arquivos
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Center for Research Libraries
CSV	Comma Separated Values
CURL	Client Uniform Resource Locator
DANS	Data Archiving and Networked Services
DC	District of Columbia
DCC	Digital Curation Center
DIN	Deutsches Institut für Normung
DINI	Deutsche Initiative für NetzwerkInformation
DIP	Dissemination Information Package
DOI	Digital Object Identifier
DPC	Digital Preservation Coalition
DPCMM	Digital Preservation Capability Maturity Model
DROID	Digital Record Object IDentification
E-Arq Brasil	Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos
ECM3	Enterprise Content Management Maturity Model
ESA	European Space Agency
GIF	Graphics Interchange Format
GUI	Graphical User Interface

HAI	History Associates Incorporated
HTML	HyperText Markup Language
ICA	International Council On Archives
InterPARES	International Research on Permanent Authentic Records in Electronic Systems
IRMT	International Records Management Trust
ISO	International Organization for Standardization
JEPG	Joint Photographic Experts Group
JHOVE	JSTOR/Harvard Object Validation Environment
JSON	JAVAScript Object Notation
JSTOR	Journal Storage Digital library of academic journals, books, and primary sources
KB	Koninklijke Bibliotheek
LC	Library of Congress
LR	Label Release
MD5	Message-Digest algorithm 5
MIT	Massachusetts Institute of Technology
MOIMS-RAC	Mission Operations Information Management Services Repository Audit and Certification
NABCB	National Accreditation Board for Certification Bodies
NARA	National Archives and Records Administration
NASA	National Aeronautics And Space Administration
NBNs	National Bibliography Numbers
NBR	Norma Brasileira
NCDCR	North Carolina Department of Natural and Cultural
NDSA	National Digital Stewardship Alliance
NEDLIB	Network Event Detection Library
NESTOR	Network of Expertise in long-term Storage
NEWG	NASA-ESA Working Group
NLNZ	National Library of New Zealand
NOBRADE	Norma Brasileira de Descrição Arquivística
OAIS	Reference model for an Open Archival Information System
OCLC	Online Computer Library Center
PAIMAS	Producer-Archive Interface Methodology Abstract Standard
PC	Personal Computer
PDF	Portable Document Format

PDF/A	Portable Document Format: Portable Document Format
PDI	Preservation Description Information
PNG	Portable Network Graphics
PREMIS	Preservation Metadata Implementation Strategies
PRONOM	Public Record Office and Nom
PTAB	Primary Trustworthy Digital Repository Authorisation Body
PURL	the persistent URL
RDC	Repositórios Digitais Confiáveis
RDC-Arq	Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis
RLG	RESEARCH LIBRARIES GROUP
SAAI	Sistema Aberto de Arquivamento de Informação
SHA	Secure Hash Algorithm
SINAR	Sistema Nacional de Arquivos
SIP	Submission Information Package
TIB	Technische Informationsbibliothek Hanover
TRAC	Trustworthy Repositories Audit & Certification: Criteria and Checklist
UBC	University of British Columbia
UNESCO	United Nations Educational, Scientific and Cultural Organization
URN	Uniform Resource Name
USB	Universal Serial Bus
XML	eXtensible Markup Language
ZBW	Leibniz-Informationszentrum Wirtschaft

SUMÁRIO

1 INTRODUÇÃO

O início do século XXI apresenta um mundo fortemente dependente do documento arquivístico digital como um meio para registrar as funções e atividades de indivíduos, organizações e governos (CONSELHO NACIONAL DE ARQUIVOS - CONARQ, 2004). A informação digital, para NESTOR (BERGMEYER *et al.*, 2009, p. 1, Tradução nossa), tornou-se:

> Uma parte indispensável de nossa cultura e herança científica. Achados científicos, documentos históricos e realizações culturais estão em crescimento acelerado, sendo apresentados em formato eletrônico e, em muitos casos, exclusivamente assim. No entanto, além das vantagens inestimáveis oferecidas por este formato, ele também traz uma séria desvantagem: os usuários precisam investir muito esforço técnico para acessar a informação. Além disso, a tecnologia subjacente ainda está passando por mais desenvolvimento em um ritmo excepcionalmente rápido[1].

O problema da preservação e manutenção de informações digitais, no longo prazo pode ser interpretado como preservação de documentos, para que a tecnologia em que se baseiam não se torne obsoleta, conforme alerta InterPARES (INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS - InterPARES, 2018, p. 6, Tradução nossa):

> Os objetos digitais requerem manutenção constante e contínua e dependem de um ecossistema complexo de *hardware, software*, padrões e regulamentos legais que estão constantemente mudando, sendo alterados ou substituídos. Quando comparados aos registros analógicos, os digitais enfrentam maior risco de deterioração, em razão do ritmo acelerado de desenvolvimento da tecnologia da informação. A preservação de registros digitais é muito mais do que a preservação de um arquivo de computador - o objetivo é permitir o acesso ao conteúdo e, ao mesmo tempo, garantir que suas características importantes sejam preservadas[2].

---

[1] Texto original: *Digital information has become an indispensable part of our cultural and scientific heritage. Scientific findings, historical documents and cultural achievements are to a rapidly increasing extent being presented in electronic form - in many cases exclusively so. However, besides the invaluable advantages offered by this form, it also carries a serious disadvantage: users need to invest a great deal of technical effort in accessing the information. Also, the underlying technology is still undergoing further development at an exceptionally fast pace.*

[2] Texto original: *Digital objects require constant and continuous maintenance and depend on complex ecosystem of hardware, software, standards and legal regulations which are constantly changing, being amended or replaced. When compared to analogue records, digital ones face greater risk of decaying, the reason for that being primarily the fast pace of information technology development. Preservation of digital records is much more than preservation of a computer file - the goal is to enable access to the content while at the same time ensuring that their important characteristics are preserved*.

Essas circunstâncias provocaram ainda, questionamentos quanto à confiabilidade da informação, uma vez que produtores e consumidores de informação necessitam identificar se as organizações de memória (museus, arquivos e bibliotecas) são capazes de garantir a autenticidade, integridade, confidencialidade e disponibilidade da informação digital no longo prazo. Assim, confrontados com a inundação de objetos digitais, os responsáveis dentro das instituições são igualmente motivados a estabelecer e comunicar sua confiabilidade, a fim de assegurar ao presente e ao futuro memórias coletivas (BERGMEYER *et al.*, 2009).

Em busca por experiências sobre a implementação, auditoria e certificação de repositórios digitais no contexto internacional, sobressaiu-se, por seu caráter distinto quanto à aplicação junto às instituições de memória alemãs, o *Catalogue of Criteria for Trusted Digital Repositories*[3]*, do Grupo NESTOR.* De acordo com Dobratz, Schoger e Strathmann (2007), a *Network of Expertise in long-term Storage (NESTOR)- Working Group on Trusted Repositories Certification*[4]*,* é fruto de uma iniciativa do Ministério da Pesquisa e Educação da Alemanha, do setor do patrimônio cultural (bibliotecas, arquivos, museus), de instituições de pesquisa (universidades, centros de processamento de dados) e de fornecedores de tecnologia (centros de informática, centros de mídia) para implantação e certificação de repositórios digitais em arquivos, museus e bibliotecas.

De forma semelhante, o *Trustworthy Repositories Audit & Certification: Criteria and Checklist*[5] (TRAC) é uma prática recomendada desenvolvida pelo *Consultative Committee for Space Data Systems*[6] (CCSDS), fornecendo às instituições diretrizes para a realização de auditorias internas para avaliar a confiabilidade dos repositórios digitais e criar uma estrutura para suportar a certificação externa. O TRAC estabelece critérios, evidências, melhores práticas e controles que os repositórios digitais podem usar para avaliar suas atividades nas áreas de infraestrutura organizacional, gerenciamento de objetos digitais e infraestrutura técnica e gerenciamento de riscos (WELCH; PHILLIPS, 2014).

O *Audit and Certification of Trustworthy Digital Repositories*[7] (ACTDR) tem por objetivo "definir uma prática recomendada na qual basear um processo de auditoria e certificação para avaliar a confiabilidade dos repositórios digitais. Seu escopo de aplicação é toda a gama de repositórios digitais" (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM - CCSDS, 2011, p. 1). Segundo Carvalho (2015), o ACTDR deriva do TRAC,

---

3 Catálogo de Critérios para Repositórios Digitais Confiáveis. Tradução do autor.
4 Rede de especialização em armazenamento no longo prazo - Grupo de trabalho sobre certificação de repositórios confiáveis. Tradução do autor.
5 Auditoria e Certificação de Repositórios Confiáveis: Critérios e Lista de Verificação. Tradução do autor.
6 Comitê Consultivo para Sistemas de Dados Espaciais. Tradução do autor.
7 Auditoria e Certificação de Repositórios Digitais Confiáveis. Tradução do autor.

publicado em 2007 pelo *Research Library Group*[8] (RLG) e o *National Archives and Records Administration*[9] (NARA), tendo-se configurado na Norma *International Organization for Standardization* [10] (NA) 16363 no ano de 2012.

Neste contexto, foram elaboradas pelo Conselho Nacional de Arquivos as *Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis* (RDC-Arq), com o objetivo de indicar parâmetros para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade (constituída de 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, permanentemente (CONSELHO NACIONAL DE ARQUIVOS - CONARQ, 2015a). Entretanto, a normativa brasileira não prevê orientações quanto à auditoria e certificação de repositórios arquivísticos digitais.

Nesta pesquisa, busca-se analisar os modelos de requisitos TRAC, NESTOR e ACTDR de forma a investigar como se realizam, no contexto internacional, a auditoria e certificação de repositórios digitais confiáveis. Pretende-se comparar os critérios dos modelos de requisitos supracitados com os requisitos do RDC-Arq, com o objetivo de propor sua atualização e possibilitar a auditoria e certificação de repositórios arquivísticos digitais, no contexto brasileiro. Essa proposta se materializará, por meio de um modelo conceitual híbrido, fruto das análises dos quatro modelos de requisitos supracitados. Serão também analisadas as ações de auditoria e certificação em cada um dos modelos de preservação digital.

Por fim, pretende-se investigar como se devem realizar os procedimentos técnicos para a transmissão de Pacotes de Submissão de Informação (SIPs), tendo por base publicações referenciais nacionais e internacionais, na área de preservação digital, por longos períodos, no intuito de tornar o Decreto nº 10.278/2020, que estabelece a técnica e os requisitos para a digitalização de documentos públicos ou privados, viável de ser efetivado, com o objetivo de transmitir e armazenar documentos arquivísticos digitalizados, legalmente válidos, por longos períodos, em repositórios digitais arquivísticos confiáveis.

1.1 PROBLEMA

Comopromover a auditoria e certificação de repositórios arquivísticos digitais, bem como realizar a transmissão de documentso arquivísticos digitalizados, no contexto

[8] Grupo de Biblioteca de Pesquisa. Tradução do autor.
[9] Administração de Arquivos e Registros Nacionais. Tradução do autor.
[10] Organização Internacional de Normalização. Tradução do autor.

brasileiro, tendo por base normas e padrões internacionalmente aceitos pela comunidade arquivística?

1.2 OBJETIVOS

Com este estudo, propõe-se atender ao objetivo geral e aos objetivos específicos a seguir.

1.2.1 Objetivo geral

Habilitar as *Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq)* a autoavaliar, auditar e certificar repositórios arquivísticos digitais, bem como transmitir documentos arquivísticos digitalizados observando regulamentações do CONARQ e do Decreto 10.278/2020.

1.2.2 Objetivos específicos

a) Analisar os critérios do Catalogue of Criteria for Trusted Digital Repositories (NESTOR), do Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) e Audit and Certification of Trustworthy Digital Repositories (ACTDR), comparando-os com os requisitos das Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq).
b) Elaborar um modelo conceitual híbrido, fruto das análises dos três modelos de requisitos supracitados, de forma a propor um formulário para autoavaliação de repositórios arquivísticos digitais confiáveis, adaptado ao contexto brasileiro e que possa subsidiar futuras atualizações do RDC-Arq;
c) Investigar como proceder a transmissão do Pacote de Submissão de informação ao RDC-Arq, observando o disposto no Decreto nº 10.278/2020 e, simultaneamente, apoiando-se nas experiências internacionais de instituições voltadas para a preservação digital, por longos períodos.

1.3 JUSTIFICATIVA

Duranti (1994) afirma que, através dos milênios, os arquivos têm representado, alternada e cumulativamente, os arsenais da administração, do direito, da história, da cultura e da informação. A razão pela qual eles puderam servir a tantas finalidades é que os documentos arquivísticos, representam um tipo de conhecimento único: gerados ou recebidos no curso das atividades pessoais ou institucionais como seus instrumentos e

subprodutos, os registros documentais são as provas primordiais para as suposições ou conclusões relativas a essas atividades e às situações que elas contribuíram para criar, eliminar, manter ou modificar. A partir dessas provas, as intenções, ações, transações e fatos podem ser comparados, analisados e avaliados, e seu sentido histórico pode ser estabelecido.

Os registros digitais diferem, significativamente, dos registros em papel, afirma Rogers (2016). Eles são voláteis e sujeitos à perda, à alteração intencional ou não, à contaminação ou corrupção, mesmo quando ainda estão sob custódia de seu criador. Sua autoria, sua procedência ou cadeia de custódia podem ser difíceis ou impossíveis de determinar. Eles podem ser transmitidos, compartilhados, e copiados com facilidade. Sua acessibilidade está sujeita à obsolescência e incompatibilidade de *hardware* e *software*. Mesmo que o criador dependa de um registro digital no curso de negócios, e mantenha sua cadeia de custódia ininterrupta, a fragilidade e vulnerabilidade de registros digitais exigem uma ação explícita para proteger a autenticidade do registro. Diante dessa constatação, Garret e Walters (1996, p. 23, Tradução nossa) concluíram que:

> Para assegurar a longevidade da informação, talvez o papel mais importante na operação de um documento arquivístico digital seja administrar a identidade, integridade e qualidade dos próprios arquivos como uma fonte confiável do registro cultural. Os usuários de informações arquivadas em formato eletrônico e de serviços de arquivo relacionados a essas informações precisam ter a garantia de que um arquivo digital é o que diz ser e que as informações ali armazenadas estão seguras no longo prazo[11].

O processo de auditoria, de acordo com Santos e Flores (2015) consiste em verificar e avaliar as metodologias adotadas pela instituição. Assim, é possível verificar a conformidade do repositório digital em relação às normas e o comprometimento com as ações de preservação digital, no que se refere à infraestrutura física, técnica e tecnológica. Após a realização da auditoria, efetua-se a análise e interpretação dos dados levantados, e, baseados nesses dados, torna-se possível avaliar o grau de confiabilidade do repositório digital conferindo ou não a certificação de repositório digital confiável.

Um exemplo de auditoria e certificação é a proporcionada pela ISO 16363, uma vez que:

---

[11] Texto original: *For assuring the longevity of information, perhaps the most important role in the operation of a digital archives is managing the identity, integrity and quality of the archives itself as a trusted source of the cultural record. Users of archived information in electronic form and of archival services relating to that information need to have assurance that a digital archives is what it says that it is and that the information stored there is safe for the long term.*

> Os benefícios de realizar a auditoria e certificação sob acreditação NA decorrem do fato de que o processo NA exige melhorias contínuas para os repositórios. O processo de credenciamento NA também exige verificação de todas as organizações em todos os níveis - repetida e consistentemente ao redor do mundo. Como tal, a certificação NA 16363, por uma organização de auditoria credenciada, evidência claramente que um repositório pode ser confiável para preservar importantes produções digitais[12] (GIARETTA *et al*., 2018, p. 166, Tradução nossa).

Assim, a relevância desta pesquisa justifica-se por trazer à discussão, no contexto dos repositórios digitais arquivísticos brasileiros, as experiências em auditoria e certificação do *Catalogue of Criteria for Trusted Digital Repositories* (NESTOR), da *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC) e do *Audit and Certification of Trustworthy Digital Repositories* (ACTDR) que se destacam por sua implementação em repositórios de arquivos, museus, bibliotecas, instituições de pesquisa e instituições comerciais e não comerciais.

O Catálogo de Critérios para Repositórios Digitais Confiáveis NESTOR, a Lista de Critérios de Verificação e Auditoria para Repositórios Digitais Confiáveis TRAC e os critérios de Auditoria e Certificação do ACTDR possuem metodologias de auditoria e certificação de repositórios digitais pautados em padrões internacionalmente aceitos, conforme podemos observar:

> O catálogo NESTOR foi compilado principalmente para aplicação na Alemanha. No entanto, também está sendo discutido e padronizado dentro do contexto internacional. É crucial identificar critérios geralmente válidos entre as condições nacionais específicas. Estes se encontram, entre outras áreas, dentro do quadro legal, da provisão de instituições públicas com recursos financeiros e humanos adequados, da estrutura organizacional nacional e do estado de desenvolvimento nacional no campo da preservação digital no longo prazo[13] (BERGMEYER, 2009, p. 8, Tradução nossa).

Além disso, o *Catalogue of Criteria for Trusted Digital Repositories* - NESTOR foi desenvolvido com o objetivo de auditar e certificar os repositórios digitais quanto à confiabilidade. Segundo NESTOR (BERGMEYER, 2009), o processo de autoavaliação

---

[12] Texto original: *The benefits of conducting audit and certification under ISO accreditation accrue from the fact that the ISO process requires continuous improvements to repositories. The ISO process of accreditation also requires checking everyone and every organisation at every level - repeatedly and consistently around the world. As such, ISO 16363 certification, by an accredited audit organisation, of a repository is clear evidence that the repository can be trusted to preserve important digital holdings.*

[13] Texto original*: The NESTOR catalogue has mainly been compiled for application in Germany, however it is also being discussed and standardised within the international context. Here it is crucial to identify generally valid criteria amongst the specifically national conditions. These lie in the legal framework, the provision of public institutions with adequate financial and human resources, in national organisational structures and the status of national development in the field of digital long-term preservation.*

estendida para arquivos digitais foi desenvolvido e oferecido com base na norma *Deutsches Institut für Normung*[14] *(DIN)* 31644 - "Critérios para arquivos digitais confiáveis", que oferece aos arquivos digitais um método harmonizado e prático para verificação de confiabilidade.

Bergmeyer (2009) conclui ainda que, embora o Selo NESTOR possa ser obtido como uma solução independente, ele também participa do Quadro Europeu de Auditoria e Certificação. Além da Certificação Básica fornecida pelo Selo de Aprovação de Dados, o Selo NESTOR concede, ainda, uma Certificação Estendida.

Quanto à compatibilidade com outras normas e modelos de preservação internacionais, é interessante lembrar, segundo NESTOR, que:

> O catálogo de critérios NESTOR leva em consideração abordagens e descobertas nacionais e internacionais, como o Certificado DINI para servidores de documentos e publicações, o relatório do RLG[15]-OCLC[16] "Repositórios Digitais Confiáveis: Atributos e Responsabilidades" (maio de 2002) e o "Auditoria e certificação de repositórios confiáveis: Critérios e lista de verificação" (TRAC), publicados pela Força-Tarefa de Certificação de Repositórios Digitais da OCLC / RLG-NARA[17] em formato de rascunho em agosto de 2005 e, em seguida, em sua versão final em Fevereiro de 2007[18]. (BERGMEYER, 2009, p. 9, Tradução nossa).

A ferramenta TRAC, por sua vez, é fruto do trabalho de muitos especialistas, representando uma gama internacional de comunidades de organizações de pesquisa, governos, arquivos de dados e patrimônio cultural. Os membros da Força-Tarefa RLG/ NARA foram escolhidos, por causa de sua experiência na construção e gerenciamento de repositórios digitais. Além disso, mais de um ano de rascunho público e discursos em conferências, permitiu-nos obter *insights* e contribuições inestimáveis da comunidade, que buscou entender e utilizar a lista de verificação de auditoria. A Força-Tarefa reunida para a elaboração da Lista de Verificação e Critérios TRAC representa mais de 160 anos de experiência coletiva em sistemas e tecnologia da informação e mais de 130 anos de experiência coletiva na preservação da informação digital (ONLINE COMPUTER LIBRARY CENTER - OCLC, 2007).

O ACTDR tem por objetivo, ressaltam Santos e Flores (2015, p. 209), "definir recomendações práticas em conformidade com o modelo de referência OAIS, para

---

[14] Instituto Alemão de Normalização. Tradução do autor.
[15] The *Research* Libraries Group, Inc.
[16] *Online Computer Library Center.*
[17] *National Archives* and Records Administration.
[18] Texto original: *The NESTOR criteria catalogue takes into consideration national and international approaches and findings such as the DINI Certificate for document and publication servers, the RLG-OCLC report "Trusted Digital Repositories: Attributes and Responsibilities" (May 2002) and the "Trustworthy Repositories Audit & Certification: Criteria and Checklist" (TRAC) published by the OCLC/RLG-NARA Digital Repository Certification Task Force in draft form in August 2005 and then in its final version in February 2007.*

fundamentar um processo de auditoria e certificação, a fim de avaliar a confiabilidade de qualquer repositório digital". Segundo CCSDS (2011), o ACTDR é destinado, principalmente. aos responsáveis pela auditoria de repositórios digitais e também àqueles que trabalham ou são responsáveis pelos repositórios digitais que buscam medir objetivamente a confiabilidade de seu repositório.

O Conselho Nacional de Arquivos, ao instituir as *Diretrizes para implementação de repositórios arquivísticos digitais confiáveis* (RDC-Arq), não contemplou ações de auditoria e certificação, conforme observa CONARQ (2015, p. 5) "Estas diretrizes visam a orientar os órgãos e as entidades integrantes do Sistema Nacional de Arquivos (SINAR) na implantação de repositórios digitais confiáveis para documentos arquivísticos digitais". Dessa forma, permaneceram lacunas quanto às orientações técnicas e parâmetros adequados à realização de auditorias e certificações, no cenário dos repositórios arquivísticos digitais brasileiros. Tal vácuo regulatório impede a existência de instituições auditoras e certificadoras no mercado brasileiro.

Portanto, o trabalho desenvolvido, nesta pesquisa, intenta preencher essa lacuna, ao trazer experiências internacionais que possam ser adaptadas a uma futura atualização do RDC-Arq, de maneira que se torne uma ferramenta de auditoria e certificação adequada à legislação arquivística brasileira.

Ao mesmo tempo, pretende-se investigar como se deve proceder a transmissão de Pacotes de Submissão de Informação para o atendimento do Decreto nº 10.278/2020, que estabelece a técnica e os requisitos para a digitalização de documentos públicos ou privados. O Decreto, para sua efetivação junto aos atores que ele elenca em sua regulamentação, necessita observar uma série de normativas e orientações arquivísticas técnicas nacionais e internacionais, embora não esteja explicitado em seu texto. Nesta pesquisa, propõe-se, tendo por base publicações referenciais nacionais e internacionais, na área de preservação digital, uma prática técnica arquivística robusta o suficiente para ser utilizada por cidadãos comuns, entidades governamentais e entidades privadas que buscam utilizar documentos arquivísticos digitalizados com valor legal, similar ao representante de origem analógica, nas situações abrangidas pelo referido decreto.

1.4 ESTRUTURA DA DISSERTAÇÃO

Esta dissertação apresenta-se dividida em seis seções, sendo que:

Na 1ª Seção, composta pela INTRODUÇÃO, apresenta-se um quadro geral a respeito dos desafios enfrentados, pela comunidade que faz uso de documentos digitais, ao redor do mundo. A 1ª Seção, ainda, subdivide-se em subseções, em que são apresentados

o Problema de pesquisa, os objetivos gerais e específicos, a justificativa para a realização desta pesquisa e a estrutura da dissertação.

Na 2ª Seção, apresentam-se conceitos revistos na literatura voltada para a temática da Preservação digital. Esta seção subdivide-se em subseções que tratam do conceito de preservação digital, da importância da preservação da informação digital, da apresentação do caso de perda de dados digitais da missão espacial Viking, e da caracterização do documento arquivístico como objeto digital. Explora conceitos relativos ao documento, passando pelo documento arquivístico analógico e seguindo em direção ao objeto digital, o documento eletrônico x digital, chegando, ao final, no documento arquivístico digital e suas características. Nesta Seção, aborda-se também a Diplomática Arquivística Digital e estratégias de preservação digital em longo prazo.

Na 3ª Seção, investigaram-se os conceitos de Repositório Digital e seus subtipos. Buscou-se, pelo contexto histórico de criação do Modelo de Referência OAIS, bem como revisitaram-se os conceitos que embasam a teoria de preservação digital apresentada no Modelo.

Na 4ª Seção, abordaram-se os modelos de Critérios de preservação digital internacionais NESTOR, TRAC e ACTDR, e o modelo brasileiro, representado pelo RDC-Arq, onde foram apresentados conceitos, metodologias e práticas de autoavaliação e certificação segundo os procedimentos de cada grupo de critérios.

Na Seção 5ª, aborda-se a Metodologia aplicada para alcançar os objetivos geral e específicos, detalhando os procedimentos a serem efetuados.

Na 6ª Seção, apresentam-se e analisam-se os resultados das comparações entre os modelos de critérios internacionais e o RDC-Arq, comparando, conceitualmente, requisitos para a preservação digital, por longos períodos, por meio de tabelas que agrupam requisitos com funções de preservação semelhantes.

2 O DOCUMENTO ARQUIVÍSTICO DIGITAL E SUA PRESERVAÇÃO

No presente capítulo, abordar-se-ão conceitos de suma importância para a temática da pesquisa, com o intuito de prover o pesquisador de informações e técnicas para atingir os objetivos estipulados.

2.1 PRESERVAÇÃO DIGITAL

A preservação digital apresenta-se, de acordo com Sampaio, Abreu e Reis (2018), como um novo paradigma que enfrenta questões acerca do tratamento do suporte e, consequentemente, do documento cuja informação encontra-se registrada.

A preservação digital é, segundo Beagrie *et al.* (2008, p. 10), o processo de gestão ativa pelo qual garantimos que um objeto será acessível no futuro:

> O período de tempo é potencialmente muito curto e rápido, dado a mudança na tecnologia e nos sistemas terá um impacto direto sobre nós e, potencialmente vasto, dado que não temos idéia até que ponto outros desejarão continuar acessando a saída digital do nosso século vinte e um. Quando o fizerem, é possível que grande parte da infraestrutura técnica que usamos para criar e ler nossos dados não esteja disponível[19]

A preservação digital surgiu, afirmam Baggio e Flores (2013), na segunda metade do século passado e intensificou-se, no início do século XXI, originando-se da necessidade de preservar materiais digitais que, rapidamente, se tornavam obsoletos e/ou degradados.

Segundo Ferreira (2006 citado por UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION - UNESCO, 2003), preservação digital é o conjunto de atividades ou processos responsáveis por garantir o acesso continuado em longo prazo à informação e ao património cultural existente em formatos digitais. Ferreira (2006, p. 20) disserta que a preservação digital consiste: “[...] na capacidade de garantir que a informação digital permaneça acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação”.

Segundo a UNESCO[20] (2003), a preservação digital consiste em processos destinados a garantir a acessibilidade contínua de materiais digitais e, para atingir esse

---

[19] Texto original: *The time span is potentially very short and given rapid change in technology and systems this will impact on us directly; and potentially vast given that we have no idea to what point others will wish to continue accessing our 21st century digital output. When they do, it is possible that much of the technical infrastructure we use to create and read our data may be unavailable.*

[20] *United Nations Educational. Scientific and Cultural Organization.*

objetivo, é necessário que os objetos digitais sejam compreendidos e gerenciados em quatro níveis: como fenômenos físicos; como codificações lógicas; como objetos conceituais que têm significado para os seres humanos; e como conjuntos de elementos essenciais que devem ser preservados a fim de oferecer aos futuros usuários a essência do objeto.

Chen (2001) observa que, tradicionalmente, preservar as coisas significava mantê-las inalteradas. Entretanto, o ambiente digital mudou, fundamentalmente, nosso conceito de exigências de preservação, uma vez que, se nos agarrarmos às informações digitais sem modificá-las, o acesso a essas informações se tornará cada vez mais difícil, se não impossível. Assim, mesmo se pudéssemos encontrar um meio físico capaz de conter os dados digitais inalterados permanentemente, os formatos para registro das informações mudariam e o *hardware* e *software* necessários para recuperar as informações tornariam-se obsoletos.

Essa situação, conclui Chen (2001), cria um paradoxo fundamental para a preservação digital: Por um lado, desejamos manter as informações digitais intactas à medida que foram criadas; por outro lado, necessitamos acessar essas informações de forma dinâmica e com ferramentas cada vez mais avançadas.

Os programas de preservação devem lidar com objetos digitais, segundo UNESCO (2003, p. 35, Tradução nossa), em quatro formas:

> - Como objetos físicos, que consistem em "inscrições" (geralmente estados binários de "zeros" e "uns") em mídia portadora, como discos ou fitas de computador;
>
> - Como objetos lógicos, que consistem em código legível por computador cuja existência em qualquer tempo específico depende das inscrições físicas, mas não estão ligadas a nenhuma mídia transportadora;
>
> - Como objetos conceituais que têm significado para o ser humano, ao contrário dos objetos lógicos ou físicos que os codificam em qualquer momento em particular.
>
> - Como feixes de elementos essenciais que incorporam a mensagem, propósito ou características para que o material foi escolhido para a conservação[21].

[21] Texto original: *Preservation programmes must deal with digital objects in four guises:*
Texto original:- *As physical objects, consisting of 'inscriptions' (usually binary states of 'on-ness' or 'off-ness') on carrier media such as computer disks or tapes.*
- As logical objects consisting of computer readable code, whose existence at any particular time depends on the physical inscriptions but is not tied to any particular carrier
- As conceptual objects that have meaning to humans, unlike the logical or physical objects that encode them at any particular time.
- As bundles of essential elements that embody the message, purpose, or features for which the material was chosen for preservation.

Essa natureza multicamadas dos objetos digitais, concluiu Thibodeau (2002), tem profundas implicações para a preservação digital, uma vez que preservação aqui tem significados diferentes para cada camada.

A preservação digital significa, para Hedstrom (1997, p. 190) "[...] o planejamento, alocação de recursos e aplicação de métodos e tecnologias para assegurar que a informação digital de valor contínuo permaneça acessível e utilizável[22]".

A ASSOCIATION FOR LIBRARY COLLECTIONS & TECHNICAL SERVICES - ALCTS[23] (2007) define preservação digital como uma combinação de políticas, estratégias e ações para assegurar o acesso e a renderização[24] precisa de conteúdo digital autenticado, reformatado e nascido, ao longo do tempo, independentemente dos desafios de falhas de mídia e mudanças tecnológicas.

A preservação digital é considerada, segundo Barbedo, Corujo e Sant'ana (2011, p. 7), por meio de três vetores:

> 1. Conjunto de atividades desenvolvidas com o fim de aumentar a vida útil da informação de arquivo, salvaguardando a utilização operacional e protegendo-os das falhas de suportes, perda física e obsolescência tecnológica;
>
> 2. Conjunto de atividades que promovem a acessibilidade continuada aos conteúdos;
>
> 3. Conjunto de atividades que assistem na preservação do conteúdo intelectual, forma, estilo, aparência e funcionalidade.

Beagrie *et al.* (2008) lembraram que a preservação digital depende da interação entre o ambiente de preservação digital e os objetivos organizacionais mais amplos e questões processuais. Estas poderiam ser questões financeiras e de pessoal, gestão de cobranças, obrigações legais, exigências de auditoria, e outras estratégias e políticas.

2.2 A IMPORTÂNCIA DA PRESERVAÇÃO DA INFORMAÇÃO DIGITAL

Em 1947, Fritz Morstein Marx**,** então membro do Gabinete de Orçamento do Presidente dos Estados Unidos da América, escreveu sobre o papel dos *records*[25](documentos arquivísticos nas fases Corrente e Intermediária)na Administração. Segundo Marx (1947, p. 241, Tradução nossa),

---

[22] Texto original: *By digital preservation, I mean the planning, resource allocation, and application of preservation methods and technologies necessary to ensure that digital information of continuing value remains accessible and usable.*

[23] *Association for Library Collections & Technical Service*.

[24] Processo pelo qual se obtém o produto final de um processamento digital qualquer. Tradução do autor.

[25] Os *records* são "informações criadas, recebidas, e mantidas como prova e informação por uma organização ou pessoa, em cumprimento de obrigações legais ou na transação de negócios".

> A lembrança pode vacilar, ou a memória de um homem pode contradizer a de outro. Somente através da preservação satisfatória de um registro dos eventos e considerações que levaram a uma determinada decisão é que aqueles que participam dela podem responder por suas ações. Um registro completo é o repórter mais objetivo e, portanto, o meio mais eficaz de exigir responsabilidade. Isto também é atestado pelo fato de que a manobra mais simples para escapar da responsabilidade sempre foi a manipulação ou mesmo a destruição do registro. Em outras palavras, um dos elementos essenciais da administração responsável é a transparência do processo administrativo, tanto no que diz respeito está acontecendo hoje e o que já se passou antes. No âmbito do governo, a exigência de transparência diz respeito tanto à política quanto às necessidades gerenciais[26].

Hobsbawn (1995) corrobora o pensamento supracitado de Marx (1947), uma vez que o historiador do século XX observou que, à medida que se aproxima do presente, fica-se cada vez mais dependente de dois tipos de fonte: a imprensa diária ou periódica e os relatórios econômicos periódicos e outras pesquisas, compilações estatísticas e outras publicações de governos nacionais e instituições internacionais.

Num esforço para exemplificar o pensamento de Hobsbawn (1995), transcreve-se aqui parte do Diário de Guerra do General de Exército dos Estados Unidos da América, Dwight D. Eisenhower, Comandante Supremo das Forças Aliadas na Europa, durante a Segunda Guerra Mundial. Eisenhower previu que, algum dia, poderiam surgir dúvidas quanto à brutalidade dos crimes nazistas, o que o levou a solicitar o envio de um grupo aleatório de jornalistas e representantes legislativos americanos e ingleses para a cidade de Gotha, a fim de tornar público o que havia ocorrido ali, sem que pairassem dúvidas quanto às evidências do que encontraram em campo. Escreveu Eisenhower, em seu diário:

> Naquele dia eu vi meu primeiro campo de horrores. Ficava próximo à cidade de Gotha. Nunca fui capaz de descrever minhas reações emocionais quando encarei pela primeira vez a evidência inquestionável da brutalidade

---

Exemplos incluem relatórios finais, e-mails confirmando uma ação ou decisão, planilhas mostrando decisões orçamentárias, fotografias ou mapas de missões de campo, que precisam ser mantidas como prova.
Documentos, por sua vez, são quaisquer "informações ou objetos registrados que podem ser tratados como unidades individuais". Exemplos incluem trabalhos em andamento, tais como rascunhos comunicações ou listas "a fazer", e transitórias registros tais como e-mails confirmando uma reunião ou confirmando o recebimento de um documento (UNITED NATIONS ARCHIVES AND RECORDS MANAGEMENT SECTION. Records and Information management guidance. 2021. Disponível em: https://archives.un.org/sites/archives.un.org/files/1-guidance_what_is_a_record.pdf).

[26] Texto original: *Recollection may falter, or one man's memory may contradict another's. Only by preservation of a satisfactory record of the events and considerations that led up to a given decision can those sharing in it be made to answer for their actions. A complete record is the most objective reporter, and hence the most effective means of exacting responsibility. This is also attested by the fact that the simplest maneuver to escape responsibility has always been the manipulation or even destruction of the record. To put it differently, one of the essentials of responsible administration is transparency of the administrative process in terms of both what is going on today and what has gone on before. In the realm of government, the requirement of transparency relates to political as well as managerial needs.*

> nazista e o desrespeito cruel a qualquer senso de decência. Até então eu só conhecia aquilo em termos gerais ou através de fontes secundárias. Estou certo, no entanto, de que jamais, em qualquer momento, experimentei uma sensação de choque igual. Visitei cada canto e esconderijo do campo, pois senti que era meu dever estar em posição, a partir de então, de testemunhar em primeira mão sobre aquelas coisas, caso em algum momento surgisse a crença ou hipótese de que "as histórias de brutalidade nazista foram apenas propaganda". Alguns integrantes da equipe de visitação foram incapazes de prosseguir com o suplício. Eu não só o fiz como, assim que retornei ao quartel-general de Patton (general estadunidense) naquela tarde, mandei mensagens a Washington e Londres requisitando que ambos os governos enviassem instantaneamente à Alemanha um grupo aleatório de editores de jornal e grupos de representantes das legislaturas nacionais. Senti que a evidência deveria ser apresentada imediatamente aos públicos americano e britânico de uma maneira que não deixaria lugar para dúvidas cínicas[27] (EISENHOWER, 1948, p. 446, Tradução nossa).

O General Eisenhower teria a mesma certeza, nesse raiar do primeiro quarto do século XXI, quanto à autenticidade e confiabilidade das informações publicadas, por jornais em meio digital, ao veicularem informações tão estarrecedoras quanto às que ele presenciou no campo de extermínio nazista, em Gotha?

Duranti (2005) aponta que, durante séculos, a nossa presunção de exatidão e autenticidade teve como premissa a presença ou ausência de elementos formais visíveis sobre os documentos que estavam sendo examinados, e em uma linha ininterrupta de custódia legítima de tais documentos. O uso da tecnologia digital, afirma a pesquisadora, ao reconfigurar esses elementos formais, permitiu não só evitar controles de produção, e fez da custódia física um conceito elusivo mas, em primeiro lugar, eliminou o original, que é a primeira instanciação completa dos dados gravados comunicada, quer através do espaço (para outros que não o autor ou entidade de origem pessoas) ou tempo (salvo para acesso posterior pelo autor, proprietário ou sucessores legítimos). Duranti concluiu que:

> A mudança tecnológica em curso está causando preocupação generalizada ao redor do mundo sobre a preservação no longo prazo do material produzido ou armazenado usando tecnologias digitais. Uma parte da memória registrada da nossa sociedade criada e preservada digitalmente já

[27] Texto original: *The same day I saw my first horror camp. It was near the town of Gotha. I have never felt able to describe my emotional reactions when I first came face to face with indisputable evidence of Nazi brutality and ruthless disregard of every shred of decency. Up to that time I had known about it only generally or through secondary sources. I am certain, however that I have never at any other time experienced an equal sense of shock. I visited every nook and cranny of the camp because I felt it my duty to be in a position from then on to testify at first hand about these things in case there ever grew up at home the belief or assumption that `the stories of Nazi brutality were just propaganda.' Some members of the visiting party were unable to through the ordeal. I not only did so but as soon as I returned to Patton's headquarters that evening I sent communications to both Washington and London, urging the two governments to send instantly to Germany a random group of newspaper editors and representative groups from the national legislatures. I felt that the evidence should be immediately placed before the American and British publics in a fashion that would leave no room for cynical doubt.*

> foi comprometida, e há enormes custos associados à recuperação de entidades eletrônicas que se tornaram inacessíveis. Enquanto a extensão em que material digital valioso foi perdido ou tornou-se recuperável apenas com grande despesa, ainda tem de ser devidamente quantificado, já é evidente que a ameaça é real e generalizada. Além disso, mesmo se pudéssemos garantir a preservação de entidades eletrônicas e superar a fragilidade da mídia e obsolescência tecnológica, materiais preservados seriam de pouco valor a menos que possamos ter certeza de que eles são: 1) precisos, isto é, exatos e livre de erros ou distorções, e 2) autêntico, o que significa que a sua identidade e a sua integridade não foram inadvertidamente ou maliciosamente comprometidas, e que eles são o que pretendem ser, imunes à corrupção e à adulteração. (DURANTI, 2005, p. 106, Tradução nossa).

Rocha e Silva (2007) apontam que a ausência de procedimentos adequados de segurança e de preservação criam dúvidas quanto à confiabilidade, autenticidade e acesso futuro.

A dificuldade da preservação digital deve-se, principalmente, alerta Arellano (2008), à necessidade de retenção do objeto digital e do seu significado. A carência maior está na definição de técnicas de preservação digital capazes de compreender e reproduzir a forma e a função original do objeto, para garantir sua autenticidade e acessibilidade, pois eles não são apenas objetos físicos.

Moore (2008) enfatiza que um grande desafio que a preservação enfrenta é como incorporar, eficazmente, novas tecnologias, conservando, ao mesmo tempo, as propriedades de preservação tais como autenticidade, integridade, e cadeia de custódia. A mudança tecnológica em curso está causando, afirma Duranti (2005), preocupação generalizada ao redor do mundo, a respeito da preservação no longo prazo do material produzido ou armazenado, usando tecnologias digitais. A dificuldade fundamental da preservação digital advém, afirmam Thomaz e Soares (2004), da natureza dos próprios objetos que busca preservar, uma vez que, diferentemente dos formatos tradicionais, os objetos digitais são acessíveis somente por meio de combinações específicas de componentes de *hardware*, *software*, mídia e pessoal técnico.

> Diante da mudança de atitude em relação ao direito dos cidadãos à informação, da possibilidade de manipulação e da volatilidade dos documentos eletrônicos, da dependência dos sistemas em relação ao *hardware* e aos *softwares,* do fracasso dos profissionais da tecnologia da informação em entender a natureza e a finalidade dos registros documentais e, em consequência, proteger sua autenticidade, vem se tornando cada vez mais claro que os arquivistas necessitam repensar o papel social de suas instituições, reexaminar os preceitos de sua profissão e articular um novo código de objetivos a fim de cumprir sua meta profissional básica. (DURANTI, 1994, p. 49).

A informação digital tornou-se, segundo NESTOR (BERGMEYER *et al.*, 2009), uma parte indispensável de nosso patrimônio cultural e científico, uma vez que descobertas científicas, documentos históricos e realizações culturais estão sendo apresentados, cada vez mais, em formato eletrônico e, em muitos casos, exclusivamente, dessa forma.

A humanidade vivencia, um período no qual a informação e, consequentemente, a produção de documentos digitais cresce em ritmo acelerado, trazendo benefícios, possibilidades e novos desafios para o tratamento de textos, bases de dados, planilhas, mensagens eletrônicas, imagens fixas ou em movimento, gravações sonoras, material gráfico e sítios da internet (NEVES; INNARELLI, 2014). Assim "a tecnologia digital, ao facilitar, drasticamente, a criação e distribuição de conteúdos, tem gerado um crescimento exponencial na produção de informação digital." (CHOY *et al.*, 2016, p. 3)[28].

2.3 O PERIGO DAS INFORMAÇÕES ARMAZENADAS EM MÍDIAS DIGITAIS POR LONGOS PERÍODOS: O CASO DA PERDA DE DADOS DA MISSÃO ESPACIAL VIKING

Em 1975, a NASA enviou duas sondas a Marte: as sondas, apelidadas de Viking 1 e Viking 2, aterrissaram na superfície marciana em 1976. O Projeto Viking da NASA encontrou um lugar na história quando se tornou a primeira missão dos EUA a pousar uma nave espacial em segurança na superfície de Marte e devolver imagens da superfície. Foram construídas duas naves espaciais idênticas, cada uma consistindo de um aterrissador e um orbitador (SCHLIEDER, 2016).

Os principais objetivos da missão Viking eram:

> - colocar dois orbitadores em torno de Marte e dois aterrissadores em sua superfície para obter imagens de alta resolução da superfície marciana;
> - caracterizar a estrutura e composição da atmosfera e da superfície; e
> - procurar evidências de vida. (URI, 2020).

Tanto os orbitadores quanto os pousadores ultrapassaram em muito a vida útil esperada de 90 dias em sua exploração científica de Marte, o que contribuiu muito para aumentar o conhecimento sobre o Planeta Vermelho, sua atmosfera e sua superfície. Os orbitadores Viking 1 e 2 continuaram suas missões até 17 de agosto de 1980, e 24 de julho de 1978, respectivamente, no total retornando 52.663 imagens de Marte, mapeando 97% de sua superfície com uma resolução de 300 metros. Os aterrissadores Viking 1 e 2 continuaram monitorando as mudanças climáticas na superfície até 11 de novembro de

[28] Texto original: *Digital technology, in dramatically easing the creation and distribution of content, has generated exponential growth in the production of digital information.*

1982 e 12 de abril de 1980, respectivamente, retornando juntos 4.500 fotografias dos dois locais de aterrissagem. (URI, 2020).

Quanto aos experimentos em busca de vida microbiana, foram realizadas três experiências biológicas distintas em cada Viking Lander. De acordo com o Dr. Gerald Soffen, cientista do Projeto Viking, o consenso pós-missão foi que a vida em Marte não foi encontrada. Entretanto, o Dr. Gilbert Levin, principal investigador do experimento Label Release (LR) (um dos três experimentos de biologia), manteve, ao longo dos anos, que os resultados de seu experimento eram consistentes e sugestivos da presença de vida microbiana em Marte. (THAN, 2012).

O experimento da LR consistia em colher um pouco do solo marciano e misturá-lo com gotas de água que continham nutrientes e átomos de carbono radioativo. A hipótese era de que, se o solo contivesse micróbios, as formas de vida metabolizariam os nutrientes e liberariam dióxido de carbono radioativo ou gás metano, que poderia ser medido por um detector de radiação na sonda. Infelizmente, os resultados dos experimentos da LR não foram apoiados pelos outros dois experimentos das sondas, ambos negativos para a vida, de modo que a agência espacial descartou a possibilidade. (THAN, 2012).

Ao final da missão, os rolos de microfilme contendo os dados da Viking foram armazenados para serem guardados em segurança e para uso posterior em potencial. (SCHLIEDER, 2016).

Levaria mais 20 anos até que alguém olhasse para alguns daqueles dados novamente. No início dos anos 2000, Joseph Miller, neurobiologista da Universidade do Sul da Califórnia, ligou para o Curador de Dados Espaciais da NASA, solicitando dados dos experimentos biológicos da Viking, uma vez que havia dúvidas quanto aos procedimentos e resultados dos experimentos LR, agora sob revisão. Para surpresa do próprio Curador, tudo o que restou dos dados foi armazenado em uns poucos rolos de microfilme. Os 24 rolos de microfilme continham imagens de páginas impressas por computador, geradas pelo Projeto Viking, para arquivamento. (KING, 2001).

Embora cada bobina fosse específica para a Viking 1 ou 2, os dados dos três experimentos de biologia foram misturados. Além disso, enquanto o foco da busca nas 24 bobinas eram os dados de biologia, havia também dados de engenharia e outros muitos outros tipos dados misturados. (KING, 2001).

Tentar digitalizar essas bobinas de microfilme era caro e, em decorrência da má qualidade de muitos quadros, provavelmente produziria arquivos muito pouco confiáveis. Mesmo se feito de forma confiável, o esforço adicional para desenvolver *software* para reconhecer, extrair e organizar os dados desejados também teria sido caro. (KING, 2001).

De acordo com History Associates Incorporated (HAI, 2020), as fitas magnéticas começaram a secar e a rachar e a NASA, percebendo o problema, ainda nos anos 90, completou a cuidadosa tarefa de transferir esses dados para CDs. Infelizmente, o *software* usado para visualizar as imagens foi criado especialmente para a missão e não é mais suportado; o que significa que as informações cuidadosamente restauradas nos CDs continham dados e imagens que não podiam ser facilmente acessadas. Recuperar apenas 3.000 de mais de 56.000 imagens levou dois anos.

Por fim, fez a cópia digital dos microfilmes, o que levou bastante tempo para ser finalizado. (KING, 2001).

Entretanto, a NASA descobriu alguns CDs de dados da Viking Lander gerados pelo Laboratorio Jet Propulsion como parte de seu esforço de restauração de dados institucionais. Uma amostra dos CDs com a documentação limitada disponível foi enviada pela NASA aos cientistas, que determinaram que os dados não podiam ser usados para identificar e recuperar a informação desejada. (KING, 2001).

No exemplo extremo da NASA, ilustra-se que a informação digital é, notavelmente, frágil e suscetível à obsolescência de software e hardware, corrupção de arquivos ou degradação da mídia de armazenamento. (HAI, 2020).

Neste momento, 45 anos depois do lançamento da missão Viking, está a caminho de Marte mais uma sonda, a Perseverance, em busca de confirmação se há ou não há vida em Marte. É a 49ª missão com destino a Marte. (NASA, 2020a).

Apenas a Missão Viking custou 1 bilhão de dólares, nos anos 1975. (NASA, 2020b). Hoje, seu valor atualizado, em janeiro de 2021, segundo o cálculo de Inflation... (2021), seria de cerca de 5 bilhões de dólares, o equivalente 25 bilhões de reais.

2.4 O DOCUMENTO ARQUIVÍSTICO COMO OBJETO DIGITAL

Para ampliar o entendimento sobre a preservação de documentos arquivísticos digitais em longo prazo, realizou-se uma revisão dos conceitos fundamentais que caracterizam o documento arquivístico, com o intuito de compreender seus conceitos basilares e, assim, possibilitar a análise de modelos de critérios para a implementação, auditoria e certificação de repositórios digitas confiáveis, tendo em vista as especificidades que caracterizam os documentos arquivísticos sob a forma digital.

Um documento consiste, de acordo com Conselho Nacional de Arquivos (CONARQ, 2005), numa unidade de registro de informações, qualquer que seja o formato ou o suporte. Para Heredia Herrera, o documento

> [...] em um sentido muito amplo e genérico é qualquer registro de informação independente de seu meio físico. Abrange tudo que pode ser transmitido pelo conhecimento humano: livros, revistas, fotografias, filmes, microfilmes, microfichas, placas, transparências, desenhos, mapas, relatórios, normas técnicas, patentes, fitas gravadas, discos, partituras, cartões perfurados, manuscritos, selos, medalhas, pinturas, modelos, fac-símiles e, em geral, tudo que tenha um caráter representativo nas três dimensões e esteja sujeito à intervenção de uma inteligência ordenadora[29]. (HERRERA, 1991, p. 121).

Thomaz (2004) considera como documento genérico qualquer informação registrada independentemente do suporte utilizado, a qual pode ser tratada como unidade. Segundo a pesquisadora, o documento genérico possui duas unidades distintas: O suporte, meio físico sobre o qual a informação é fixada; e a mensagem ou notícia veiculada.

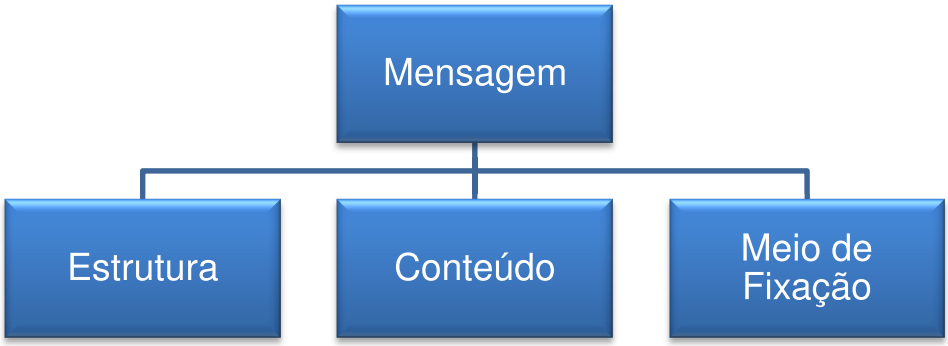
FIGURA 1 - Documento. Primeiro nível de desdobramento

FONTE: Thomaz (2004).

A mensagem pode ser decomposta em outros três elementos, quais sejam: a Estrutura sobre a qual a informação foi registrada, envolvendo cabeçalhos e outros dispositivos para identificar e rotular partes do documento; o Conteúdo propriamente dito; e o Meio de Fixação desse conteúdo, com possibilidades para o texto, o gráfico, a figura, a tabela, etc. (THOMAZ, 2004).

[29] Texto original: *Documento en un sentido muy amplio y genérico es todo registro de información independiente de su soporte físico. Abarca todo lo que puede transmitir el conocimiento humano: libros, revistas, fotografías, films, microfilmes, microfichas, láminas, transparencias, diseños, mapas, informes, normas técnicas, patentes, cintas grabadas, discos, partituras, fichas perforadas, manuscritas, sellos, medallas, cuadros, modelos, facsímiles y de manera general todo lo que tenga carácter representativo en las tres dimensiones y esté sometido a la intervención de una inteligencia ordenadora.*

FIGURA 2 - Documento. Segundo Nível de Desdobramento



FONTE: Thomaz (2004).

Schellenberg (1974, p. 41) define *archives*, num sentido que, atualmente, corresponde à Fase Permanente, como "[...] os documentos de qualquer instituição pública ou privada que hajam sido considerados de valor, merecendo preservação permanente para fins de referência e de pesquisa e que hajam sido depositados ou selecionados para depósito, num arquivo de custódia permanente."

Herrera (1991, p. 17) introduz novas variáveis, definindo *arquivo* como

> [...] um ou mais conjuntos de documentos, qualquer que seja sua data, sua forma e suporte material, acumulados em um processo natural por uma pessoa ou instituição pública ou privada no curso de sua gestão, preservados, respeitando essa ordem, para servir de testemunho e informação para a pessoa ou instituição que a produz, para os cidadãos ou para servir como fontes da história[30].

O *Guide for Managing Electronic Records from na Archival Perspective* considera que um documento arquivístico é uma informação inserida num suporte (registrada) produzida ou recebida no início, condução ou conclusão de uma atividade institucional ou individual e que compreende conteúdo, contexto e estrutura suficientes para proporcionar evidência da atividade. (INTERNATIONAL COUNCIL ON ARCHIVES - ICA, 1997).

Documentos arquivísticos são diferenciados de outros documentos, segundo Thomassem (2006), pelos motivos de sua criação.

> Diferentemente de livros em uma biblioteca, que são produtos de uma atividade de coleção consciente, documentos arquivísticos têm em comum o fato de que eles estão vinculados ao processo pelos quais foram gerados. Os documentos arquivísticos estão inseridos num processo, e isto quer

[30] Texto original: *Archivo es uno o más conjuntos de documentos, sea cual sea su fecha, sua forma y soporte material, acumulados en un proceso natural por una persona o institución pública o privada en el transcurso de su gestión, conservados, respetando aquel orden, para servir como testimonio e información para la persona o institución que lo produce, para los ciudadanos o para servir de fuentes de historia.*

> dizer que são gerados e estruturados por processos de trabalho. Um processo de trabalho é uma cadeia de atividades coerentes, com um início e um fim, e direcionadas a um objetivo específico. Acima de tudo, este objetivo é a razão para a existência, ou a missão do produtor dos documentos; é também o que estabelece vínculos entre os processos de trabalho, os quais tomamos por arquivos como um todo coerente (THOMASSEM, 2006, p. 6).

Os documentos arquivísticos caracterizam-se, aponta CONARQ (2015a,), por registrar e apoiarem as atividades do órgão ou entidade, servindo de evidência dessas atividades, bem como de fonte de informação para a pesquisa, e para assegurar os direitos dos cidadãos. O Glossário da Câmara Técnica de Documentos Eletrônicos define, de acordo com Brasil (2020, p. 22), documento arquivístico como sendo o "documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência."

Antes de conceituar o documento arquivístico digital propriamente dito, é necessáo perpassar pelos conceitos de objeto digital e suas estruturas constituintes, bem como pelas definições de documento eletronico, documento digital, documento nato digital e documento digitalizado, com o intuito de elaborar uma base conceitual sólida para propiciar o entendimento a respeito dos repositórios digitais confiáveis.

2.5 O OBJETO DIGITAL

O objeto digital pode ser definido como qualquer objeto de informação que pode ser representado usando uma sequência de dígitos binários. (FERREIRA, 2006). Para Consultive Committee for Space Data Systems (CCSDS, 2012, p. 1-11.), objeto digital é "um objeto composto de um conjunto de seqüências de *bits*[31,32]." Segundo Library of Congress (2015), objeto digital é "uma unidade discreta de informação sujeita à preservação digital[33]". Para Thibodeau (2002, p. 3), um objeto digital é um "objeto de informação, de qualquer tipo de informação ou de qualquer formato, que é expresso em formato digital[34]."

---

[31] Conceito de *bits*: As menores formas de armazenamento de dados são representadas por dígitos binários ou *bits*.. Coleções de *bits* são interpretadas pelo computador e são relatadas aos usuários como caracteres, palavras, e assim por diante, e são basicamente transformadas em um formato mais apropriado para o consumo humano não-mecânico. Em essência, este processo identifica uma associação padrão entre determinados padrões e caracteres binários, de modo que a compatibilidade entre sistemas e componentes do sistema é assegurada. O conjunto mais comum de associações é o Código Padrão Americano para Intercâmbio de Informações - ASCII. (BRITZ, 2013, p. 273). Tradução do Autor.

[32] Texto original: *Digital Object: An object composed of a set of bit sequences*.

[33] Texto original: *Digital Object: a discrete unit of information subject to digital preservation*.

[34] Texto original: *Digital Object: a digital object is an information object, of any type of information or any format, that is expressed in digital form.*

Para Kallinikos, Aaltonen e Marton (2010), os objetos digitais são marcados por um conjunto limitado de atributos variáveis, porém genéricos, como editabilidade, interatividade, abertura e distribuição.**Editabilidade**: Os objetos digitais são editáveis, maleáveis e permitem, ao menos em princípio, modificações contínuas e sistemáticas, contrastando com os artefatos convencionais. (KALLINIKOS; AALTONEN; MARTON, 2010).

Interatividade: Os objetos digitais, de acordo com Kallinikos, Aaltonen e Marton (2010), são interativos no sentido de oferecer caminhos alternativos, por meio dos quais os agentes humanos podem ativar funções embutidas no objeto ou explorar os arranjos dos itens de informação subjacentes a ele e os serviços que ele medeia. Nesse sentido, a interatividade permite ações de natureza contingente (dependendo da escolha do usuário), uma condição que diferencia os objetos digitais dos objetos não contingentes, e reprime as respostas dos artefatos físicos e a natureza inerte do papel e de outros registros ou artefatos não digitais.

Abertura: É possível acessar e modificar objetos digitais, por meio de outros objetos digitais, bem como pelo acesso aos princípios ou regras subjacentes do programa que regem o comportamento do objeto digital ou seu código-fonte. Dessa forma, os objetos digitais são abertos e reprogramáveis no sentido de serem acessíveis e modificáveis por um programa (um objeto digital) diferente daquele que rege seu próprio comportamento. (KALLINIKOS; AALTONEN; MARTON, 2010).

Distribuição: Como resultados da interoperabilidade e abertura, os objetos digitais são distribuídos e, portanto, raramente são contidos em uma única fonte ou instituição, não sendo mais que montagens temporárias compostas de funções, itens de informação ou componentes espalhados por infraestruturas de informação e pela Internet. (KALLINIKOS; AALTONEN; MARTON, 2010). Os objetos digitais são transfronteiriços e, em comparação com as mídias empacotadas e únicas como os livros, as mídias em rede não têm uma borda identificável que as defina como uma entidade óbvia. Essas bordas têm que ser criadas e mantidas tecnologicamente. Além disso, a desburocratização possibilita várias combinações a partir de uma ecologia maior de itens, procedimentos e programas, uma condição que torna os objetos digitais fluidos e crucialmente transfiguráveis. (KALLINIKOS; AALTONEN; MARTON, 2010).

O objeto digital tem uma definição ambígua, afirma Thibodeau (2002), porque todos os objetos digitais são entidades com herança múltipla; ou seja, as propriedades de qualquer objeto digital são herdadas de três classes: um objeto físico, um objeto lógico e um

objeto conceitual, e suas propriedades em cada um desses níveis podem ser, significativamente, diferentes. Dessa forma, Thibodeau (2002) propõe a definição de três termos que especificavam o objeto digital de acordo com o contexto em que é expresso: Objetos Físicos, Objetos Lógicos e Objetos Conceituais.

Como um Objeto Físico, um objeto digital é simplesmente uma inscrição de sinais em um suporte. Basicamente, o nível físico trata de arquivos físicos que são identificados e gerenciados por algum sistema de armazenamento. A inscrição física é independente do significado das partes inscritas. No nível físico de armazenamento, o sistema de computador não sabe o que os *bits* significam. A inscrição física não implica morfologia, sintaxe ou semântica. (THIBODEAU, 2002).

As regras que regem um Objeto Lógico, aponta Thibodeau (2002), são independentes da maneira como os dados são escritos em um meio físico. Um objeto lógico é uma unidade reconhecida por um *software* de aplicação. Esse reconhecimento é tipicamente baseado no tipo de dado e um conjunto de regras para o reconhecimento digital, representando as informações. As regras que se aplicam no nível lógico determinam como a informação é codificada em *bits* e como as diferentes codificações são traduzidas para outros formatos;

O Objeto Conceitual é, para Thibodeau (2002), o objeto com o qual lidamos no mundo real: ele é uma entidade que reconhecemos como uma unidade significativa de informação, como um livro, um contrato, um mapa, ou uma fotografia. As propriedades dos objetos conceituais são aquelas que são significativas no mundo real. O conteúdo e a estrutura de um objeto conceitual devem ser contidos de alguma forma no objeto lógico ou nos objetos que o representam em forma digital. No entanto, o mesmo conteúdo conceitual pode ser representado em codificações digitais muito diferentes, e a estrutura conceitual pode diferir, substancialmente, da estrutura do objeto lógico.

UNESCO (2003) acrescenta que os objetos digitais se apresentam também "como feixes de elementos essenciais que encarnam a mensagem, objetivo ou características pelas quais o material foi escolhido para preservação[35]".

Para Kahn e Wilensky (2006), um objeto digital é uma estrutura de dados cujos componentes principais são material digital ou dados, mais um identificador exclusivo para esse material, chamado de identificador (e, talvez, outro material) [36].

---

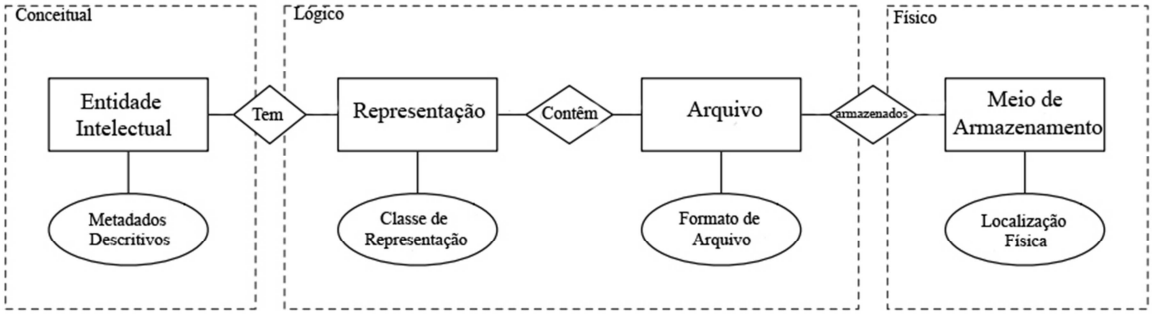
[35] Texto original: *As bundles of **essential elements** that embody the message, purpose, or features for which the material was chosen for preservation.*

[36] Texto original: *A digital object is a data structure whose principal components are digital material, or data, plus a unique identifier for this material, called a handle (and, perhaps, other material).*

Berg-Cross *et al.* (2015) consideram que um objeto digital é representado por um fluxo de *bits*, e é referenciado e identificado por um Identificador Persistente (PID[37]) e possui propriedades que são descritas por metadados[38].

A Figura 3 foi utilizada por Faria (2017), para ilustrar vários componentes que estruturam um Objeto Digital e os relaciona com os três níveis definidos por Thibodeau (2002):

FIGURA 3 - Estrutura de um Objeto Digital



FONTE: Faria (2017). Adaptado pelo autor.

No Nível Conceitual, temos a Entidade Intelectual e os Metadados Descritivos. A Entidade intelectual consiste num conjunto de conteúdo que é considerado uma única unidade intelectual para fins de gerenciamento e descrição. Por exemplo, um determinado livro, mapa, fotografia ou banco de dados. Uma Entidade Intelectual pode incluir outras entidades intelectuais. Por exemplo, um site pode incluir uma página da Web; uma página da Web pode incluir uma imagem. Uma entidade intelectual pode ter uma ou mais representações digitais. (LIBRARY OF CONGRESS, 2015).

Os Metadados Descritivos fornecem informações sobre o conteúdo intelectual de um objeto (ou seja, entidade intelectual) e também podem conter dados que descrevem os atributos físicos do objeto (no caso de haver uma contraparte análoga). Os metadados descritivos suportam tarefas específicas do usuário, tais como descoberta e identificação de conteúdo. (FARIA, 2017).

No Nível Lógico temos a Representação, com sua Classe de Representação, e o Arquivo e seu Formato de Arquivo. A Representação é o conjunto de arquivos, incluindo os

---

[37] *Persistent Identifier* (PID): Um identificador persistente é um identificador duradouro representado por uma cadeia de caracteres que identifica exclusivamente um objeto digital e que se destina a ser resolvido de forma persistente para informações significativas de estado sobre o objeto digital.

[38] Metadados: Em seu sentido mais estrito, metadados são dados sobre dados. Tais dados informativos incluem dados sobre modificação de arquivos, acesso, datas de criação, revisão e eliminação (BRITZ, 2013, p. 338, tradução do autor).

metadados estruturais, necessários para uma entrega completa e razoável de uma Entidade Intelectual. (FARIA, 2017).

Classe de Representação é um agrupamento de representações baseado em características técnicas para fins de preservação digital. (FARIA, 2017).

O Arquivo constitui-se de uma sequência nomeada e ordenada de *bytes*[39] que é conhecida por um sistema operacional. Um Arquivo pode ser zero ou mais bytes e tem um formato de arquivo, permissões de acesso e características do sistema de arquivo, como tamanho e data da última modificação. (LIBRARY OF CONGRESS, 2015).

O Formato do Arquivo consiste em um conjunto de regras sintáticas e semânticas para que o mapeamento entre um modelo de informação e um fluxo de *bits* serializado (FARIA, 2017).

No Nível Físico, temos o temos o Meio de Armazenamento e a Localização Física. Meio de Armazenamento é o meio físico no qual o objeto digital, representado por seus arquivos, é armazenado. Por exemplo, fita magnética, disco rígido. (LIBRARY OF CONGRESS, 2015).

Localização física consiste no local, posição ou endereço específico do meio de armazenamento (FARIA, 2017).

2.6 O DOCUMENTO ELETRÔNICO, O DOCUMENTO DIGITAL E O DOCUMENTO ARQUIVÍSTICO DIGITAL

Documento eletronico consiste em “informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável, por meio de um equipamento eletrônico.” (BRASIL, 2020). Salienta-se, ainda que, na literatura arquivística internacional, algumas vezes encontra-se o termo “documento eletrônico” como sinônimo de “documento digital”.

Documento digital consiste em “informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional.” (BRASIL, 2020).

Para International Research on Permanent Authentic Records in Electronic Systems (InterPARES, 2001a), o documento digital é “um componente digital, ou um grupo de componentes digitais, que é salvo, e que é tratado e gerenciado como um documento[40].”

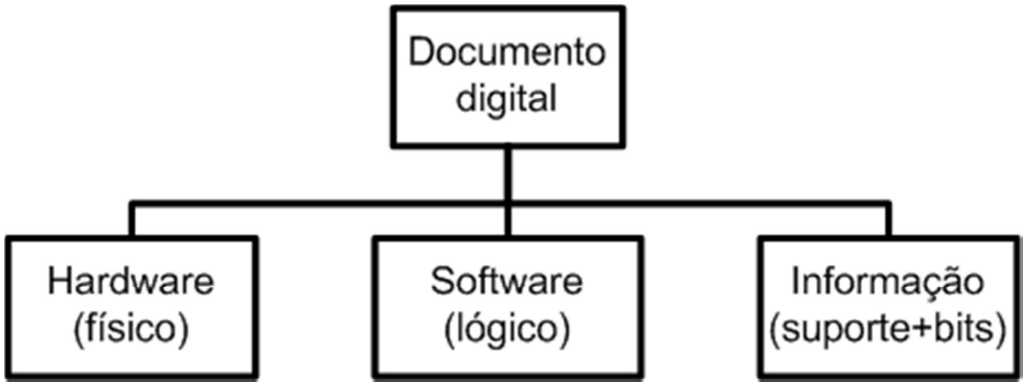
---

[39] Byte: O menor desses agrupamentos ocorre quando oito bits são combinados para formar um byte. Cada byte de dados representa uma letra, número ou caractere. Para exemplo, a sequência de dados brutos de 01000001 aparece para o usuário como a letra maiúscula "A" (BRITZ, 2013, p. 28, tradução do autor).

[40] Texto original: *A digital component, or group of digital components, that is saved and is treated and managed as a document.*

Innarelli (2015) apresenta a estrutura de um documento digital na Figura 4 em que apresentam-se os três elementos básicos de um documento digital: o *hardware*, o *software* e informação.

FIGURA 4 - Estrutura do documento digital



FONTE: Innarelli (2015).

Na estrutura, apresentam-se os elementos computacionais (*hardware e software*) e os elementos referentes ao suporte e às informações registradas na forma de *bits*. Inanrelli (2015) ressalta que essa visão não é consensual e que a principal discussão refere-se ao entendimento do terceiro item apresentado, o qual indica a informação (suporte+*bits*).

Uma distinção importante de ser feita entre documento nato-digital e documento digitalizado, segundo Innarelli (2015), é que o documento nato digital é aquele documento digital produzido diretamente em formato digital e tem todo o seu ciclo vital em meio digital. Para o mesmo autor, o documento digitalizado é o documento digital produzido por meio do processo de conversão de um documento analógico para o formato digital, por dispositivo apropriado, como um escâner.

Destaca-se que ambos são documentos digitais (o nato digital e o digitalizado), pois em sua forma final dependem do hardware, do software e do suporte+informação para serem processados e manifestados. O que os diferencia é a forma de produção. Enquanto que, no documento digitalizado, a produção é feita a partir de um documento analógico, por meio de um dispositivo computacional de digitalização, no documento nato digital, a produção ocorre diretamente em formato digital, por meio de um sistema informatizado ou de um equipamento computacional. O entendimento dos modos de produção é de fundamental importância, visto que influencia diretamente nos processos de gestão de sua preservação (INNARELLI, 2015).

Um documento arquivístico digital consiste, de acordo com Neves e Innarelli (2014), em informação gerada no exercício das atividades e funções de uma pessoa física

ou jurídica e registrada em qualquer suporte ou tecnologia integra o arquivo da mesma. Em outras palavras, é um documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema informatizado.

O documento arquivístico digital pode ser definido, de acordo com Brasil (2020), como “documento digital reconhecido e tratado como um documento arquivístico”, ou seja, documentos produzidos, recebidos e acumulados em razão de atividades administrativas, legais, informativas.

Com esta pesquisa, baseando-se nos conceitos apresentados anteriormente sobre objeto digital e, ao mesmo tempo, relacionando-os com os conceitos referentes aos documentos arquivísticos digitais, conclui-se que o documento arquivístico digital pode ser caracterizado como um objeto digital produzido, recebido e acumulado em razão de atividades administrativas, legais ou informativas, diferenciando-os de outros documentos digitais em razão de seu contexto de produção.

Ao contrário de um documento arquivístico analógico, relata Millar (2009a), um documento arquivístico digital pode ser manipulado, transmitido ou processado por um computador. Um documento arquivístico digital é um registro que é criado, gerado, enviado, comunicado, recebido ou armazenado por meios eletrônicos e isso requer alguma forma de tecnologia informática para acesso e uso.

As informações digitais, explica Millar (2009a), são compostas de “zeros” e “uns” - *bits* - para formar um *byte*. Um *byte* consiste em oito *bits* ou uma combinação totalizando oito “zeros” e “uns” que representam um caracter. Por exemplo, um “H” maiúsculo é representado em código binário como 01001000. Um “h” minúsculo é representado como “01101000”. Os *bytes* múltiplos são formados para criar uma palavra ou uma imagem.

> Um documento arquivístico digital é composto dos *bits* (representação digital) e de um registro observável ou produto perceptível gerado a partir dos *bits*. O produto, que pode ser visível, como um documento de texto, ou audível, como uma gravação sonora, é criado imediatamente à medida que a pessoa insere dados ou instruções no computador, usando um teclado ou outro dispositivo (MILLAR, 2009a, p. 23).

Para “criar” um documento arquivístico digital, conclui Millar (2009a), nem o produto perceptível nem a representação digital podem ser separados. Em outras palavras, a fim de gerar esse produto observável, novamente, a qualquer momento no futuro, é necessário preservar a representação digital - os *bits* - de uma forma estável e segura. A preservação de um documento arquivístico digital envolve a preservação da capacidade de recriar aquele produto observável repetidamente, com o intuito de que o documento arquivístico continue a cumprir o propósito para o qual foi criado.

Algumas características únicas dos documentos arquivísticos digitais influenciam as estratégias e métodos de trabalho eficazes para sua gestão e preservação no longo prazo. As seis características seguem elencadas a seguir, distinguindo os documentos arquivísticos digitais daqueles em forma “tradicional”:

> 1. **Gravação e o uso de símbolos**: O conteúdo de um documento arquivístico digital é registrado de uma forma e em um meio de alta densidade (em um registro magnético ou dispositivo ótico) que não pode ser acessado diretamente (lido) por um ser humano, e é representado por símbolos (dígitos binários) que devem ser decodificados. Em geral, quando um documento arquivístico digital é produzido e armazenado, ele é transferido e transformado de um formato legível por humanos para um formato legível por máquinas. Esta versão legível por máquina é a informação registrada que constitui o arquivo (ICA, 1997, p. 25).

Para a recuperação do documento arquivístico digital, ICA (1997) aponta-se que a transferência e a transformação vão por outro caminho. Como os seres humanos não podem ler um documento arquivístico digital como ele é, é crucial que a transformação de volta ao formato legível pelo ser humano siga as mesmas especificações como foram utilizadas para a transformação, em primeiro lugar. Para conseguir isto, é necessário não apenas preservar o documento arquivístico digital mas também é necessário acesso ao equipamento (*hardware e software*) para “ler” o arquivo e fazer as transformações corretas somadas aos controles para garantir que o que se vê é o que está registrado.

> 2. **Conexão entre o conteúdo e a mídia**: O conteúdo de um documento arquivístico tradicional é gravado em um meio de armazenamento, como um pedaço de papel e não pode ser separado desse meio. O conteúdo de um documento arquivístico digital é também registrado em um meio, mas de tempos em tempos é necessário separá-lo do dispositivo original e transferi-lo a outros tipos, e muitas vezes, de diferentes dispositivos de armazenamento, por conta da obsolescência tecnológica. Ao contrário dos arquivos tradicionais, um documento arquivístico digital não é, portanto, permanentemente anexado a um meio ou dispositivo de armazenamento específico, de modo que as oportunidades de corrupção aumentam. Isso apresenta problemas adicionais para garantir que a autenticidade e a confiabilidade do documento arquivístico digital sejam mantidas.
>
> 3. **Características da estrutura física e lógica**: A estrutura de um documento arquivístico analógico é, de acordo com ICA (1997), aparente para o usuário. A estrutura é parte integrante de qualquer documento em papel, e um dos principais critérios para avaliar sua autenticidade.A estrutura física de um documento arquivístico digital não é facilmente aparente, e normalmente desconhecida para o usuário comum. É resultado da estrutura que o produtor criou em sua tela, mas depende também do sistema informático (*hardware e software*) e do espaço disponível no dispositivo de armazenamento (por exemplo, o disco rígido, pendrive). Toda vez que o documento arquivístico digital é transferido para outro dispositivo, a estrutura física pode mudar. O usuário sempre precisará de um sistema de computador que seja capaz de recuperar o registro, e que, portanto,

deve ser capaz de “ler” a estrutura física. Mas, exceto por isso, a estrutura física será de nenhum valor e sem interesse para ele. Ou seja, o documento arquivístico digital não depende de nenhuma gravação. ICA (1997) explana que, em razão da estrutura física de um documento arquivístico digital ser variável e não facilmente visível, não pode desempenhar o mesmo papel que para os documentos arquivísticos tradicionais (analógicos). Portanto, há necessidade de uma estrutura lógica que permita identificar (delimitar) cada documento arquivístico digital e representar seus elementos estruturais internos (como campos em um esquema ou tabela, margens, parágrafos, etc.). Essa estrutura lógica de um documento arquivístico digital será, em geral, a estrutura que o produtor criou em sua tela. Para que seja considerado completo e autêntico, o documento arquivístico deve preservar essa estrutura de alguma forma, e o sistema de computador deve reconstruí-la ao transformar o documento arquivístico digital de volta para um formato legível pelo ser humano. A estrutura lógica de um documento arquivístico digital é representada e armazenada como símbolos ou dados (dígitos binários). Assim, as especificações dessa codificação devem estar disponíveis para qualquer recuperação do documento arquivístico.

4. **Metadados**: Este é um conceito importante para os documentos arquivísticos digitais porque metadados sobre o contexto e a estrutura de um documento arquivístico são necessários para que o documento seja compreensível e utilizável. Como declarado no conceito de um documento arquivístico, a informação sobre o contexto é um dos elementos necessários para fornecer evidência da atividade que o documento representa. Os documentos arquivísticos digitais carecem de certos elementos dos documentos arquivísticos tradicionais que contribuem para estabelecer a relação entre um documento de arquivo e seu contexto funcional e administrativo. Assim, os documentos arquivísticos digitais são fortemente dependentes não apenas de um contexto administrativo bem documentado, mas de metadados que descrevam como as informações são registradas. Metadados que mapeiam os dados administrativos e relações documentais entre itens individuais dentro de um sistema particular de *record keeping,* durante o ciclo de vida daquele documento, fornecem parte do contexto do registro que deve ser preservado. .

5. **Identificação dos *records***: Um documento arquivístico digital não pode ser identificado por meio de ser uma entidade física, mas constitui, ao invés disso, conclui ICA (1997), como entidade lógica, que é o resultado de uma transação ou fornece provas de uma atividade. Em muitos casos, tais entidades (isto é, documentos arquivísticos digitais) têm um paralelo nos registros correspondentes em papel, como cartas, contratos, memorandos, registros, etc. Em outros casos, os paralelos aos documentos arquivísticos tradicionais correspondentes são menos óbvios ou podem estar ausentes (por exemplo, no caso de alguns tipos de bancos de dados, hipertexto, planilhas eletrônicas, multimídia, etc. Sistemas).

6. **Preservação dos documentos ao longo do tempo**: Preservar os documentos tradicionais significa armazenar unidades físicas (folhas de papel, volumes, etc.) nas melhores condições possíveis, a fim de evitar danos, e para reparar danos se e quando ocorre. A preservação de documentos arquivísticos digitais requer que as unidades físicas (os meios de armazenamento) sejam armazenadas nas melhores condições possíveis, mas independentemente de quão boas sejam essas condições, as informações digitais ‘desaparecerão’ após um período de tempo bastante curto (cinco a trinta anos, dependendo do tipo de suporte). Além disso, a maioria dos sistemas de computação estão fadados a ficarem obsoletos em um período de tempo ainda mais curto. Assim, a fim de preservar os

> documentos arquivísticos digitais, eles devem, de tempos em tempos, ser migrados para novos sistemas e plataformas tecnológicas, ou seja, ser copiados para novos dispositivos de armazenamento e, em alguns casos, convertidos para um formato adequado para novos sistemas informáticos. (ICA, 1997, p. 26).

Segundo Millar (2009a), os documentos arquivísticos digitais têm três atributos importantes: conteúdo, contexto e estrutura.

> - Conteúdo é o que diz o registro.
>
> - Estrutura diz respeito tanto à aparência quanto à disposição do conteúdo (para exemplo, o layout, fontes, quebras de página e parágrafo, tabelas, gráficos, quadros e assim por diante) e a relação física ou, mais apropriadamente, lógica do documento a outros documentos relacionados no sistema (por exemplo, onde um documento é encontrado em uma pasta de arquivos ou em um diário vinculado).
>
> - Contexto é a informação de fundo que ajuda a explicar o significado do documento. Uma informação identifica o documento em particular, tal como o título, autor e data de criação. Outro elemento de informação identifica o criador e o propósito da criação, tais como a natureza do negócio função ou atividade ou a agência e unidade criadora em questão[41]. (MILLAR, 2009a, p. 22, Tradução nossa).

Segundo Millar (2009), o conteúdo, o contexto e a estrutura dos registros devem ser preservados ao longo de sua vida útil; caso contrário, sua integridade será afetada, e eles podem não ter mais o mesmo significado ou não ser mais compreensíveis. A qualidade das informações extraídas dos documentos arquivísticos depende da preservação da integridade dos registros.

2.7 A DIPLOMÁTICA ARQUIVÍSTICA DIGITAL

A questão da falsificação de documentos está, segundo Tognoli (2013), presente na história das civilizações, desde a Antiguidade, uma vez que a autenticidade documental não era uma característica intrínseca ao documento, sendo atribuída a ele, de acordo com a instituição na qual estava armazenado.

---

[41] Texto original: *Content is what the record says.*
- Structure relates to both the appearance and arrangement of the content (for example, the layout, fonts, page and paragraph breaks, tables, graphs, charts and so on) and the physical or, more appropriately, logical relationship of the record to other related records in the system (for example, where a document is found in a file folder or in a bound journal).
- Context is the background information that helps explain the meaning of the document. One piece of information identifies the particular document, such as the title, author and date of creation. Another piece of information identifies the creator and the purpose of creation, such as the nature of the business function or activity or the creating agency and unit concerned.

> Na Antiguidade, a autenticidade era uma característica atribuída ao documento de acordo com o local no qual ele era depositado. Quando os cidadãos precisavam legitimar seus documentos para provar deveres e direitos, depositavam-nos em templos ou depósitos públicos (*dépôt publics*), que garantiam a eles fé pública, considerando-os monumentos incorruptíveis. (TOGNOLI, 2013, p. 21).

Nesse sentido, registrou-se, na Idade Média, uma maior preocupação com a aplicação de normas para a confecção de documentos, emergindo, assim, um período de grande importância para o espírito crítico, no qual a consciência da força de um documento escrito foi manifestada.

> A história da Diplomática está fundamentalmente ligada à das falsificações. Buscando enunciar métodos e elementos para a verificação da autenticidade/falsidade de documentos, várias obras foram escritas. Essas obras constituem-se, na maioria, de tratados e manuais redigidos durante o Antigo Regime e a Época Moderna e, embora possuíssem objetivos diferentes, foram, ao longo dos anos, se complementando para formar as bases teóricas da Diplomática. Enquanto os tratados escritos no Antigo Regime tinham como objetivo comprovar a autenticidade dos documentos para fins prático-jurídicos, os manuais modernos buscavam também identificar elementos para provar a autenticidade de documentos medievais que eram utilizados como fonte para a História. (TOGNOLI, 2013, p. 19).

A Diplomática é, segundo Delmas (2015), a ciência que estuda os documentos de arquivo propriamente ditos, em sua condição de documentos a partir de sua elaboração, sua forma e sua transmissão, para julgar sua autenticidade e considerar seu valor de testemunho e de informação.

> Os princípios e métodos de diplomáticos foram estabelecidos em 1681, em um tratado escrito pelo monge beneditino Jean Mabillon chamado *De Re Diplomatica* que analisou, entre outras coisas, a língua dos documentos, suas partes características, seus selos, e os sistemas de cronologia usados. Com base nesse exame, Mabillon afirmou que, para um determinado tempo e lugar, a forma correta para um documento genuíno, e apresentou os princípios gerais da Diplomática. O uso original da Diplomática foi determinar a autenticidade de um registro para fins legais; o que continuou até o século XVIII, quando muitas faculdades de Direito Europeu incorporaram seus conceitos e princípios em seus currículos. (InterPARES, 2001a p. 2).

Segundo Rondinelli (2013, p. 140):

> O final do século XX e começo do XXI são marcados por novos desafios estabelecidos com a chegada dos documentos digitais. Os desafios tiveram impactos tanto na Diplomática quanto na Arquivologia. O momento exige que a análise documental se aprofunde na gênese do documento, nos

> elementos de forma e identificação do o status de transmissão, assim como a Arquivologia, que deve contribuir para classificação, temporalização, descrição e preservação.

A associação das teorias da Arquivologia e da Diplomática,no que tange à gênese, constituição e transmissão dos documentos arquivísticos, bem como seu relacionamento contextual no que diz respeito às ações, funções e produtores, conclui Tognoli (2018), pode ser definida como Diplomática Arquivística..

Nesse contexto, Mogollón e Rodríguez (2019, p. 55) afirmam que “as autoras Paola Carucci e Luciana Duranti foram pioneiras em desenvolver um tipo de Diplomática Especial, destinado ao contexto digital, ao adaptar metodologias e teorias da Diplomática Tradicional para documentos da moderna burocracia italiana.”

> Os estudos pioneiros sobre essa nova abordagem foram elaborados no contexto do Projeto InterPARES (*International Research on Permanent Authentic Records in Electronic Systems Project*[42]) que reuniu profissionais de diferentes áreas e países, entre os anos 1999 e 2019, com o objetivo de desenvolver o conhecimento necessário para preservar documentos arquivísticos digitais autênticos no longo prazo e criar diretrizes para garantir, além da preservação dos materiais digitais, a segurança quanto a sua autenticidade e confiabilidade. (InterPARES, 2001a).

O Projeto InterPARES foi resultado do crescente interesse nos resultados do projeto de pesquisa ‘Preservação da Integridade dos Registros Eletrônicos’, comumente chamado de Projeto UBC, que foi realizado na Universidade da British Columbia, Escola de Biblioteca, Arquivo e Estudos de Informação, em 1997. “O Projeto UBC definiu os requisitos para a criação, manipulação e preservação de documentos arquivísticos nas fases corrente e intermediária eletrônicos confiáveis.” (INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS - InterPARES, 2001b). Os pesquisadores do Projeto InterPARES foram organizados em equipes nacionais e multinacionais para dois propósitos:

> - Assegurar o financiamento a partir de fontes distintas e;
>
> - Trabalhar como unidades de investigação que partilham de um contexto jurídico-administrativo comum, num esforço internacional multidisciplinar onde grupos de diversas origens culturais e acadêmicas investigaram soluções universais para problemas comuns. (InterPARES, 2001a).

O Projeto InterPARES desenvolveu o conhecimento teórico e metodológico essencial para a preservação permanente de registros gerados, eletronicamente, e, com

[42] Pesquisa Internacional sobre Registros Autênticos Permanentes em Sistemas Eletrônicos. Tradução do Autor.

base nesse conhecimento, para formular estratégias, modelos, políticas e normas capazes de garantir a sua preservação. Para atingir esse objetivo, a pesquisa foi organizada em quatro domínios de investigação; sendo que uma força-tarefa correspondente foi formada para lidar com as questões de pesquisa específicas para cada domínio. (InterPARES, 2001b). São elas:

a) Força-Tarefa de Autenticidade;
b) Força-Tarefa de Avaliação;
c) Força Tarefa de Preservação;
d) Força Tarefa de Estratégia.

O objetivo da Força-Tarefa de Autenticidade era identificar os requisitos conceituais para avaliar e manter a autenticidade dos registros eletrônicos. Seu principal resultado foi o desenvolvimento de dois conjuntos de requisitos:

> - Requisitos que sustentam a presunção de autenticidade de registros eletrônicos antes de serem transferidos para a custódia do preservador; e
> - Exigências que suportem a produção de cópias autênticas de registros eletrônicos após terem sido transferidos para a custódia do preservador (InterPARES, 2001b).

Um documento arquivístico digital , visto da perspectiva da Diplomática Arquivística Contemporânea, como seu equivalente analógico, é, de acordo com International Research on Permanent Authentic Records in Electronic Systems (InterPARES, 2020c), um complexo de elementos e suas relações. Ele possui uma série de características identificáveis, incluindo uma forma documental fixa, um conteúdo estável, ligação com outros registros, e um contexto identificável. Participa ou apoia uma ação, seja processualmente ou como parte do processo de tomada de decisão e pelo menos três pessoas (autor, escritor e destinatário) estão envolvidos em sua criação (embora essas três pessoas conceituais possam de fato, ser apenas uma pessoa física ou jurídica).

2.8 ESTRATÉGIAS PARA PRESERVAÇÃO DIGITAL NO LONGO PRAZO

A preservação digital envolve, de acordo com UNESCO (2003), a escolha e implementação de uma variedade crescente de estratégias, atendendo às necessidades de preservação das diferentes camadas dos objetos digitais. As estratégias incluem a preservação de três níveis: o físico, o conceitual e o lógico.

Preservação do nível físico

As estratégias para manter o nível físico dos objetos digitais, também chamadas de técnicas de preservação em nível de *bits*, são bem conhecidas na tecnologia da informação, e são empregadas em muitos domínios.

> Estas estratégias incluem, mas não estão restritas à atualização da mídia de armazenamento, backup *point-in-time*, redundância de dados online (por exemplo, RAID[43]), federação de dados (por exemplo, LOCKSS[44], Grid[45], HDFS[46]) e verificações periódicas de correção de arquivos, que são comumente compreendidas e utilizadas por especialistas em gerenciamento de informações[47]. (FARIA, 2017, p. 8).

Preservação do nível lógico

A sequência lógica deve ser armazenada em um objeto físico, esclarece Thibodeau (2002). Ela pode ser congruente com um objeto físico. A maneira como os arquivos são armazenados é irrelevante no nível lógico, desde que os objetos contidos estejam nos lugares apropriados quando a informação é emitida. Isso exige que cada objeto lógico tenha seu próprio identificador persistente, e que o local onde cada objeto é armazenado deve ser especificado. Mais importante, para preservar a informação digital como objetos lógicos, temos que conhecer os requisitos para o processamento correto do tipo de dado de cada objeto e qual *software* pode realizar o processamento correto.

Preservação do nível conceitual

Embora a preservação do nível conceitual seja assegurada até certo ponto pela preservação do nível físico e do nível lógico, há riscos no nível conceitual que não são cuidados nos níveis inferiores, aponta Thibodeau (2002). Da mesma forma que no nível lógico, para que uma entidade intelectual seja corretamente compreendida pelo usuário é necessário que haja um contexto conceitual compartilhado. Assim como em um documento analógico, um usuário pode precisar compreender a linguagem em que as informações são descritas, pode ser necessário conhecer alguns conceitos, reconhecer algum objeto físico, estar atento de algum domínio de conhecimento ou ter um contexto social comum.

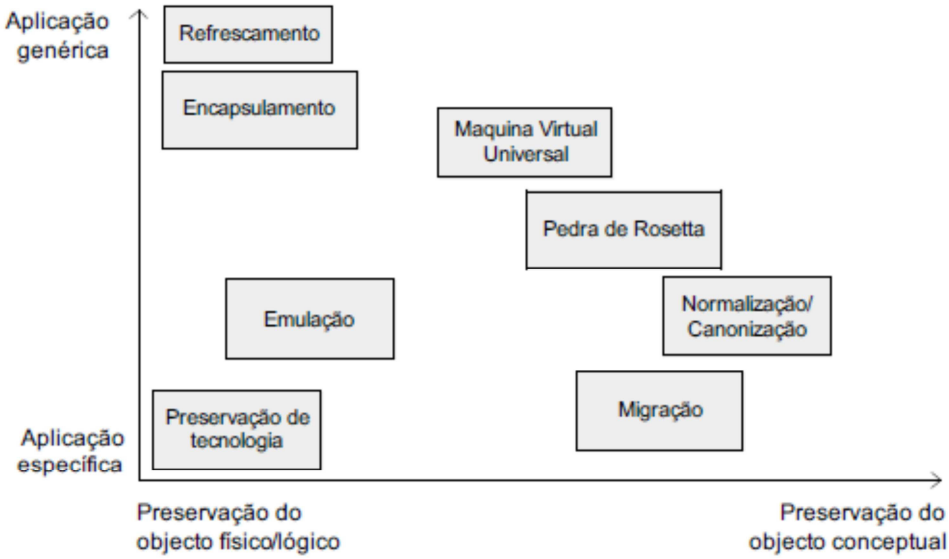
---

[43] *Redundant Array of Independent Disks*
[44] *Lots of Copies Keep Stuff Safe.*
[45] *Global Research Identifier Database*
[46] *Hadoop Distributed File System.*
[47] *These strategies include, but are not restricted to, storage media refresh, point-in-time backup, online data redundancy (e.g. RAID), data federation (e.g. LOCKSS, Grid, HDFS) and periodic file fixity checks, which are commonly understood and used by information management experts.*

Na Figura 5, mostra-se uma série de métodos diferentes posicionados em relação a dois exios: o eixo das ordenadas, voltado para a aplicação dos métodos de preservação digital, partindo do específico para o genérico, numa ascendente. No eixo das abscissas, nota-se a preservação do objeto digital, numa crescente, partindo dos níveis físicos e lógicos, em direção ao nível conceitual de preservação. Pode observar-se que a figura não contempla todos os métodos de preservação digital, como, por exemplo, metadados de preservação.

Thibodeou (2002) deu ênfase em mostrar uma variedade de maneiras de superar a obsolescência tecnológica. O primeiro propósito foi mostrar a robustez da grade como uma estrutura para caracterizar e avaliar métodos de preservação. O segundo foi enfatizar para aqueles que são preocupados com a preservação digital que precisam estar abertas às possibilidades que a Tecnologia da Informação está constantemente criando. O terceiro objetivo foi refletir sobre o fato de que, no ambiente digital, a preservação não se limita à transmissão digital informações ao longo do tempo. Portanto, métodos desenvolvidos para possibilitar a transmissão de informações confiáveis e autênticas, por meio de um desses tipos de limites podem ser aplicáveis através de outros.

FIGURA 5 - Classificação das diferentes estratégias de Preservação Digital



FONTE: Ferreira (2006). Adaptado de Thibodeau (2002).

2.9 PRINCIPAIS ESTRATÉGIAS DE PRESERVAÇÃO DIGITAL

Segundo Márdero Arellano (2008, p. 61):

> Os principais métodos recomendados para a preservação dos objetos digitais podem ser agrupados em dois tipos: os estruturais e os operacionais. Os métodos estruturais lidam dos investimentos iniciais por parte das instituições que estão se preparando para implementar algum processo de preservação e que adotam ou adaptam um dos modelos de metadados existentes ou seu próprio esquema. Já as atividades operacionais são as medidas concretas aplicadas aos objetos digitais.

No Quadro 1, apresentam-se os métodos de preservação digital mais utilizados.

QUADRO 1 - Métodos de preservação digital

Métodos Estruturais	**Métodos Operacionais**
-Adoção de padrões	-Conservação de *software/hardware*
-Elaboração de normas	-Migração de suporte
-Formação de consórcios	-Preservação do conteúdo
-Metadados de preservação digital	-Conversão de formatos
-Montagem de infraestrutura	-Emulação

FONTE: Arellano (2008, p. 61).

Preservação de Tecnologia

Essa estratégia consiste, de acordo com Ferreira (2006, p. 32), “na conservação e manutenção de todo o hardware e software necessários à correta apresentação dos objetos digitais”. Trata-se sobretudo da criação de museus de tecnologia. O foco da preservação não se concentra no objeto conceitual, mas na preservação do objeto digital na sua forma original. Os impulsionadores dessa estratégia consideram-na a única forma suficientemente eficaz para assegurar que os objetos digitais são experimentados de forma fidedigna.

> A preservação de tecnologia implica a conservação e manutenção de todo o *hardware* e *software* necessários à correta apresentação dos objetos digitais. Neste âmbito, o foco da preservação concentra-se, não no objeto conceitual, mas sim na preservação do objeto digital na sua forma original. (BARBEDO; CORUJO; SANT’ANA, 2011, p. 52).

Algumas desvantagens apresentadas por Barbedo; Corujo; Sant’ana (2011) na preservação de tecnologia são:

- O fato de qualquer plataforma tecnológica acabar por se tornar obsoleta;

- A existência de dificuldades na gestão do espaço físico;

- A manutenção e custos de operação;

- O fato do acesso à informação estar limitado a alguns locais físicos do globo e com condicionalismos acrescidos ao nível da reutilização da informação.

Verificou-se, nesta pesquisa, que a preservação de tecnoclogia apresenta-se como uma estratégia ineficaz, uma vez que o decaimento magnético dos suportes de armazenamento, compostos de ligas de Ferro, Cobalto, entre outros metais, é uma característica instrínseca destes elementos, que levará, ao cabo de cerca de 4 décadas ou menos, à perda das orientações magnéticas das nanopartículas, interpretadas como bits pelas cabeças de leitura dos drives de disco rígido.

Emulação

A emulação corresponde, de acordo com Barbedo, Corujo e Sant'ana (2011, p. 52), "à utilização de um *software,* denominado emulador, que é capaz de reproduzir o comportamento de uma plataforma de *hardwar*e e/ou *software*, numa outra plataforma que, em princípio, seria incompatível."

As principais vantagens da emulação incluem, relatam Barbedo, Corujo e Sant'ana (2011, p. 53):

> O fato de preservar, de forma fiel, as características e as funcionalidades do objeto digital original e, embora foque na preservação do objeto lógico no seu formato original, não sofre de alguns dos problemas da estratégia de preservação de tecnologia como, por exemplo, o envelhecimento do *hardware*. No entanto, uma das desvantagens é que o emulador pode tornar-se obsoleto e a sua utilização pressupõe que os utilizadores do futuro sejam capazes de operar adequadamente aplicações e sistemas operacionais há muito desaparecidos.

Explica Ferreira (2006) que existem dois tipos de emuladores: emuladores de sistemas operativos e de hardware. Os emuladores de sistemas operativos focam na reprodução de um sistema operativo por completo, permitindoa execução de diversas aplicações no contexto de um único emulador. Os emuladores de *hardware* visam a simular o comportamento de uma plataforma de hardware, possibilitando que vários sistemas operativos e aplicações correspondentes possam ser executados no contexto de um único emulador.

Monitorização de suportes e formatos

"A monitorização de suportes e formatos prevê processos de verificação automática, manual e semiautomática dos objetos digiais." (BARBEDO; CORUJO; SANT'ANA, 2011, p. 52). As preocupações da monitorização prendem-se com as seguintes questões:

a) Tempo de vida estimado dos suportes;
b) Tempo médio de prevalência de uma versão de *software*;
c) Retrocompatibilidade assegurada pelos fabricantes.

Encapsulamento

O encapsulamento, de acordo com Barbedo, Corujo e Sant'ana (2011, p. 53), "consiste em preservar, juntamente com o objeto digital, toda a informação necessária e suficiente para permitir o futuro desenvolvimento de conversores, visualizadores." O encapsulamento está orientado a objetos que apenas serão acessados num futuro distante. Permite adiar a responsabilidade de preservação, e o desenvolvimento futuro de visualizadores, migradores ou emuladores.

O conceito, por trás do encapsulamento, de acordo com International Records Management Trust (IRMT, 2016, p. 64) é que os registros digitais a serem preservados devam ser "autodescritivos, na medida em que o conteúdo do registro contém todos os metadados necessários." Isso é realizado, utilizando-se *wrappers*[48] XML[49] que encapsulam o registro e contêm os metadados, descrevendo as relações lógicas:

a) entre os componentes do registro
b) entre o registro e o processo que o gerou e quaisquer outros metadados necessários para entender o registro.

A desvantagem, porém, é a necessidade de estar ciente que objetos complexos possuem especificações complexas e que uma especificação incompleta poderá ter um efeito desastroso para a preservação do objeto digital.

Migração e transferência de suporte

[48] Embrulhos. Tradução do autor.
[49] Sigla para *eXtensible Markup Language*, é um tipo de linguagem de marcação que define regras para codificar diferentes documentos.

"Migração é a transferência periódica de materiais digitais de uma configuração de *hardware/software* para outra, ou de uma geração de computadores com determinada tecnologia para uma geração subsequente", afirma a Garret e Walters (1996, p. 6).

> O objetivo da migração é preservar a integridade dos objetos digitais e para manter a capacidade de recuperação dos clientes, e, de outra forma, usá-las em face da tecnologia em constante mudança. A migração inclui a atualização como um meio de preservação digital, mas difere no sentido de que nem sempre é possível fazer uma cópia digital exata ou réplica de um banco de dados ou outro objeto de informação, como hardware e software mudam, bem como ainda manter a compatibilidade do objeto com a nova geração da tecnologia. (GARRET; WALTERS, 1996, p. 6).

A migração de formatos e suportes refere-se, de acordo com Barbedo, Corujo e Sant'ana (2011, p. 53), à transferência de documentos contidos num determinado suporte ou formato para outro suporte ou formato mais atualizado. É o processo responsável pela reorganização dos elementos de informação que constituem um objeto digital. Foca-se, sobretudo, na preservação do seu conteúdo intelectual, ou seja, na preservação do objeto conceitual e na verificação frequente da integridade dos suportes físicos. O principal objetivo é evitar a obsolescência tecnológica, mantendo os objetos digitais compatíveis com as tecnologias atuais, de forma a permitir a sua interpretação sem necessidade de recorrer a artefactos menos convencionais. A migração prevê processos de:

a) Refrescamento no nível de suportes;
b) Processos de migração entre formatos;
c) Transposição conjunta de formatos e suportes.

O Refrescamento refere-se, de acordo com IRMT (2016), à leitura e reescrita de dados armazenados para garantir que os dados sejam retidos com precisão. Isso pode ocorrer quando o hardware e/ou os meios de armazenamento estão sendo atualizados para aproveitar os avanços tecnológicos (por exemplo, aumento da capacidade de armazenamento), para reduzir custos ou para acomodar novas exigências comerciais. Essa transposição de formatos e suportes apresenta, entretanto, algumas desvantagens como:

> - Probabilidade de algumas propriedades dos objetos digitais não serem corretamente transferidas para o formato de destino adotado;
>
> - Existência de incompatibilidades entre os formatos de origem e destino;
>
> - Inadequação dos conversores;
>
> - Obsolescência de formatos (BARBEDO; CORUJO; SANT'ANA, 2011, p. 53).

> Durante a transposição de documentos para novos formatos existe, ainda, a possibilidade de perda de informação no nível da estrutura, de metadados e, por vezes, do conteúdo. Em face da possibilidade de perda de informação, deve recorrer-se a estratégias que incluam documentar exaustivamente o processo de migração (através de metadados). Desta forma tenta-se garantir que o que se perde não compromete a autenticidade e fidedignidade do documento (BARBEDO; CORUJO; SANT'ANA, 2011, p. 54).

Existem algumas variantes no caso específico da transferência de formatos:

a) Atualização de versões

A atualização de versões é, segundo Ferreira (2006) a estratégia de preservação mais vulgarmente utilizada. Essencialmente, consiste em atualizar os materiais digitais produzidos por um determinado software, recorrendo a uma versão mais atual do mesmo software.

b) Conversão para formatos concorrentes

Uma forma de garantir que os objetos digitais sobrevivam a rupturas tecnológicas que levem à descontinuidade de determinado software, consiste em convertê-los para formatos de uma linha de produtos concorrentes. "Permite ultrapassar o risco de descontinuidade de formatos, convertendo objetos digitais para formatos análogos, independentemente da aplicação utilizada na sua criação." (FERREIRA, 2006, p. 38).

c) Normalização

Corresponde à migração para um número reduzido de formatos compatíveis, o que poderá evitar futuras complicações no nível de direitos autorais ou pagamento de *royalties*. Promove, também, a interoperabilidade entre sistemas distintos. "O fato de serem utilizados formatos abertos e independentes da plataforma permite que diferentes configurações de *hardware* e *software* sejam capazes de interpretar os objetos digitais." (BARBEDO; CORUJO; SANT'ANA, 2011, p. 54).

A normalização, segundo Garrett e Waters (1996, p. 6), envolve:

> [...] a conversão de registros digitais para um formato padrão para reduzir o número de formatos que devem ser gerenciados. A retenção de registros digitais em muitos formatos diferentes pode ser desafiador e caro. Os formatos e o software de suporte devem ser monitorados regularmente para garantir que não sejam obsoletos ou que sua integridade não tenha sido corroída por mudanças na tecnologia. O uso de formatos-padrão reduz o

> risco para a integridade dos registros, tornando possível o acesso a eles por meio de *software* que suporta os formatos padrão[50].

d) Migração a pedido

Nessa estratégia, os registros digitais só são convertidos quando há um pedido para eles.

> Os registros são deixados em seu formato nativo, e uma ferramenta de conversão para fins especiais é desenvolvida para garantir que, se houver solicitação, os registros selecionados possam ser convertidos para um formato que possa ser lido e compreendido. Isto economiza os custos de conversão de séries inteiras de registros digitais. Esta é uma estratégia útil quando é provável que apenas alguns poucos registros sejam acessados. Há o risco de que os registros, caso dependam de uma única ferramenta tecnológica, possam se tornar inacessíveis ao longo do tempo, mas esta abordagem elimina ou reduz muito os custos de conversão[51]. (IRMT, 2016, p. 62).

Nesse tipo de migração, Ferreira (2006, p. 40) disserta que, "ao invés de as conversões serem aplicadas ao objeto digital mais atual, as migrações serão aplicadas ao objeto original". Assim, se de uma dada conversão resultar num objeto substancialmente diferente do original, numa futura conversão, o problema poderá ser resolvido, recorrendo-se a um conversor de melhor qualidade ou a um formato de destino mais adequado.

---

[50] Texto original: *converting digital records to a standard format to reduce the number of formats that must be managed. Retaining digital records in many different formats can be challenging and costly. The formats and supporting software must be monitored regularly to ensure that they are not obsolete or that their integrity has not been eroded by changes in the technology. Using standard formats reduces the risk to the integrity of the records making it possible to access them by software that supports the standard formats.*

[51] Texto original: *The records are left in their native format, and a special-purpose conversion tool is developed to ensure that if there is request, the selected records can be converted to a format that can be read and understood. This saves the costs of converting entire series of digital records. This is a useful strategy when it is likely that only a few records will be accessed. There is the risk that the records, if they are dependent on a single technology tool, could become inaccessible over time, but this approach does eliminate or greatly reduce the costs of conversion.*

3 REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS E O MODELO DE REFERÊNCIA OPEN ARCHIVE INFORMATION SYSTEM - OAIS

No intuito de investigar o conceito Repositório Arquivístico Digital Confiável, abordado nas *Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis* (RDC-Arq), elaboradas pelo Conselho Nacional de Arquivos, buscaram-se definições em fontes conceituais de produções científicas voltadas à preservação digital no longo prazo. Para tanto, foram utilizadas consultadas as publicações elencadas no RDC-Arq, uma vez que forneceram seus alicerces terminológicos.

Num sentido crescente de complexidade, buscou-se informações a respeito da abstração conceitual Repositório Digital, seguindo, a partir daí, para o entendimento da noção de Repositório Digital Confiável e, finalmente, seguiu-se em direção à definição Repositório Digital Arquivístico Confiável, a fim de evidenciar as características distintas de cada um.

3.1 REPOSITÓRIO DIGITAL E REPOSITÓRIO DIGITAL CONFIÁVEL

O conceito de Repositório Digital, segundo RLG (2001, p. 5, Tradução nossa), consiste em "uma organização que é responsável pela manutenção, em longo prazo, dos recursos, bem como para disponibilizá-los às comunidades acordadas entre o depositante e os repositórios[52]." Para Bergmeyer *et al.* (2009), um repositório digital é uma organização que assumiu a responsabilidade pela preservação e acessibilidade, no longo prazo, de objetos digitais, e também pela sua interpretabilidade, com a finalidade de serem utilizados por uma comunidade designada específica. O termo "Longo prazo", significa, segundo Bergmeyer *et al.* (2009), um intervalo temporal que perdura além das mudanças tecnológicas (para *hardware e software*) e também quaisquer alterações à comunidade designada.

Um Repositório Digital, de acordo CONARQ (2015a, p. 9), consiste:

> Nun ambiente de armazenamento e gerenciamento de materiais digitais. Esse ambiente constitui-se de uma solução informatizada em que os materiais são capturados, armazenados, preservados e acessados. Um repositório digital é, então, um complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de *hardware, software* e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos.

[52] Texto original: "*an organization that has responsibility for the long-term maintenance of digital resources, as well as for making them available to communities agreed on by the depositor and the repository".*

O conceito proposto por RLG (2001) quanto a um Repositório Digital Confiável está configurado da seguinte forma:

> Um repositório digital confiável é aquele cuja missão é fornecer acesso no longo prazo a recursos digitais gerenciados; que aceita a responsabilidade pela manutenção no longo prazo de recursos digitais em nome depositantes e em benefício dos usuários atuais e futuros; que projeta seu(s) sistema(s) de acordo com convenções e padrões comumente aceitos para garantir a continuidade gerenciamento, acesso e segurança dos materiais depositados nele; que estabelece metodologias para avaliação do sistema que atenda às expectativas de confiabilidade da comunidade; isso pode depender de executar suas responsabilidades de longo prazo com depositantes e usuários de maneira aberta e explícita; e cujas políticas, práticas e desempenho possam ser auditadas e medidas[53]. (RLG, 2001, p. 12, Tradução nossa).

Um Repositório Digital Confiável é, segundo RLG/OCLC Working Group on Digital Archive Attributes (2002, p. 5, Tradução nossa), "aquele cuja missão é fornecer acesso confiável e de longo prazo a recursos digitais gerenciados para a comunidade designada, agora e no futuro[54]." Ainda, segundo aponta RLG/OCLC Working Group on Digital Archive Attributes (2002, p. 5, Tradução nossa), os Repositórios Digitais Confiáveis devem atender às seguintes expectativas:

> - Aceitar a responsabilidade pela manutenção no longo prazo dos recursos digitais em nome de seus depositantes e em benefício dos usuários atuais e futuros;
>
> - Ter um sistema organizacional que suporte não apenas a viabilidade no longo prazo do repositório, mas também as informações digitais pelas quais é responsável;
>
> - Demonstrar responsabilidade fiscal e sustentabilidade;
>
> - Projetar seu(s) sistema(s) de acordo com as convenções comumente aceitas e padrões para garantir o gerenciamento, acesso e segurança contínuos dos materiais depositado dentro dele;
>
> - Estabelecer metodologias para avaliação do sistema que atendam às expectativas de confiabilidade da comunidade;
>
> - Cumprir suas responsabilidades de longo prazo com depositantes e usuários aberta e explicitamente;

---

[53] Texto original: *A reliable digital repository is one whose mission is to provide long-term access to managed digital resources; that accepts responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users; that designs its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it; that establishes methodologies for system evaluation that meet community expectations of trustworthiness; that can be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly; and whose policies, practices, and performance can be audited and measured.*

[54] Texto original: *A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future.*

> - Ter políticas, práticas e desempenho que possam ser auditados e medidos; e
>
> - Observar os seguintes fatores relativos às responsabilidades organizacionais e de curadoria dos repositórios: escopo dos materiais depositados, gerenciamento do ciclo de vida e preservação, atuação junto a uma ampla gama de parceiros, questões legais relacionadas com a propriedade dos materiais armazenados e implicações financeiras[55].

De acordo com RLG/NARA (2007, p. 3, Tradução nossa), tem-se que o repositório digital confiável

> [...] entenderá ameaças e riscos a seus sistemas. Como articulado por Rosenthal et al. (2005), essas ameaças em potencial incluem falha de mídia, falha de *hardware*, falha de *software*, erros de comunicação, falha nos serviços de rede, obsolescência de mídia e hardware, obsolescência de software, erro do operador, desastre natural, ataque externo, ataque interno, falha econômica e falha organizacional. Monitoramento constante, planejamento e manutenção constantes, bem como ações conscientes serão necessárias para a implementação de estratégias nos repositórios para cumprir sua missão de preservação digital[56].

Repositório digital confiável é, para CONARQ (2015a, p. 9), "um repositório digital capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário."

---

[55] Texto original: *Accept responsibility for the long-term maintenance of digital resources on behalf of its depositors and for the benefit of current and future users;*
Have an organizational system that supports not only long-term viability of the repository, but also the digital information for which it has responsibility;
Demonstrate fiscal responsibility and sustainability;
Design its system(s) in accordance with commonly accepted conventions and standards to ensure the ongoing management, access, and security of materials deposited within it;
Establish methodologies for system evaluation that meet community expectations of trustworthiness;
Be depended upon to carry out its long-term responsibilities to depositors and users openly and explicitly;
Have policies, practices, and performance that can be audited and measured; and
Observe the following factors related to the repository's organizational and curative responsibilities: scope of deposited materials, lifecycle management and preservation, performance with a wide range of partners, legal issues related to the ownership of stored materials and financial implications.

[56] Texto original: *A trusted digital repository will understand threats to and risks within its systems. As articulated by Rosenthal et al. (2005), these potential threats include media failure, hardware failure, software failure, communication errors, failure of network services, media and hardware obsolescence, software obsolescence, operator error, natural disaster, external attack, internal attack, economic failure, and organizational failure. Constant monitoring, planning, and maintenance, as well as conscious actions and strategy implementation will be required of repositories to carry out their mission of digital preservation.*

3.2 REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Entre todos os manuais, relatórios e modelos de referência pesquisados, o conceito “Repositório Arquivístico Digital Confiável” foi encontrado, no âmbito desta pesquisa, apenas no RDC-Arq. Dessa forma, segundo CONARQ (2015a, p. 10), um Repositório Arquivístico Digital Confiável deve “ser capaz, de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável”.

Abaixo, apresenta-se o Quadro 2, onde evidenciam-se os resultados da busca por conceitos referentes a “Repositório Digital”, “Repositório Digital Confiável” e “Repositório arquivístico Digital Confiável”, partindo de análise das publicações citadas no texto do RDC-arq.

QUADRO 2 - Presença dos conceitos “Repositório Digital” e “Repositório Digital Confiável” em publicações citadas no RDC-Arq.

Documento	Apresenta o conceito “Repositório Digital”?		Apresenta o conceito “Repositório Digital Confiável”?		Apresenta o conceito “Repositório Arquivístico Digital Confiável”?	
	sim	**não**	**sim**	**não**	**sim**	**não**
Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources (2001)	x		x			x
Trusted Digital Repositories: Attributes and Responsibilities - TDR (2002)		x	x			x
Trustworthy Repositories Audit & Certification: Criteria and Checklist - TRAC (2007)		x	x			x
Digital Repository Audit Method Based on Risk Assessment - DRAMBORA (2007)	x			x		x
Catalogue of Criteria for Trusted Digital Repositories - NESTOR (2009)	x			x		x
Audit And Certification Of Trustworthy Digital Repositories - ACTDR (2011)		x	x			x
Recommended Practice For An Open Archival Information System (OAIS) Reference Model (2012)		x		x		x
Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis - RDC-Arq (2015)	x		x		x	

FONTE: : Desenvolvido pelo autor.

3.3 ANTECEDENTES HISTÓRICOS: A CRIAÇÃO DO CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS

Nas décadas de 1960 e 1970, à medida que a Era Espacial evoluia, havia um interesse crescente em estimular a cooperação internacional como uma maneira de aprimorar a exploração espacial, relata Consultative Committee for Space Data System

CCSDS (2020), como muitas agências espaciais investiram grandes somas de dinheiro no desenvolvimento de infraestrutura de suporte a missões espaciais, surgiu o conceito de "suporte cruzado", pelo qual uma Agência Espacial poderia oferecer seus serviços de tratamento de dados a outra, aumentando, assim, as oportunidades de realização de missões internacionais. Durante esses primeiros dias, ressalta CCSDS (2020), na ausência de padrões de dados espaciais acordados internacionalmente, o "suporte cruzado" era geralmente tratado pela introdução de adaptadores de "caixa preta" para forjar compatibilidade nas interfaces entre as agências. Essas "caixas pretas" foram configuradas exclusivamente para cada caso individual.

À medida que a exploração espacial avançava na década de 1980, assevera CCSDS (2020), os avanços tecnológicos na computação de espaçonaves, recursos de memória e comunicação viabilizaram a padronização das maneiras pelas quais as espaçonaves e os sistemas de dados terrestres trocavam informações. Ao mesmo tempo, os custos de implementação e operação dessas missões espaciais estavam aumentando significativamente. Para aproveitar as oportunidades apresentadas pelos avanços tecnológicos e enfrentar os desafios fiscais, foram tomadas algumas medidas iniciais que levaram à formação do *Consultative Committee for Space Data Systems*[57].

> Em março de 1981, o Grupo de Trabalho NASA[58] - ESA[59] (NEWG) realizou sua primeira reunião para abordar o desenvolvimento cooperativo de padrões de dados espaciais, inicialmente nas áreas de naves espaciais 'telemetria de pacotes' e, em seguida, em 'telecomunicação de pacotes'. Em janeiro de 1982, em um *Workshop* Internacional sobre Sistemas de Dados Espaciais, realizado em Washington, DC, EUA, essa atividade bilateral foi ampliada e muitas das agências espaciais do mundo se reuniram para começar a discutir problemas comuns em relação a informações e sistemas de dados espaciais. Nessa reunião, foram tomadas as etapas finais para formalizar as atividades internacionais de padronização de dados espaciais, criando o CCSDS, que teve sua reunião inaugural no *Centre National d'Études Spatiales*[60] - CNES em Toulouse, França, em 04 e 08 de outubro de 1982[61].(CCSDS, 2020, Tradução nossa).

---

57 Comitê Consultivo para Sistemas de Dados Espaciais Tradução do autor.
58 Agência Espacial Norte Americana. Tradução do autor.
59 Agência Espacial Europeia. Tradução do autor.
60 Centro Nacional de Estudos Espaciais. Tradução do autor.
61 Texto original: *In March 1981, the NASA-ESA Working Group (NEWG) held its first meeting to address cooperative development of space data standards, initially in the areas of spacecraft "packet telemetry" and then in "packet telecommand". In January 1982, at an International Workshop on Space Data Systems held in Washington, DC, USA, this bilateral activity was broadened and many of the world's space agencies met to begin discussing common problems relative to space information and data systems. At that meeting, the final steps were taken to formalize international space data standardization activities by creating the CCSDS, which then had its inaugural meeting at CNES in Toulouse, France on 04-08 October 1982.*

Dessa forma, segundo CCSDS (2020), o Comitê foi encarregado de estudar os problemas do apoio cruzado e, por meio dos esforços coletivos de seus especialistas internacionais, desenvolver soluções padronizadas avançadas para esses desafios de troca de dados de missões espaciais. Essas soluções, chamadas “Recomendações do CCSDS”, foram os principais produtos do Comitê, durante a maior parte de seus primeiros vinte anos. Assim, o projeto de recomendações do CCSDS foi criado, revisado pelas agências participantes do CCSDS e, posteriormente, adotado por aquelas agências como recomendações finais que serviram para orientar o desenvolvimento interno de padrões por cada um dos membros.

Essas atividades iniciais do CCSDS aprimoraram significativamente o planejamento e a execução de missões espaciais cooperativas realizadas pelas agências participantes.

A Carta do CCSDS, aprovada em 1982, e atualizada nos anos de 1999 e 2004, apresenta os seguintes objetivos:

> - proporcionar um fórum através do qual as agências interessadas possam trocar informações técnicas relativas ao desenvolvimento ou aplicação de padrões para tecnologias de informação relacionadas ao espaço;
>
> - identificar os elementos comuns dos sistemas de dados espaciais que, se implementados de maneira padronizada, resultarão em melhorias significativas nas operaçções de futuras missões espaciais cooperativas ou no compartilhamento de produtos das missões;
>
> - desenvolver, por consenso, padrões apropriados que guiarão o desenvolvimento da infraestrutura da agência, para maximizar a interoperabilidade;
>
> - facilitar e promover o uso de software e hardware desenvolvidos sob o programa CCSDS por todas as agências participantes;
>
> - promover a aplicação dos padrões na comunidade de missões espaciais; e
>
> - manter conhecimento de outras atividades internacionais de padronização que podem ter impacto direto no projeto ou operação de sistemas de dados de missões espaciais[62]. (CONSULTATIVE COMMITTEE FOR SPACE DATA - CCSDS, 2004a, tradução nossa).

[62] Texto original: *The objectives of the CCSDS are:*
- to provide a forum whereby interested agencies may exchange technical information relative to the development or application of standards for space-related information technologies;
- to identify those common elements of space data systems which, if implemented in a standardized way, will result in significant enhancements in the operation of future cooperative space missions, or in the sharing of mission products;
- to develop through consensus appropriate standards that will guide the development of agency infrastructure so that interoperability is maximized;
- to facilitate and promote the use of soft ware and hardware developed under the CCSDS programme by all participating agencies;
- to promote the application of the standards within the space mission community; and

Em 1991, o CCSDS firmou um acordo de cooperação com a Organização Internacional de Normalização (ISO), quando foi acordado que as Recomendações do CCSDS seriam avançadas ao Subcomitê 13 no Comitê Técnico 20 (Veículos Aeronáuticos e Espaciais), no qual, por meio dos procedimentos normais de revisão e votação da ISO, elas progrediram para Normas Internacionais completas. (CCSDS, 2020).

3.4 A PRÁTICA RECOMENDADA PARA O MODELO DE REFERÊNCIA *OPEN ARCHIVAL INFORMATION SYSTEM (OAIS)*

Originalmente, o Modelo de Referência OAIS consiste num esforço amplo para desenvolver padrões formais para o armazenamento de longo prazo de dados digitais gerados a partir de missões espaciais. Desde então, “serviu de base para numerosas arquiteturas, padrões e protocolos, influenciou sistemas de design, requisitos de metadados, certificação e outras questões centrais para a preservação digital.” (LAVOIE, 2014, p. 1).

“Este é um modelo funcional geral, independente de qualquer programa ou equipamento informático específico, que constitui um quadro teórico, conceitual, terminológico e de referência para a criação de repositórios.[63].” (ZAZO; LORENZO-CÁCERES, 2017, p. 534, Tradução nossa).

No Brasil, segundo CONARQ (2015a, p. 8), “o Modelo de Referência *OAIS* foi traduzido pela Associação Brasileira de Normas Técnicas - ABNT, e publicado sob a forma da norma ABNT NBR 15472: 2007, com o título ‘Sistema Aberto de Arquivamento de Informação - SAAI’.”

A adoção do esquema SAAI poderá, ainda, produzir benefícios econômicos, uma vez que a padronização de entidades e processos comuns favorece a redução de custos, através do compartilhamento de componentes de sistemas. Além disso, a padronização promove o desenvolvimento do mercado fornecedor, transformando produtos e serviços altamente personalizados em versões padronizadas menos onerosas. (THOMAZ; SOARES, 2004, p. 16).De acordo, ainda, com Thomaz e Soares (2004, p. 16), o desenvolvimento de outros padrões, em apoio ao modelo de referência OAIS, serviria para promover a interoperabilidade entre bibliotecas, arquivos e outras instituições que mantêm informação digital por longos períodos..

- to maintain cognizance of other international standardization activities that may have direct impact on the design or operation of space mission data systems.

63 Texto original: Se trata de un modelo funcional de carácter general, independiente de cualquier programa o equipamiento informático específico, que constituye un marco teórico, conceptual, terminológico y de referencia para la creación de repositorios.

3.4.1 O Arquivo OAIS

Um OAIS é um Arquivo, descrito como uma "organização, que pode ser parte de uma organização maior, de pessoas e sistemas, e que aceitou a responsabilidade de preservar a informação e torná-la disponível para uma Comunidade Designada" (CCSDS, 2012).

> Reúne-se um conjunto de tais responsabilidades, tal como definido neste Modelo de Referência OAIS, e isso permite que um Arquivo OAIS seja distinguido de outros usos do termo "arquivo". O termo "Aberto", no Modelo de Referência OAIS, é usado para implicar que esta Recomendação, bem como futuras recomendações e normas, são desenvolvidos em fóruns abertos, e isso não implica que o acesso ao Arquivo é irrestrito[64]. (CCSDS, 2012, p. 1, Tradução nossa).

Para Lee (2005, p. 4), "mesmo antes de atingir qualquer status formalmente aprovado no CCSDS ou na Organização Internacional de Normalização (ISO), o OAIS recebeu considerável atenção dos envolvidos na pesquisa e desenvolvimento da preservação digital." A Conformidade-OAIS tem sido um requisito de projeto declarado fundamental para os principais esforços de preservação digital e desenvolvimento de repositórios nos Arquivos Nacionais dos EUA[65] (NARA), Biblioteca do Congresso dos EUA[66] (LC), Biblioteca Britânica, Biblioteca Nacional da França[67] (BnF), Biblioteca Nacional dos Países Baixos[68] (KB), Centro de Curadoria Digital[69] (DCC) no Reino Unido, Centro de Biblioteca de Computadores Online[70] (OCLC), Acadêmico JSTOR[71], bem como vários sistemas de bibliotecas universitárias e agências espaciais, aponta Lee (2005).

> O OAIS também serviu de base para várias iniciativas muito importantes na área de preservação digital de metadados, incluindo CEDARS[72] (exemplares de CURL[73] em arquivos digitais), NEDLIB[74] (Biblioteca Europeia de Depósitos em Rede) e dois esforços conjuntos do RLG / OCLC - o Grupo de Trabalho sobre Metadados de Preservação e, em seguida, Grupo de Trabalho Estratégias de Implementação de Metadados de

---

64 Texto original: *It meets a set of such responsibilities as defined in this document, and this allows an OAIS Archive to be distinguished from other uses of the term 'archive'. The term 'Open' in OAIS is used to imply that this Recommendation, as well as future related Recommendations and standards, are developed in open forums, and it does not imply that access to the Archive is unrestricted.*

65 *National Archives and Records Administration.*

66 *Library of Congress.*

67 *Bibliothèque nationale de France.*

68 *Koninklijke Bibliotheek.*

69 *Digital Curation Centre.*

70 *Online Computer Library Center, Inc.*

71 *Journal Storage Digital library of academic journals, books, and primary sources.*

72 *CURL Exemplars in Digital ARchiveS.*

73 *Client Uniform Resource Locator.*

74 *Network Event Detection Library.*

> Preservação (PREMIS[75]). RLG e a OCLC também desenvolveram em conjunto orientações sobre atributos de repositórios digitais confiáveis, que se baseiam no OAIS. Uma das primeiras atividades da *Digital Preservation Coalition* (DPC) no Reino Unido, após sua formação em 2001, foi desenvolver, juntamente com o *British National Space Centre* (BNSC), um seminário para discutir e "aumentar o perfil" do OAIS. O CCSDS está envidando esforços para desenvolver padrões de acompanhamento baseados no OAIS, começando com o *Producer-Archive Interface Method Abstract* (PAIMAS), que alcançou o status de Livro Azul em dezembro de 2003. RLG e NARA formaram uma Força-Tarefa de Certificação de Repositório Digital, cujos esforços estão explicitamente vinculados ao OAIS e pretendem contribuir para os esforços de padronização do Arquivo ISO; e uma iniciativa do *Center for Research Libraries* (CRL) está estendendo o trabalho de certificação RLG / NARA, com financiamento da Fundação Andrew W. Mellon. Um grande número de outros projetos de pesquisa e desenvolvimento é baseado ou reivindica conformidade com o OAIS. (LEE, 2005, p. 4, Tradução nossa)[76]

Portanto, esta pesquisa considerou fundamental diferenciar o conceito de Arquivo OAIS do conceito usualmente atribuído a um Arquivo, do ponto de vista da Ciência Arquivística.

3.4.2 O desenvolvimento do Modelo de Referência OAIS

Segundo Lavoie (2014), o CCSDS foi criado em 1982, e constitui-se num fórum para as agências espaciais de diversas nações interessadas no desenvolvimento cooperativo de padrões de manipulação de dados em apoio da investigação espacial. Em 1990, o CCSDS lançou um arranjo cooperativo com a International Organization for Standardization (ISO), em busca de soluções para os problemas de manipulação de dados compartilhados por seus membros. (LAVOIE, 2014).

> A pedido da ISO, o CCSDS iniciou os trabalhos destinados a desenvolver padrões formais para o armazenamento de longo prazo de dados digitais

---

[75] *Data Dictionary for Preservation Metadata.*

[76] Texto original: *The OAIS has also served as the basis for several very prominent digital preservation metadata initiatives, including CEDARS (CURL Exemplars in Digital Archives), NEDLIB (Networked European Deposit Library), and two joint Research Libraries Group (RLG) / OCLC efforts - the Working Group on Preservation Metadata and then the Preservation Metadata Implementation Strategies (PREMIS) Working Group. RLG and OCLC have also jointly developed guidance on attributes of trusted digital repositories, which builds off of the OAIS. One of the earliest activities of the Digital Preservation Coalition (DPC) in the UK after its formation in 2001 was to develop, along with the British National Space Centre (BNSC), a seminar to discuss and "raise the profile of" the OAIS. The CCSDS is undertaking efforts to developed follow-on standards based on the OAIS, starting with the Producer-Archive Interface Methodology Abstract Standard (PAIMAS), which reached Blue Book status in December 2003. RLG and NARA formed a Digital Repository Certification Task Force, whose efforts are explicitly tied to the OAIS and intended to contribute to the ISO Archiving standardization efforts; and an initiative by the Center for Research Libraries (CRL) is extending the RLG/NARA certification work, with funding from the Andrew W. Mellon Foundation. A large number of other research and development projects are either based on or claim conformance to the OAIS.*

> gerados a partir de missões espaciais. Na preparação para este esforço, o CCSDS não encontrou nenhum quadro amplamente aceito que poderia servir como uma base para atividades de construção de normas: nada, por exemplo, que estabelecesse conceitos e terminologia associados com a preservação digital compartilhados; caracterizasse as funções básicas que constituem um sistema de armazenamento digital; ou definisse os atributos importantes da informação de objetos digitais para os quais os esforços de preservação seriam dirigidos. (LAVOIE, 2014, p. 5).

Diante da ausência de uma estrutura única, Lavoie (2014, p. 5) lembra que “o CCSDS determinou que seu primeiro passo seria criar uma.” O workshop internacional convocado pelo CCSDS, em 1995, validou essa estratégia e foi proposta uma estratégia para desenvolver um modelo de referência para um “Sistema Aberto de Arquivamento de Informação” - SAAI. De acordo com essa proposta, o modelo de referência do CCSDS definiria os componentes funcionais básicos de um sistema dedicado à preservação de longo prazo da informação digital, detalhando as principais interfaces dos sistemas internos e externos e caracterizando os objetos de informação gerenciados pelo sistema. Essas descrições seriam expressas em termos de um conjunto bem definido de conceitos e terminologias transcendentes, já mapeados para vocabulários específicos do domínio. O modelo de referência também enumeraria um conjunto de requisitos mínimos que o sistema de arquivamento deveria atender. Quando concluído, o modelo de referência representaria uma estrutura compreensível e consistente para descrever e analisar problemas de preservação digital, forneceria uma base sólida para a futura atividade de construção de padrões e serviria como ponto de referência para fornecedores interessados em criar produtos e serviços de preservação.

Salienta Lavoie (2014, p. 5) que, “estritamente falando, o modelo de referência pode ser aplicado à preservação em longo prazo de itens de qualquer forma, incluindo artefatos físicos.”

O modelo de referência não faz suposições sobre a natureza da informação a ser preservada; consequentemente, a informação poderia ser, como o próprio modelo de referência mesmo, uma rocha lunar. No entanto, é no mundo digital que o modelo de referência OAIS ganhou sua maior visibilidade e aceitação.

Desde os primeiros estágios do desenvolvimento do modelo de referência, Lavoie (2014, p. 6) lembra que “o CCSDS reconheceu que sua relevância estendeu-se muito além da comunidade de dados espaciais.” O modelo de referência abordaria aspectos fundamentais sobre a preservação no longo prazo de materiais digitais que abrangem a implementação de vários domínios específicos. Consequentemente, foi tomada a decisão de tornar aberto o processo de elaboração do modelo para qualquer indivíduo ou organização interessada. Ao adotar essa abordagem ecumênica, o CCSDS alcançou além da

comunidade de dados espaciais para envolver um conjunto diversificado de organizações no governo, setor privado e academia. O desenvolvimento do modelo de referência foi uma oportunidade para consolidar o entendimento das necessidades e requisitos de preservação digital, reunindo as vertentes de atividades isoladas de preservação digital em uma caracterização compartilhada dos limites do problema.

> O Sistema Aberto de Arquivamento de Informação pode sugerir duas ideias: Sistema Aberto de Arquivamento de Informação e Sistema Aberto de Informação Arquivística. O primeiro é o mais usado e produzido pelos tradutores e, em qualquer caso, o adjetivo (aberto) refere-se ao sistema de informações de arquivo, não apenas ao arquivo. O próprio modelo deixa isso claro, afirmando que o termo "aberto" é usado para sugerir que ele foi desenvolvido em fóruns abertos e não significa que o acesso ao arquivo é ilimitado[77] (MUNDET; CARRERA, 2016, p. 229, Tradução nossa).

Os trabalhos desenvolvidos pelos membros do CCSDS destinaram-se a desenvolver padrões formais para o armazenamento no longo prazo de dados digitais gerados a partir de missões espaciais, envolvendo, de acordo com CCSDS (2012), o desenvolvimento de um modelo de referência para um Sistema Aberto de Arquivamento de Informação - SAAI. Para Lavoie (2014, p. 2, Tradução nossa), o Modelo de Referência OAIS representaria:

> [...] um quadro abrangente e consistente para descrever e analisar questões de preservação digital, fornecer uma base sólida para a atividade de construção de normas futuras, e servir como um ponto de referência para os fornecedores interessados em construir produtos e serviços de preservação digital. O modelo de referência OAIS foi aprovado em janeiro de 2002 como ISO 14721. Norma Internacional; uma versão revista e atualizada foi publicada em 2012, como a norma ISO 14721: 2012[78].

O Modelo de Referência OAIS foca, particularmente, em informação digital, tanto nas formas primárias de informação quanto a informação de apoio para ambos os materiais em formatos digitais e fisicamente arquivados. Dessa forma, o modelo acomoda informação que é inerentemente não-digital (por exemplo, uma amostra física), mas a modelação e

---

[77] Texto original: *The Open Archival Information System can suggest two ideas: open archival information system and open system of archival information. The first is the most frequently used and produced by the translators, and in any case the adjective (open) refers to the archive information* system, not just to the archive. The model itself makes this clear, by stating that the term “open” is *used to imply that it has been developed in open forums and does not mean that access to the file is unlimited.*

[78] Texto original*: The reference model would represent a comprehensive and consistent framework for describing and analysing digital preservation issues, provide a sound footing for future standards-building activity, and serve as a point of reference for vendors interested in building digital preservation products and services. The OAIS reference model was approved in January 2002 as ISO International Standard 14721; a revised and updated version was published in 2012 as ISO Standard 14721:2012.*

manutenção de tais informações não é abordada em detalhe. (CCSDS, 2012). Esse modelo de referência fornece várias inovações, tais como:

> - fornece uma estrutura para a compreensão e maior conscientização sobre conceitos de arquivamento necessários para preservação e acesso a informações digitais de longo prazo;
>
> - fornece os conceitos necessários para que as organizações não-arquivísticas sejam participantes eficazes no processo de preservação;
>
> - fornece uma estrutura, incluindo terminologia e conceitos, para descrever e comparar arquiteturas e operações de arquivos existentes e futuros;
>
> - fornece uma estrutura para descrever e comparar diferentes estratégias e técnicas de preservação de longo prazo;
>
> - fornece uma base para comparar os modelos de dados de informação digital preservados por Arquivos e para discutir como os modelos de dados e as informações subjacentes podem mudar com o tempo;
>
> - fornece uma estrutura que pode ser expandida por outros esforços para cobrir a preservação de informações de longo prazo que não estão em formato digital (por exemplo, mídia física e amostras físicas);
>
> - amplia o consenso sobre os elementos e processos da preservação da informação digital no longo prazo e acesso e promove um mercado maior ao qual os fornecedores podem apoiar;
>
> - orienta a identificação e produção de normas relacionadas ao OAIS[79]. (CCSDS, 2012, p. 1, Tradução nossa).

O Modelo de Referência OAIS pode, ser aplicável a qualquer arquivo. É especificamente aplicável a organizações com a responsabilidade de tornar a informação disponível por um longo prazo, como organizações responsáveis pelo processamento e distribuição em resposta à necessidades programáticas. O Modelo OAIS também é de interesse para as organizações e indivíduos que criam informações que podem precisar de preservação a longo prazo e àqueles que podem adquirir informações a partir desses arquivos. (CCSDS, 2012).

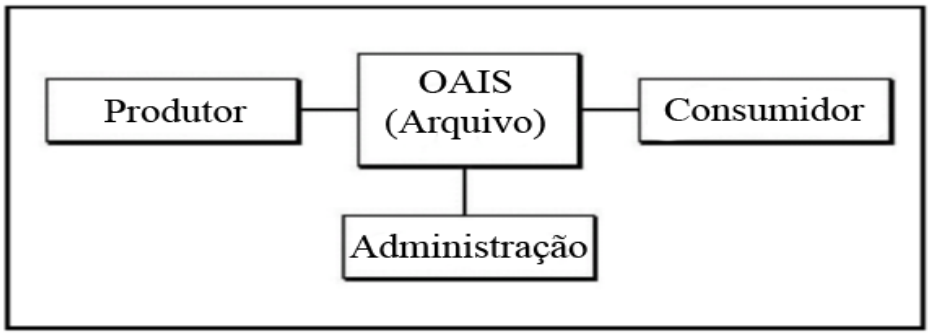
---

[79] Texto original*: - provides a framework for the understanding and increased awareness of archival concepts needed for Long Term digital information preservation and access;*
- provides the concepts needed by non-archival organizations to be effective participants in the preservation process;
- provides a framework, including terminology and concepts, for describing and comparing architectures and operations of existing and future Archives;
- provides a framework for describing and comparing different Long Term Preservation strategies and techniques;
- provides a basis for comparing the data models of digital information preserved by Archives and for discussing how data models and the underlying information may change over time;
- provides a framework that may be expanded by other efforts to cover Long Term Preservation of information that is NOT in digital form (e.g., physical media and physical samples);
- expands consensus on the elements and processes for Long Term digital information preservation and access, and promotes a larger market which vendors can support;
- guides the identification and production of OAIS related standards.

3.4.3 O Ambiente OAIS e seus conceitos

O Ambiente circundante a um OAIS é representado na Figura 6.

FIGURA 6 - Ambiente OAIS



FONTE: CCSDS (2012, p. 2). Tradução nossa.

- O Produtor , de acordo com Lavoie (2014, p. 9), corresponde aos "indivíduos, organizações ou sistemas que transferem informações para o OAIS no longo prazo preservação." A negociação entre Produtores e o Arquivo OAIS especifica o conteúdo e os metadados associados que o Produtor deverá fornecer no evento de transmissão do Pacote de Submissão de Informação, ao OAIS, por meio de um processo de ingestão que aceita os dados submetidos e prepara-o para a inclusão no Armazenamento de Arquivos. A interação entre o OAIS e os Produtores é formalizada e orientada por um Acordo de Submissão, que estabelece detalhes específicos da interação, tais como o tipo de informação apresentada, os metadados que o Produtor deverá fornecer, a logística da transferência da custódia do Produtor para o Arquivo OAIS, e quaisquer restrições de acesso ligadas ao material a ser preservado pelo OAIS. As normas *Producer-Archive Interface Methodology Abstract Standard*[80] (PAIMAS) e *Producer-Archive Interface Specification*[81] (PAIS) descrevem a interação entre os Produtores e o Arquivo OAIS (LAVOIE, 2014, p. 8).

> O PAIMAS é uma norma recomendada pelo CCSDS que identifica e fornece um quadro para as interações que ocorrem entre um Produtor de informação e um Arquivo OAIS. Cobre as fases iniciais do processo de entrada definido pelo OAIS, com o objetivo de fornecer um método padronizado para definir formalmente os objetos de informação digital a serem transferidos de um Produtor para um Arquivo e para o empacotamento eficaz desses objetos sob a forma de SIP, que apoia a transferência e validação dos dados. (MUNDET; CARRERA, 2016, p. 241).

"O PAIS é uma especificação desenvolvida pelo CCSDS com o objetivo de fornecer um método padronizado de modelagem de dados a serem transferidos de um

[80] Metodologia de Interface Produtor-Arquivo Padrão Abstrato. Tradução do autor.
[81] Especificação da Interface Produtor-Arquivo. Tradução do autor.

Produtor de informação para um Arquivo OAIS e, posteriormente, validação por este último." (MUNDET; CARRERA, 2016, p. 241).

"Administração é o papel desempenhado por aqueles que definem a política global do OAIS como um componente em um domínio mais amplo de políticas, por exemplo, como parte de uma organização maior." (CCSDS, 2012, p. 2). As responsabilidades da administração incluem, segundo Lavoie (2014, p. 9) "a formulação, revisão e, em algumas circunstâncias, a aplicação da estrutura política de alto nível que rege as atividades da OAIS."

> Exemplos de funções desempenhadas pela Administração incluem planejamento estratégico, definição do escopo da coleção arquivada no OAIS, e articulação da garantia de preservação associada aos itens confiados ao arquivo. A Administração também pode representar a fonte de financiamento do OAIS, e, muitas vezes, serve como supervisão, revisando periodicamente o OAIS políticas, desempenho e riscos[82] (LAVOIE, 2014, p. 9, Tradução nossa).

"Consumidor é o papel desempenhado por pessoas ou sistemas do cliente, que interagem com serviços OAIS para encontrar e adquirir informações de interesse preservadas." (CCSDS, 2012, p. 2-3).

> O Modelo de Referência OAIS define uma classe especial de consumidores conhecida como 'Comunidade Designada'. Ela consiste no subconjunto de consumidores que devem compreender, de forma independente, as informações arquivadas na forma em que se encontram preservadas e disponibilizados pelo OAIS, de forma que estes são seus usuários primários. (LAVOIE, 2014, p. 10).

"Os consumidores interagem com o Arquivo OAIS de diversas maneiras, incluindo consultas para assistência, buscas e solicitações de acesso aos objetos de informação arquivados." (LAVOIE, 2014, p. 10).

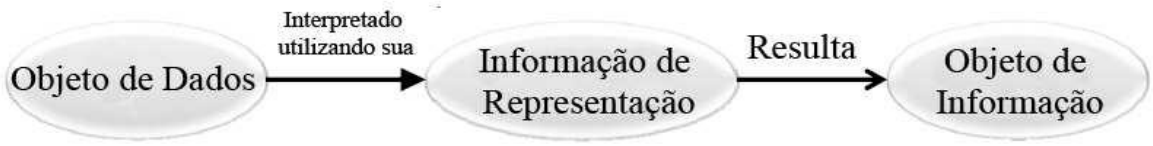
É importante frisar que, nesta pesquisa, verificou-se que a Comunidade Designada pode constituir-se de uma vasta pluralidade de consumidores, sendo que, no universo arquivístico, estes consumidores podem ser os próprios produtores dos documentos arquivísticos digitais e até mesmo cidadãos utilizando-se de seu direito de acesso a informações públicas não-classificadas. A Informação no Modelo de Referência OAIS

---

[82] Texto original: *Examples of functions carried out by Management include strategic planning, defining the scope of the OAIS's archived collection, and articulating the preservation guarantee associated with items entrusted to the archive. Management may also represent the funding source for the OAIS, and often serves in an oversight capacity, periodically reviewing the OAIS's policies, performance, and risks.*

Informação é definida como qualquer tipo de conhecimento que pode ser trocado, e essa informação é sempre expressa (ou seja, representada) por algum tipo de dados em uma troca. (CCSDS, 2012).

FIGURA 7 - Obtendo informações de dados



FONTE: CCSDS (2012, p. 2-4). Tradução nossa.

O Objeto de Dados (Também denominado Objeto de Dados de Conteúdo por alguns autores) pode assumir a forma de qualquer classe de material: texto, imagens, vídeo, bases de dados, programas de computador - até mesmo material físico, como amostras de solo. (LAVOIE, 2014).

> O Objeto de Dados de Conteúdo pode ser composto de um único objeto, autossuficiente - por exemplo, um documento em formato PDF[83]; ele também pode abranger vários objetos, como um site que é constituído de texto (arquivos HTML[84]) e imagens estáticas (GIF[85] ou JPEG[86]). O ponto-chave é que o OAIS é responsável pela preservação do Objeto de Dados de Conteúdo, no longo prazo, bem como torná-lo disponível em uma forma que é, independentemente, compreensível pela Comunidade Designada[87]. (LAVOIE, 2014, p. 16, Tradução nossa).

O Objeto de Dados pode ser expresso, de acordo com CCSDS (2012, p. 4/21) "como um objeto físico (uma rocha lunar, por exemplo) em conjunto com alguma 'Informação de Representação', ou pode ser expressa como um objeto digital (um sequência de *bits*, por exemplo) juntamente com a Informação de Representação, dando significado a esses *bits*".

> Informações de Representação são informações necessárias para processar e compreender as sequências que constituem o objeto de dados.

---

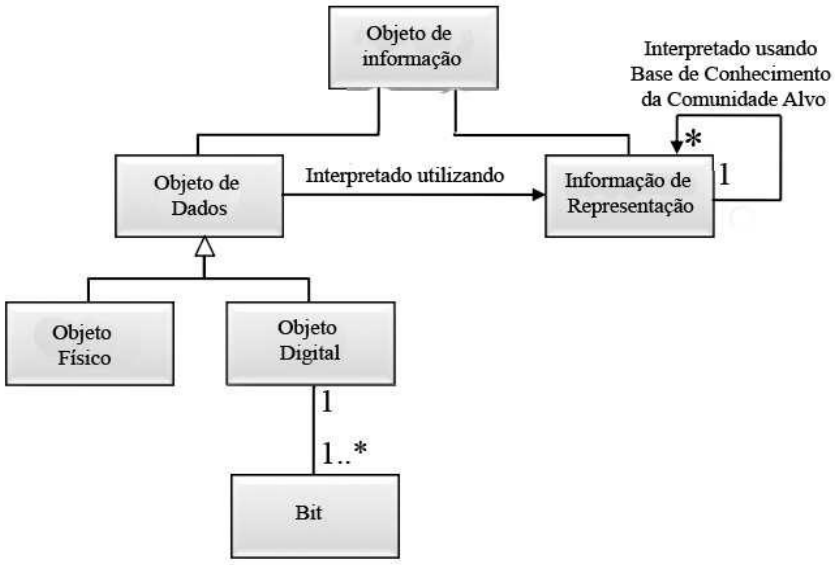
83 *Portable Document Format.*
84 *HyperText Markup Language.*
85 *Graphics Interchange Format.*
86 *Joint Photographic Experts Group.*
87 Texto original: *The Content Data Object can take the form of any class of material: text, images, video, databases, computer programs - even physical material such as soil samples or fossils. The Content Data Object may be comprised of a single, self-contained object - for example, a document in PDF format; it may also encompass multiple objects, such as a website consisting of text (HTML files) and static images (GIF or JPEG files). The key point is that the OAIS is responsible for preserving the Content Data Object over the long term, as well as for making it available in a form that is independently understandable by the Designated Community.*

> Informações de Representação podem incluir uma descrição do ambiente de *hardware* e *software* necessários para exibir o objeto de dados e / ou acessar seu conteúdo. (LAVOIE, 2014, p. 15).

A interpretação do objeto de dados com informação significativa pela Comunidade Designada é obtida, pela combinação da Base de Conhecimento da Comunidade Designada e a Informação de Representação associada ao Objeto de Dados. Cada indivíduo (ou classe de indivíduos, no caso de uma Comunidade Designada), tem uma Base de Conhecimento, que é usada para entender e interpretar a informação. "O Objeto de Dados, a Base de Conhecimento da Comunidade Designada e a Informação de Representação, quando combinados, formam um Objeto de Informação, que representa uma 'informação significativa' para a Comunidade Designada." (THOMAZ; SOARES, 2004, p. 12).

Nas Figuras 7 e 8, ilutra-se o processo de formação do Objeto de Informação.

FIGURA 8 - Objeto de Informação



FONTE CCSDS (2012, p. 4/25). Adaptado. Tradução nossa.

3.4.4 Tipos de Informação de Representação

A Informação de Representação pode assumir duas formas, explica Saramago (2004, p. 4): "Informação Estrutural e Informação Semântica."

> A Informação Estrutural interpreta os *bits* organizando os por tipos de dados, grupos de tipos de dados e outros significados de alto nível, devendo incluir a especificação do formato dos dados e uma descrição do ambiente

> do *hardware* e do *software* em que os dados foram criados, e essenciais para o acesso posterior. (SARAMAGO, 2004, p. 4).

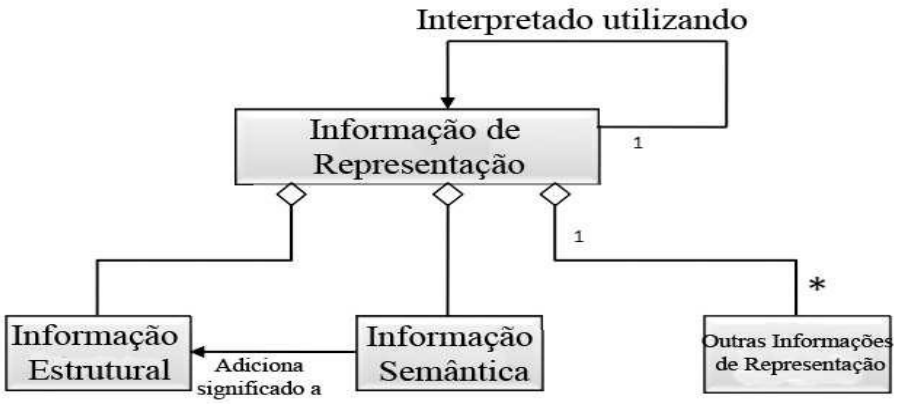
O objetivo da Informação de Representação é, de acordo com CCSDS (2012, p. 4/22):

> Converter as sequências de bits em informações mais significativas. Isto é feito descrevendo o 'Formato' ou o conceito de 'Estrutura de Dados', que devem ser aplicados às sequências de bits e que, por sua vez, resultam em valores mais significativos tais como caracteres, números, pixels, tabelas, etc.
>
> Estes tipos comuns de dados de computador, agregações destes tipos de dados e regras de mapeamento que localizam a partir dos tipos de dados subjacentes aos conceitos de nível superior, necessários para compreender o Objeto Digital, são chamados de Informações Estruturais da Informação de Representação. Estas estruturas são comumente identificadas pelo nome ou pela posição relativa dentro das sequências de *bits* associadas. A informação da estrutura é frequentemente referida como o 'Formato' do objeto digital (CCSDS, 2012, p. 4/22).

"A Informação Semântica acrescenta significado à estrutura dos dados, identificada através da informação estrutural." (SARAMAGO, 2004, p. 4). As Informações de Representação fornecidas pelas Informações de Estrutura raramente são suficientes. Mesmo no caso em que o Objeto Digital é interpretado como uma seqüência de caracteres de texto, e descrito como tal qual nas Informações de Estrutura, as informações adicionais sobre qual linguagem estava sendo expressa deveriam ser fornecidas. "Este tipo adicional de informação exigido é chamado de Informação Semântica." (CCSDS, 2012, p. 4/22). Saramago (2004, p. 6) explica que:

> No ambiente do modelo OAIS a representação da informação encontra-se ela própria em formato digital e por esse motivo deve acrescentar-se informação adicional para interpretar o fluxo de *bits* da representação da informação, é por este motivo, necessária a existência de uma terceira camada de representação da informação, etc. O modelo de referência OAIS recomenda que o resultado da rede de representação termine com a elaboração de um documento físico que dê por finda a construção da rede e dê início ao processo de interpretação.

FIGURA 9 - Objeto de Informação de Representação



FONTE CCSDS (2012, p. 4/23, Tradução nossa).

Na Figura 10, também mostra-se que as Informações de Representação podem conter outras Informações de Representação. Isso indica que a taxonomia das Informações de Representação aqui apresentada está longe de estar completa, aponta CCSDS (2012, p. 4/23, Tradução nossa):

> [...]*software*, algoritmos, criptografia, instruções escritas e muitas outras coisas podem ser necessárias para entender o Objeto de Dados de Conteúdo, todas elas, portanto, seriam, por definição, Informação de Representação, mas não seriam obviamente Informações Estruturais ou Informações Semânticas. Informações que definem como as Informações Estruturais e de Semântica se relacionam entre si, ou o software necessário para processar um arquivo de banco de dados seriam consideradas como outras Informações de Representação[88].

Conforme observado na Figrua 09, cada item da Informação de Representação pode ter múltiplos componentes, incluindo múltiplas Informações de Representação, cada uma com suas próprias Informações de Representação. Dessa forma, conclui CCSDS (2012, p. 4/23), “para preservar o significado de um Objeto de Informação, suas Informações de Representação também devem ser preservadas.”

[88] Texto original: *For example software, algorithms, encryption, written instructions and many other things may be needed to understand the Content Data Object, all of which therefore would be, by definition, Representation Information, yet would not obviously be either Structure or Semantics. Information defining how the Structure and the Semantic Information relate to each other, or software needed to process a database file would be regarded as Other Representation Information.*

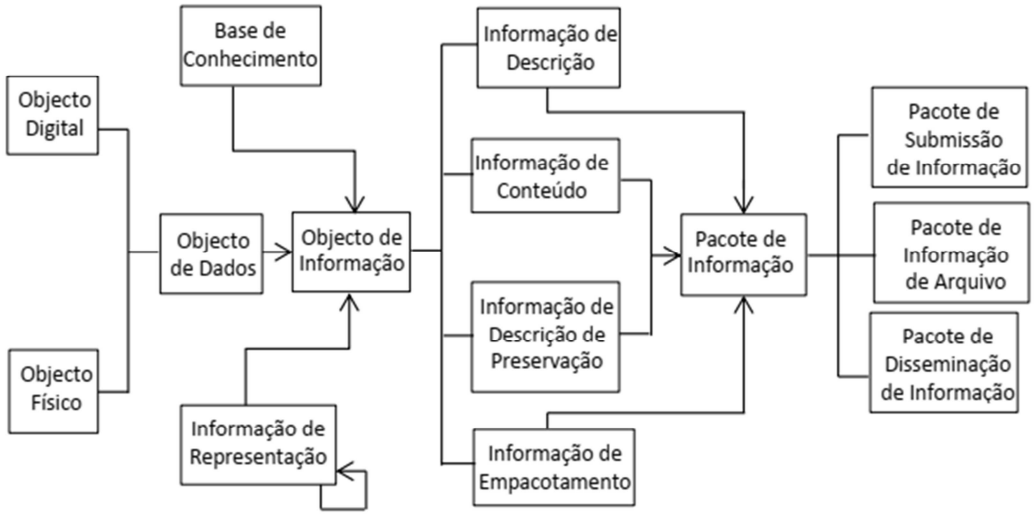
3.4.5 Taxonomia das Classes de Objetos de Informação utilizados pelo OAIS

"Há muitos tipos de informações envolvidos na preservação, por longos períodos, em um OAIS", revela CCSDS (2012, p. 4/26). Cada um desses tipos pode ser visto como um Objeto de Informação completo, na medida em que contém um Objeto de Dados e Informações de Representação adequadas para compreender os dados.

Um Objeto de Informação pode ser, de acordo com Thomaz e Soares (2004, p. 13) de quatro tipos: "Informação de Conteúdo, Informação de Descrição de Preservação, Informação de Pacote e Informação Descritiva." Na Figura 11, ilustra-se o Modelo de Informação no OAIS.

> A Informação de Conteúdo é a informação principal, alvo da preservação associada à sua Informação de Representação. A Informação de Descrição de Preservação (PDI) contém a informação necessária para preservar adequadamente a Informação de Conteúdo à qual está associada, podendo ser decomposta em quatro subcategorias a saber: Referência (descritores), Contexto (relacionamentos com o ambiente), Proveniência (proveniência e histórico) e Rigidez (informação para a comprovação de integridade e autenticidade). A Informação de Pacote reúne a Informação de Conteúdo e a Informação de Descrição de Preservação em um pacote identificável, enquanto a Informação Descritiva facilita o acesso à Informação de Pacote através de ferramentas de pesquisa e recuperação. (THOMAZ; SOARES, 2004, p. 13).

FIGURA 10 - Modelo de Informação no OAIS



FONTE: Corujo (2014).

Segundo CCSDS (2012, p. 2/5), "cada apresentação de informações a um OAIS por um Produtor, e cada divulgação de informações a um Consumidor, acontece por meio

de uma ou mais transmissões discretas. Dessa forma, é conveniente definir o conceito de Pacote de Informação."

Um Pacote de Informação, conforme apresentado na Figura 11, é um *contêiner* conceitual de dois tipos de informações: Informações de Conteúdo e Informações de Descrição para Preservação (PDI). As Informações de Conteúdo e as PDIs são vistas como encapsuladas e identificáveis pelo Pacote de Informação. O pacote resultante é visto como sendo detectável em virtude da Informação de Descrição. (CCSDS, 2012).

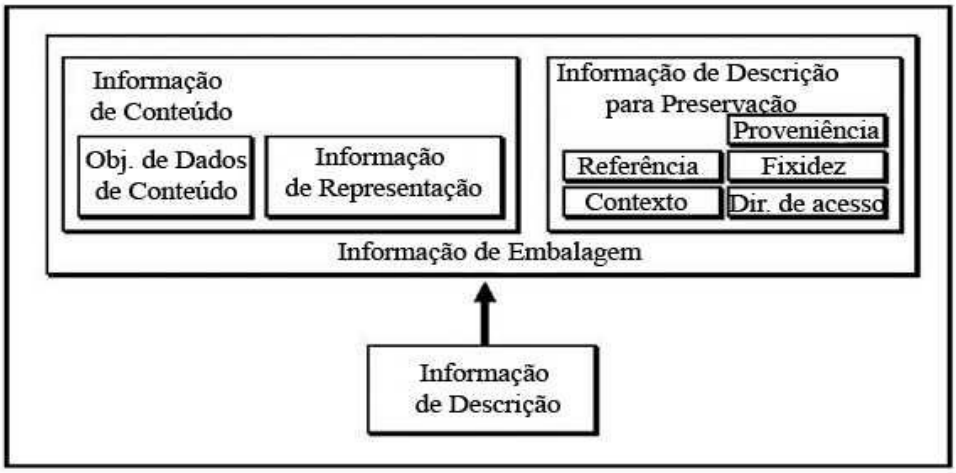
De acordo com Corujo (2014, p. 76), "vários tipos de pacotes de informação são utilizados no processo de arquivamento." Pacotes de informação podem ser usados para estruturar e armazenar a informação custodiada no OAIS, para transportar a informação do produtor ao Arquivo OAIS, ou para o transporte de informação solicitada entre o OAIS e os consumidores.

FIGURA 11- Conceito de Pacote de Informação e Relacionamentos

FONTE: CCSDS (2012, p. 2/6, Tradução nossa). Adaptado.

Lavoie (2014) apresenta o Pacote de Informação com maior detalhamento dos componentes internos, conforme observamos na Figura 12.

FIGURA 12 - Pacote de Informação



FONTE: Lavoie (2014, p. 16, Tradução nossa). Adaptado.

"A Informação de Conteúdo é aquela informação", segundo CCSDS (2012, p. 2/6), que é o alvo original da preservação. Ela consiste no Objeto de Dados de conteúdo (objeto físico ou objeto digital, ou seja, *bits*) e suas Informações de Representação associadas necessárias para criar o Objeto de Dados de Conteúdo compreensível para a Comunidade Designada.

As Informações de Descrição para Preservação aplicam-se às Informações de Conteúdo e são necessárias para a preservação destas últimas, para garantir que sejam claramente identificadas e para o entendimento do ambiente em que as Informações de Conteúdo foram criadas. As Informações de Descrição de Preservação são divididas em cinco tipos de informações de preservação denominadas Proveniência, Contexto, Referência, Fixidade e Direitos de Acesso.

> - A Proveniência descreve a fonte das Informações de Conteúdo, que teve a custódia de desde a sua origem e seu histórico (incluindo o histórico de processamento).
>
> - O Contexto descreve como as Informações de Conteúdo se relacionam com outras informações fora do Pacote de Informações.
>
> - A Referência fornece um ou mais identificadores, ou sistemas de identificadores, pelos quais as Informações de Conteúdo podem ser identificadas exclusivamente.
>
> - A Fixidade fornece um invólucro ou escudo protetor que protege as Informações do Conteúdo de alteração não documentada.
>
> - Os Direitos de Acesso fornecem os termos de acesso, incluindo preservação, distribuição e uso de informações de conteúdo. (CCSDS, 2012, p. 2/6, Tradução nossa).

A Informação de Embalagem (Também chamada de Informação de Empacotamento) é aquela informação que, para CCSDS (2012, p. 2/6), “real ou logicamente, vincula, identifica e relaciona as Informações de Conteúdo e a PDI.”

> Já a Informação de Descrição é aquela informação usada para descobrir qual pacote possui as Informações de Conteúdo de interesse. Dependendo da configuração, isso pode não ser mais que um título descritivo do Pacote de Informações que aparece em alguma mensagem ou pode ser um conjunto de atributos que podem ser pesquisados em um serviço de catálogo (CCSDS 2012, p. 2/6).

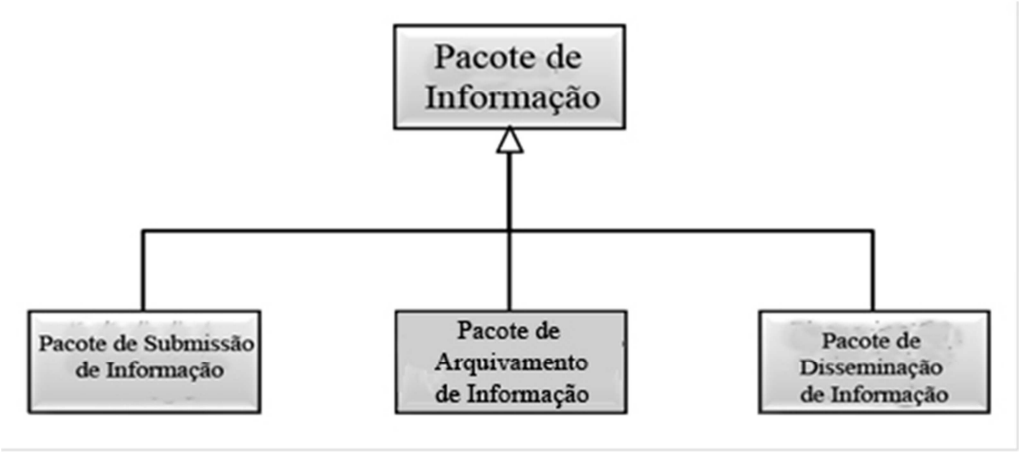
3.4.6 Tipos de Pacotes de Informação

De acordo com Lavoie (2014, p .2):

> O Modelo de Referência OAIS é construído em torno do conceito de um pacote de informação, que consiste no objeto, o foco de preservação, juntamente com os metadados necessários para suportar sua preservação por longos períodos, acesso e compreensibilidade, vinculados em um único pacote lógico.

Na Figura 13, mostram-se as três importantes variantes do conceito do Pacote de Informação adotadas no Modelo de Referência OAIS: o Pacote de Submissão de Informação (SIP), o Pacote de Arquivamento de Informação (AIP), e o Pacote de Disseminação de Informação (DIP).

FIGURA 13 - Taxonomia de um Pacote de Informação



FONTE: CCSDS (2012, p. 4/35, Tradução nossa).

O Pacote de Submissão de Informação é aquele, segundo CCSDS (2012, p. 2/7) “pacote que é enviado a um OAIS por um Produtor.” Sua forma e conteúdo detalhado são tipicamente negociados entre o Produtor e o OAIS tendo como referência a norma *Producer-*

Archive Interface Methodology Abstract Standard - PAIMAS. A maioria dos SIPs terá algumas Informações de Conteúdo e alguma Informação de Descrição para Preservação (PDI).

O pacote de informações é entregue pelo Produtor ao OAIS, afirma CCSDS (2012, p. 1/15), “para uso na construção ou atualização de um ou mais AIPs e/ou o Informações descritivas associadas.”

“O Pacote de Arquivamento de Informações (AIP) consiste nas Informações de Conteúdo e na Informação de Descrição para Preservação (PDI), que são preservados dentro de um OAIS”, pontua CCSDS (2012, p. 1/9).

Corujo (2014) disserta que o AIP possui funções de preservação e é fruto da transformação de um ou mais SIPs. Além disso, é composto por um conjunto completo de PDIs da Informação de Conteúdo a que se refere, podendo também conter uma coleção de outros AIPs. A sua Informação de Empacotamento deve estar em conformidade com as normas internas do Arquivo OAIS e pode variar, uma vez que é gerido pelo OAIS. A Informação de Descrição para Preservação associada a um AIP pode ser extensa e será gerida pelo OAIS para que os consumidores possam encontrar e solicitar a Informação de Conteúdo do seu interesse.

O Pacote de Disseminação Informação (DIP) constitui-se, de acordo com CCSDS (2012, p. 1/11), “num Pacote Informativo, derivado de um ou mais AIPs, e enviadas pelo Arquivo OAIS ao Consumidor em resposta a um pedido.”

A Informação fornecida pode ou não incluir, salienta Corujo (2014, p. 78), “a totalidade da Informação de Representação ou do PDI, mas a forma de apresentação tem que observar os requisitos do suporte e do Consumidor.” A Informação de Empacotamento deve ser disponibilizada numa forma em que a Comunidade Designada possa distinguir claramente a informação que solicitou.

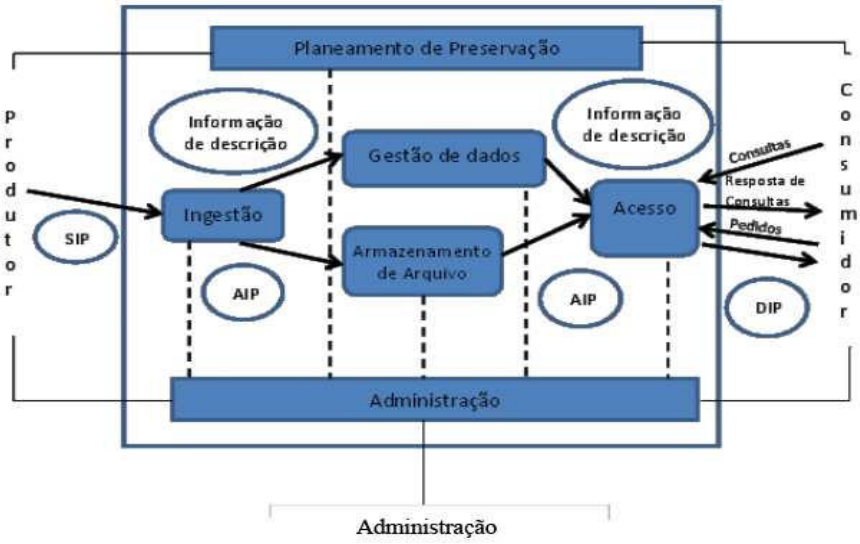
3.4.7 O Modelo Funcional OAIS

O Modelo OAIS descreve, de acordo com Flores e Hedlund (2014), as interfaces internas e externas do sistema e os objetos de informação que são manipulados no seu interior. Há uma rigorosa interação os elementos propostos, designados “Entidades”, que estabelece o fluxo documental, desde a inserção do documento até à sua disponibilização ao usuário.

Logo abaixo, na Figura 14, apresenta-se o Modelo Funcional (OAIS) e suas entidades funcionais, conforme apresentado por Thomaz e Soares (2004). Em um primeiro nível de detalhamento, são identificadas seis entidades funcionais: Recepção,

Armazenamento, Gerenciamento de Dados, Administração do Sistema, Planejamento de Preservação e Acesso.

FIGURA 14 - O Modelo Funcional OAIS



FONTE: Corujo (2014).

A entidade Recepção (também denominada *Ingest*, Ingestão ou Admissão) é responsável, segundo Thomaz e Soares (2004, p. 14), "pela aceitação dos Pacotes de Submissão de Informação (SIP) dos Produtores (ou de componentes internos sob controle da Administração do Sistema) e preparação dos conteúdos para armazenamento e gerenciamento dentro do arquivo." Lavoie (2014, p. 16) afirma que "a função *Ingest* serve como interface externa da OAIS com os Produtores, gerenciando todo o processo de aceitação da custódia das informações apresentadas e sua preparação para a retenção de arquivos." Mais especificamente, conforme explicam Thomaz e Soares (2004, p. 14):

> A entidade Recepção recebe SIPs, verifica a qualidade dos SIPs, gera Pacotes de Arquivamento de Informação (AIPs), de acordo com a formatação de dados e padrões de documentação do arquivo, e gera Informação Descritiva dos AIPs (metadados para pesquisa e recuperação, ícones para navegação, etc). Finalmente, transfere os recém-criados AIPs e Informações Descritivas associadas para a entidade Armazenamento e para a entidade Gerenciamento de Dados, respectivamente.

A entidade Armazenamento lida, segundo Mundet e Carrera (2016, p. 241):

> Com o armazenamento, manutenção e recuperação da AIP, o que implica no recebimento do pedido de armazenamento e uma AIP, transportando-o para armazenamento permanente, gerenciando a hierarquia de armazenamento, substituindo as mídias, verificando erros, duplicando o conteúdo e armazenando em uma instalação separada para recuperação em caso de catástrofe, e fornecendo dados à entidade funcional de acesso para cumprir pedidos. A entidade Gerenciamento de Dados mantém e

> acessa tanto a Informação Descritiva, de maneira que identifica e documenta tanto os acervos do arquivo, quanto os dados administrativos usados para gerenciá-lo. Especificamente, a entidade Gerenciamento de Dados administra a base de dados do arquivo (mantém os esquemas e definições de visões e integridade referencial), promove suas atualizações (carrega nova informação descritiva ou dados administrativos do arquivo) e consulta os dados da entidade para gerar relatórios. (THOMAZ; SOARES, 2004, p. 14).

A entidade Administração do Sistema gerencia a rotina operacional do arquivo como um todo, de forma que suas funções, para Thomaz e Soares (2004, p. 14), "incluem solicitar e negociar acordos de submissão com Produtores, auditar as submissões para garantir que estão atendendo aos padrões do arquivo e gerenciar a configuração do hardware e software do sistema." A entidade Administração do Sistema desempenha, também, funções mais técnicas para análise e melhoria do desempenho geral das operações do arquivo e migração/atualização de seus conteúdos. É responsável, ainda, por cumprir e manter os padrões e políticas do arquivo, fornecer suporte ao cliente e atender solicitações pendentes.

"A entidade Planejamento de Preservação monitora o ambiente SAAI e fornece recomendações para garantir que a informação armazenada permaneça acessível por longo prazo à Comunidade Designada, mesmo que o ambiente computacional original torne-se obsoleto." (THOMAZ; SOARES, 2004, p. 14).

A entidade Acesso apoia os Consumidores na determinação da existência, descrição, localização e disponibilidade da informação armazenada no SAAI, e permite que os Consumidores solicitem e recebam produtos de informação. Suas funções incluem comunicar com os Consumidores para receber solicitações, aplicar controles para limitar o acesso (principalmente à informação protegida), coordenar a execução de solicitações para que se completem com sucesso, gerar respostas (Pacotes de Disseminação de Informação, resultados, relatórios) e entregar as respostas aos Consumidores. (THOMAZ; SOARES, 2004, p. 14).

> Os serviços típicos prestados pela entidade Acesso em apoio ao Consumidor incluem o processamento de consultas ao acervo do arquivo OAIS - especificamente, encaminhando o pedido à Gerência de Dados e apresentando a resposta (por exemplo, um conjunto de resultados) para o Consumidor; e coordenar a recuperação e entrega do conteúdo solicitado - encaminhando o pedido ao Arquivamento, recebendo os itens solicitados e executando as transformações que forem necessárias (como a alteração do formato do item arquivado para um formato mais adequado para divulgação, ou removendo os metadados desnecessários) que devem ocorrer antes da entrega ao Consumidor. (LAVOIE, 2014, p. 13).

As seis entidades funcionais OAIS gerenciam o fluxo de informação entre os Produtores e o Arquivo e entre o Arquivo e os Consumidores. Vistas juntas, afirmam

Thomaz e Soares (2004, p. 14), “identificam os processos-chave típicos da maioria dos arquivos dedicados à preservação de informação digital.”

3.5 TRANSMISSÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS COM VALOR LEGAL NO CONTEXTO BRASILEIRO

Instituído em 18 de março de 2020, o Decreto nº 10.278 estabelece a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais. Diante do escopo desta pesquisa, voltada à análise de modelos de critérios de repositórios digitais e de possíveis compatibilidades conceituais junto às diretrizes que orientam os repositórios arquivísticos digitais brasileiros quanto à preservação, por longos períodos, verificou-se a premente necessidade de uma metodologia que seja capaz de assegurar que os documentos arquivísticos digitalizados mantenham suas características nos processos de negócio em meio digital. Nesse ínterim, nesta pesquisa, almeja-se propor procedimentos técnicos que possam ser executados pelos arquivistas das instituições públicas brasileiras nas esferas Federal, Estadual e municipal, bem como pelos Produtores de documentos arquivísticos digitalizados, observando publicações normativas internacionais como Modelo de Referência OAIS, o *Producer-Archive Interface Methodology Abstract Standard* (PAIMAS), e o *Into the Archive - a guide for the information transfer to a digital repository,* produzido pelo Grupo NESTOR. As ferramentas digitais utilizadas, nesta pesquisa, são disponibilizadas, gratuitamente, pelos desenvolvedores, em seus *sites* e apresentam o código-fonte aberto a quem quiser pesquisar e otimizar seu mecanismo de funcionamento, além de serem utilizadas por instituições de pesquisas internacionais que trabalham na temática da preservação digital, por longos períodos. As ferramentas trazidas, neste estudo, apresentam Interface Gráfica de Usuário, no intuito de facilitar a tarefa de criação de SIPs por pessoas que não tenham experiência em trabalhar com interfaces de linha de comando, que requerem conhecimentos mais avançados sobre computação e programação.

A regulamentação presente no Decreto 10.278/2020 decorre da aprovação da Lei nº 13.874/2019, que instituiu a Declaração de Direitos de Liberdade Econômica e estabeleceu normas de proteção à livre iniciativa e ao livre exercício de atividade econômica e disposições sobre a atuação do Estado como agente normativo e regulador, cujo art. 3º, inciso X, confere a toda pessoa natural e jurídica o direito de arquivar qualquer documento por meio digital com produção de efeitos legais e para comprovação de atos públicos. (BRASIL, 2019).

O Decreto 10.278/2020 inicia-se definindo seu objetivo logo no artigo 1º, onde estabelece a técnica e os requisitos para a digitalização de documentos públicos ou

privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais, citando os documentos que ele visa a regulamentar. (BRASIL, 2020).

Logo, em seguida, em seu artigo 2º, o decreto em questão esclarece quem são as pessoas às quais se destinam suas disposições e o objeto que será regulamentado. Nesse caso, o objeto é o documento arquivístico digitalizado produzido por:

> I - pessoas jurídicas de direito público interno,
> II - pessoas jurídicas de direito privado;
> III - pessoas naturais.

É oportuno determinar quem são as pessoas jurídicas de direito interno, pessoas jurídicas de direito privado e pessoas naturais, no intuito de enquadrá-las entre as entidades do PAIMAS, Essa recomendação define a metodologia para a estruturação das ações que são necessárias a partir do tempo inicial de contato entre o Produtor e o Arquivo até os objetos de informação serem recebidos e validados pelo Arquivo. Essas ações abrangem a primeira etapa do Processo *Ingest*, conforme definido no Modelo de Referência OAIS (CONSULTIVE COMMITTEE FOR SPACE DATA SYSTEMS - CCSDS, 2004b).

Assim, partindo da premissa exposta pelo Artigo 41 da Lei nº 10.406/2002, que instituiu o Código Civil, temos que pessoas jurídicas de direito público interno são:

> Art. 41:
> I - a União;
> II - os Estados, o Distrito Federal e os Territórios;
> III - os Municípios;
> IV - as autarquias, inclusive as associações públicas;
> V - as demais entidades de caráter público, criadas por lei.
> Parágrafo único. Salvo disposição em contrário, as pessoas jurídicas de direito público, a que se tenha dado estrutura de direito privado, regem-se, no que couber, quanto ao seu funcionamento, pelas normas deste Código. (BRASIL, 2002).

Da mesma forma, o Artigo 44 da Lei nº 10.406/2002 define que são pessoas jurídicas de direito privado**:**

> Art. 44
> I - as associações;
> II - as sociedades;
> III - as fundações.
> IV - as organizações religiosas;

> V - os partidos políticos.
>
> VI - as empresas individuais de responsabilidade limitada. (BRASIL, 2002).

Já pessoas naturais são definidas pelo Artigo 1º da Lei nº 10.406/2002 como toda pessoa que é capaz de direitos e deveres na ordem civil.

Nesta pesquisa, consideraram-se as pessoas jurídicas de direito público interno, pessoas jurídicas de direito privado e pessoas naturais como Produtoras, partindo do entendimento do PAIMAS e do Modelo de Referência OAIS.

O Arquivo, neste caso, pode ser entendido com um Arquivo OAIS, e constituem-se dos repositórios arquivísticos digitais das instituições integrantes do SINAR.

Os Consumidores serão, neste estudo, considerados como sendo as mesmas pessoas entendidas como Produtores, e que podem estender-se a qualquer cidadão brasileiro que deseje exercer seu direito de acesso a informações estatais de seu interesse, baseando-se Lei nº 12.527/2011, comhecida como Lei de Acesso à Informação.

O Apêndice G traz as Fases de interação entre o Produtor e o arquivo, apresentadas na normativa PAIMAS, a fim de subsidiar esta pesquisa com uma metodologia internacionalmente aceita que possa nortear procedimentos a similares a serem adotados nesta pesquisa.A Transmissão de objetos digitais em modelos de preservação digital internacionais

O *Producer-Archive Interface Methodology Abstract Standard* (PAIMAS), de acordo com Caplan, Kehoe e Pawletko (2010), é um padrão ISO que se baseia no Modelo de Referência para um Sistema de Informação de Arquivo Aberto (OAIS) e utiliza conceitos como definidos nesse documento. Especificamente, ele elabora todas as ações e negociações que um produtor de conteúdo (Produtor) e um repositório (Arquivo) devem tomar, desde o seu contato inicial, por meio da transmissão de SIPs para um repositório, para o recebimento e validação dos SIPs pelo repositório.

De acordo com CCSDS (2004b), as relações entre os Arquivos e os Produtores raramente são simples e fáceis, uma vez que existem sérias dificuldades com a gestão da Interface Produtor-Arquivo em todos os contextos em que foram analisadas na preparação da recomendação PAIMAS, por exemplo, em arquivos tradicionais, bibliotecas, centros de dados científicos, arquivos de negócios. Essas dificuldades, geralmente, levam a um aumento da carga de trabalho e podem ter consequências de impacto negativo sobre a qualidade das informações arquivadas. Elas também podem ter um efeito sobre a relação entre o Arquivo e o Produtor.

Os problemas potenciais incluem o seguinte:

> - os objetos digitais recebidos não estão de acordo com o que o Arquivo espera;
>
> - o que o Produtor entrega não foi claramente definido;
>
> - o cronograma de ingestão não é cumprido pelo Produtor;
>
> - erros nas transferências são detectados tardiamente pelo Arquivo, ou não são detectados antes do uso. (CCSDS, 2004b, p. 1-2).

O PAIMAS é estruturado, relatam Caplan, Kehoe e Pawletko (2010), em torno de fases e ações, que devem ocorrer em ordem. A Fase Preliminar, com 46 etapas e a Fase de Definição Formal, com 36 etapas, culminam com a elaboração de um Acordo de Submissão de Informações. As fases seguintes, que são as Fases de Transferência e Validação, são bastante breves e completam o Projeto Produtor-Arquivo. No Apêndice G - *Fases das Interações Produtor-Arquivo,* apresentam-se essas fases com maior detalhamento

Quaisquer registros que estejam sendo transferidos para o Repositório Digital Confiável, segundo IRMT (2016), devem ser validados, colocados em quarentena e verificados para vírus no ponto de ingerir. As etapas para essa parte do processo de ingestão são as seguintes:

> - Antes do *ingest*[89], os registros devem ser validados ou executados através de um *checksum*[90] que cria um resumo numérico de um registro digital (por exemplo, uma contagem do número de *bits* no registro). Isto permite que o receptor verifique se o fluxo de *bits* recebido é exatamente o mesmo que o enviado. O software de *checksum* inclui o JHOVE[91] e o Jacksum[92].
>
> - Outro *checksum* deve ser executado assim que os registros digitais forem transferidos para o repositório.
>
> - Os dois *checksums* então devem ser comparados. Se forem idênticos, o registro tem foi transmitida corretamente para o repositório digital.
>
> - Uma vez validados, os registros digitais precisam ser colocados em quarentena para garantir que os novos registros ingeridos não infectarão o repositório digital com nenhum vírus. Todos os registros ingeridos em um repositório digital devem ser colocados em quarentena em um servidor separado ou outra localização na rede por até 30 dias antes de serem realmente colocados no repositório. Isto é necessário para que programas de varredura de vírus atualizem seus bancos de dados, garantindo assim que todos os vírus possam ser detectados e removidos.
>
> - Uma vez realizada a verificação do vírus, deve ser executado um *checksum* final e comparado com o *checksum* após o *ingest*, novamente para garantir que o registro digital não tenha sido corrompido ou alterado durante qualquer um dos procedimentos de ingestão.

[89] Ingestão.
[90] Soma de verificação
[91] *JSTOR/Harvard Object Validation Environment.*
[92] Software que realiza somas de verificação.

> Todas essas ações precisam ser registradas nos metadados que são ingeridos com os registros[93]. (IRMT, 2016, p. 74, Tradução nossa).

Para Millar (2009b), o processo de admissão de arquivos em um repositório digital se efetiva da seguinte maneira:

> A fim de garantir que os registros sejam transferidos para o armazenamento com sucesso, os seguintes procedimentos de ingestão também precisam ser seguidos.
>
> 1 Garantir que cada objeto digital a ser transferido tenha um identificador único persistente.
>
> 2 Verificar todos os objetos em busca de vírus e outras formas de códigos maliciosos (Esta é uma das muitas razões pelas quais é essencial garantir que o *software* antivírus esteja disponível e atualizado). Idealmente, os objetos devem ser escaneados, colocados em quarentena por um mês e, após o final deste período, escaneados novamente, para garantir que as víroses muito recentes sejam detectadas. Quaisquer PCs ou servidores usados para a transferência de documentos eletrônicos devem ser protegidos com programas antivírus atualizados.
>
> 3 Antes de transferir quaisquer registros, é necessário efetuar cópias de segurança dos mesmos, verificar sua integridade e armazena-los em uma área segura. Estes registros duplicados devem ser mantidos até que se saiba que o processo de preservação foi bem sucedido; Eles podem ser necessários como cópias-mestras caso algo dê errado com o processo de ingestão.
>
> 4 Uma vez que os registros tenham sido ingeridos, é necessário testar novamente os registros preservados para garantir que qualquer redução na funcionalidade, ou perda de conteúdo, estrutura ou formato, esteja dentro de limites aceitáveis. Se o processo de transferência não incluir nenhuma normalização ou outras etapas que afetem a codificação do arquivo dos componentes digitais, então um meio de validação dos registros é realizar um *checksum*, uma vez que discutido anteriormente. O *checksum* é executado antes e depois que os registros são transferidos a fim de confirmar que os registros não foram alterados durante a transferência. Se

---

[93] Texto original: *Any records being transferred into the TDR must be validated, quarantined and checked for viruses at the point of ingest. The steps for this part of the ingest process are as follows:*
- Prior to ingest, records should be validated or run through a checksum that creates a numerical summary of a digital record (eg a count of the number of bits in the record).
This enables the receiver to check to see whether the bit stream received is exactly the same as that sent. Checksum software includes JHOVE and jacksum.
- Another checksum should be run once the digital records are transferred to the repository.
- The two checksums then should be compared. If they are identical, the record has been correctly transmitted to the digital repository.
- Once validated, digital records need to be quarantined to ensure that newly ingested digital records will not infect the digital repository with any viruses. All records ingested into a digital repository should be quarantined on a separate server or location on the network for up to 30 days before they are actually placed in the repository. This is for virus scanning programmes to update their virus detection databases, thus ensuring that all viruses can be detected and removed.
- Once the virus check has been performed, one final checksum should be run and compared to the checksum upon ingest, again to ensure that the digital record has not been corrupted or altered during any of the ingest procedures.
All of these actions either need to be logged in the metadata that is ingested with the records.

> os registros tiverem sido corrompidos ou alterados de alguma forma, o checksum marcará o objeto digital como defeituoso.
>
> 5 A integridade de todos os metadados relevantes associados com os registros preservados também deve ser verificada. Em outras palavras, é importante assegurar que nenhum dos metadados foi alterado durante a transferência dos registros. Os metadados também devem ser atualizados para registrar o trabalho que tem sido feito para admitir os registros no repositório. Se a integridade dos registros não puder ser verificada, o processo de preservação terá de ser repetido em novas duplicatas dos registros da fonte. Se neste ponto o processo de ingestão ainda resulta em erros inaceitáveis, todo estratégia de preservação pode precisar ser reavaliada[94]. (MILLAR, 2009b, p. 44-45, Tradução nossa).

Conforme observa-se no descrito acima, pode-se concluir que o processo de admissão é bastante complexo e implica numa série de ações executadas por diferentes *softwares*, mas com um objetivo único, ao final: garantir a correspondência entre os *bits* fornecidos pelo Produtor e o fluxo de *bits* recebido pelo Repositório Digital Confiável, apoiados por metadados que fornecem evidências baseadas em critérios matemáticos e lógicos, através de algorítimos.

---

[94] *In order to ensure records are transferred to storage successfully, the following ingest procedures also need to be followed.*
1 Ensure that each digital object to be transferred has a unique persistent identifier (as discussed earlier).
2 Scan all objects for viruses and other forms of malicious code. (This is one of many reasons why it is essential to ensure that antivirus software is available and up to date.) Ideally, objects should be quarantined for one month after scanning, and rescanned at the end of this period to ensure that very recent viruses can be detected. Any PCs or servers used for the transfer of electronic records should also be protected with up-to-date antivirus software.
3 Before transferring any records, make backup copies of them, verify their integrity and store them in a secure area. These duplicate source records should be held until it is known that the preservation process has been successful; they may be needed as master copies should something go wrong with the ingest process.
4 Once records have been ingested, test the preserved records again to ensure that any reduction in functionality, or loss of content, structure or format, is within acceptable limits. If the transfer process does not include any normalisation or other steps that affect the file encoding of the digital components, then one means of validating records is to perform a checksum, as discussed earlier. The checksum is run before and after the records are transferred in order to confirm that the records are not altered during the transfer. If the records have been corrupted or altered in any way, the checksum will tag the digital object as faulty.
5 The integrity of all relevant metadata associated with the preserved records should also be verified. In other words, it is important to ensure none of the metadata has changed during the transfer of the records. Metadata should also be updated to record the work that has been done to ingest the records into the repository. If the integrity of the records cannot be verified, the preservation process will need to be repeated on new duplicates of the source records. If at this point the ingest process still results in unacceptable errors, the entire preservation strategy may need to be re-evaluated.

4 MODELOS DE REQUISITOS PARA PRESERVAÇÃO DE LONGO PRAZO EM REPOSITÓRIOS DIGITAIS

> Uma vez que a tecnologia evolui a intervalos de tempo cada vez menores e, juntamente com ela, toda a infraestrutura de suporte da informação a preservar, é preciso perceber e agir imediatamente a cada alteração de um componente do sistema de arquivamento digital, não se tratando de escolher essa ou aquela corrente ou linha tecnológica, mas o que importa realmente é a adoção de uma filosofia de monitoramento tecnológico continuado, tornando a mudança aliada da preservação. (THOMAZ; SOARES, 2004, p. 16).

Partindo do Modelo de Referência OAIS, que serviu de base para variadas arquiteturas, padrões e protocolos, conjuntos de metadados e outras questões primordiais para a preservação digital, foram analisados os modelos de critérios NESTOR, TRAC e ACTDR, comparando-os com os requisitos apresentados no RDC-Arq, no intuito de investigar a compatibilidade conceitual entre os modelos.

4.1 DIRETRIZES PARA A IMPLEMENTAÇÃO DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS (RDC-ARQ)

Criadas por meio da Resolução do Conselho Nacional de Arquivos nº 39/ 2014 e alteradas pela Resolução nº 43/2015, *as Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis* (RDC-Arq) visam a orientar os órgãos e as entidades integrantes do Sistema Nacional de Arquivos (SINAR) na implantação de repositórios digitais confiáveis para documentos arquivísticos digitais. (CONARQ, 2015a).

Destaca-se que a principal alteração entre a Resolução n.º 39 e a Resolução n.º 43 foi a modificação da nomenclatura para *Repositórios Arquivísticos Digitais Confiáveis* e o acréscimo à sigla RDC-Arq. De acordo com Gonçalez (2017), tal modificação é bastante pertinente, visto que repositórios arquivísticos digitais 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. Para Gava e Flores (2020) tal modificação traz em si um significado muito importante: ter-se um Repositório Digital Confiável (RDC) adjetivado, ou seja, um RDC Arquivístico, com características específicas, ou seja, um Repositório Digital que incorpora em seu funcionamento princípios e normas arquivísticas, e não apenas um RDC voltado para documentos arquivísticos, no sentido de gerenciar e preservar apenas um tipo específico de material digital, dentre de tantos outros diferentes tipos de materiais digitais.

Segundo a Orientação Técnica n.º 3, Novembro / 2015 - Cenários de uso de RDC-Arq em conjunto com o Sistema Informatizado de Gestão arquivística de Documentos -

SIGAD, um RDC-Arq é um ambiente de preservação e acesso, pelo tempo que for necessário, para documentos arquivísticos digitais, capaz de atender aos procedimentos preconizados pela Arquivologia nas idades corrente, intermediária e permanente, e aos requisitos de um repositório digital. As *Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis* indicam parâmetros para repositórios arquivísticos digitais confiáveis, de forma a garantir a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade, o acesso e a preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais, por longos períodos de tempo ou, até mesmo, permanentemente. Elas visam a orientar os órgãos e as entidades integrantes do SINAR na implantação de repositórios digitais confiáveis para documentos arquivísticos digitais. São integrantes do SINAR:

> - Arquivo Nacional;
> - arquivos do Poder Executivo Federal;
> - arquivos do Poder Legislativo Federal;
> - arquivos do Poder Judiciário Federal;
> - arquivos estaduais dos poderes Executivo, Legislativo e Judiciário;
> - arquivos do Distrito Federal dos poderes Executivo, Legislativo e Judiciário e
> - arquivos municipais dos poderes Executivo e Legislativo. (CONARQ, 2015b, p. 5).

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

Os requisitos do RDC-Arq estão organizados em três conjuntos: Infraestrutura organizacional; Gerenciamento do documento digital; e Tecnologia, infraestrutura técnica e segurança. Logo abaixo, segue Tabela 1, demonstrativo da organização dos requisitos.

TABELA 1 - Organização dos requisitos de um RDC-Arq

Conjuntos	Grupos	Quantidade de Requisitos
I	Infraestrutura organizacional	17
II	Gerenciamento do documento digital	43
III	Tecnologia, infraestrutura técnica e segurança	14

FONTE: Desenvolvido pelo Autor.

Verificou-se, nesta pesquisa, que o RDC-Arq não orienta quanto a procedimentos de auditoria e certificação de repositórios arquivísticos digitais confiáveis.

4.2 CATALOGUE OF CRITERIA FOR TRUSTED DIGITAL REPOSITORIES (NESTOR)

Em dezembro de 2004, o projeto alemão *Network of expertise in the long-term storage of digital resources for Germany* - NESTOR[95] configurou, segundo Dobratz, Schoger e Strathmann (2007), o Grupo de Trabalho NESTOR em Certificação de Repositórios Digitais Confiáveis, composto por representantes de bibliotecas nacionais, estaduais e universitárias, arquivos federais e estaduais, museus, centros de dados, editores e especialistas de certificação, da Alemanha e da Áustria.

O Grupo de Trabalho NESTOR incentiva, relatam Dobratz e Schoger (2005), a implementação de Repositórios de objetos digitais confiáveis e orienta os gerentes de repositório e fornecedores para a padronização e cooperação entre repositórios, fornecendo um catálogo de critério e métricas para a avaliação, levando em consideração as condições do contexto alemão no processo de certificação. De acordo com Dobratz, Schoger e Strathmann (2007),

> Tendo em conta o trabalho da Força-Tarefa Certificação de Repositórios Digitais do *Research Libraries Group* (RLG) em 2002, o grupo NESTOR centrou-se na identificação de características e valores que podem ser relevantes na avaliação de repositórios de objetos digitais (aqueles que já existem, bem como aqueles que são apenas emergentes ou, ainda, só ainda estão sendo planejados). O objetivo é formar uma rede de confiança em que os repositórios digitais possam funcionar como arquivos digitais no longo prazo dentro de vários ambientes: a comunidade de bibliotecas, o mundo de arquivo (em um sentido tradicional), a comunidade do museu, e outros produtores de dados tais como governos, instituições, centros de dados mundiais e editoras[96].

Em janeiro de 2005, o grupo NESTOR realizou uma pesquisa em pequena escala sobre padrões recentes e uso dentro de repositórios digitais. Ele foi seguido por um *workshop* público, em junho de 2005, e de uma mesa redonda especializada, em março 2006. O primeiro grande relatório, a Versão nº1 do catálogo de critérios, foi publicado em junho de 2006 (DOBRATZ; SCHOGER; STRATHMANN, 2007). A Versão nº2 foi publicada, em 2009, e incorporou grande quantidade dos comentários recebidos.

---

[95] Rede de Especialização em Armazenamento de Longo Prazo de Recursos Digitais. Tradução do autor.

[96] Texto original: *Taking into account the work of Digital Repository Certification Task Force of the Research Libraries Group (RLG) in 2002 the NESTOR group has focused on identifying features and values that may be relevant in evaluating digital object repositories (those that already exist as well as those which are just emerging or, as yet, are only planned). The aim is to form a web of trustworthiness in which digital repositories can function as long- term digital archives within various environments: the library community, the archival world (in a traditional sense), the museum community, and other data producers such as government institutions, world data centers, and publishing houses.*

Os critérios são definidos, segundo Bergmeyer *et al.* (2009, p. 1), “em estreita colaboração com uma ampla gama de diferentes organizações de memória, produtores de informações, especialistas e outras partes interessadas.” Essa abordagem aberta garante um alto grau de validade universal, adequação ao uso prático e também para a ampla aceitação dos resultados. O grupo de trabalho é composto por representantes selecionados de vários grupos interessados no arquivamento digital de longo prazo: produtores e utilizadores de informação digital, operadores de arquivos digitais por longos prazos, organizações de memória, e peritos técnicos. O grupo organiza *workshops* e mesas redondas com o intuito de favorecer a cooperação de um público tão vasto (DOBRATZ; SCHOGER, 2005).

O objetivo do Catálogo de Critérios para Repositórios Digitais NESTOR é formular critérios, relativamente abstratos, que podem ser usados para um amplo espectro de repositórios digitais de longo prazo e que vão manter a sua validade por um longo período. Os critérios são, cada um, acompanhados por explicações extensas e exemplos concretos de diferentes áreas, sendo oportuno lembrar que os exemplos são estado-de-arte em termos de tecnologia e organização, embora, em alguns casos eles só possam fazer sentido no contexto de uma determinada tarefa de arquivamento. Eles não pretendem ser completos (BERGMEYER *et al.*, 2009).

O Catálogo de Critérios para Repositórios Digitais Confiáveis do Grupo NESTOR foi compilado, principalmente, para aplicação na Alemanha mas, no entanto, também está sendo discutido e padronizado dentro do contexto internacional. Componentes importantes para a avaliação incluem as exigências locais e as diferenças políticas, jurídicas e financeiras na Alemanha, na Europa e nos EUA para arquivos, museus, bibliotecas, centros de dados, etc., e, portanto, concluem Dobratz e Schoger (2005), há, sem dúvida, uma necessidade de diferentes esquemas de avaliação, levando-se em conta essas condições especiais. É crucial identificar critérios geralmente válidos entre as condições nacionais específicas. Esses critérios encontram-se, entre outras áreas, dentro do quadro legal, da prestação de instituições públicas com recursos financeiros e humanos adequados, da estrutura organizacional nacional e do estado de desenvolvimento nacional no campo da preservação digital, em longo prazo (BERGMEYER *et al.*, 2009). São grupos de interesse em potencial para confiabilidade:

> - usuários do repositório que desejam acessar informações confiáveis - hoje e no futuro;
>
> - produtores de dados e provedores de conteúdo para os quais a certificação fornece um meio de garantia de qualidade ao escolher um serviço potencial fornecedores;

> - alocadores de recursos, agências de financiamento e outras instituições que precisam tomar decisões de financiamento e concessão, e
>
> - repositórios digitais de longo prazo que desejam obter confiabilidade e demonstrar isso ao público, seja para cumprir requisitos legais ou para sobreviver no mercado [97](DOBRATZ; SCHOGER; STRATHMANN, 2007, Tradução nossa.).

Ainda, segundo Dobratz, Schoger e Strathmann (2007) revelam, o Catálogo de Critérios para Repositórios Digitais Confiáveis NESTOR utiliza, por exemplo, os conceitos de Pacote de Informação conforme propõe o Modelo OAIS: Pacote de Informações de Submissão (SIP) para ingestão, Pacote de Informação de Arquivo (AIP) para o armazenamento e Pacote de Divulgação de Informação (DIP) para acesso.

O Modelo de Referência OAIS serve, sempre que possível, como base para a terminologia e estrutura do Catálogo de Critérios para Repositórios Digitais Confiáveis NESTOR, argumenta Bergmeyer *et al.* (2009), uma vez que os conceitos do OAIS são usados para descrever os principais processos de preservação digital, desde a ingestão, armazenamento de arquivos até o acesso, bem como descreve o ciclo de vida de objetos digitais no repositório.

4.2.1 Autoavaliação e Certificação utilizando o Catálogo de Critérios NESTOR

De acordo com Bergmeyer *et al.* (2009), o processo de autoavaliação estendida para arquivos digitais desenvolvidos pelo Grupo de trabalho NESTOR com base na norma *Deutsches Institut Fur Normung*[98] (*DIN) 31644 - Information and documentation - Criteria for trustworthy digital archives*[99]*,* oferece aos arquivos digitais um método harmonizado e prático de verificar se são confiáveis. Se a avaliação revisada produzir um resultado positivo, eles terão o direito de divulgá-la, usando o Selo NESTOR para *Trustworthy Digital Archives*[100].

> Este é o foco principal do trabalho do grupo de trabalho NESTOR "Repositórios confiáveis - Certificação". Ele identifica critérios que permitem avaliar a confiabilidade de um repositório digital, nos níveis organizacional e técnico. Os critérios são definidos em estreita colaboração com uma ampla gama de diferentes organizações de memória, produtores de informações, especialistas e outras partes interessadas. Essa abordagem aberta garante

---

[97] Texto original: *Potential interest groups for trustworthiness are: repository users who want to access trustworthy information - today and in the future, data producers and content providers for whom certification provides a means of quality assurance when choosing potential service providers, resource allocators, funding agencies and othe institutions that need to make funding and granting decisions, and long-term digital repositories that want to gain trustworthiness and demonstrate this to the public either to fulfill legal requirements or to survive in the market.*

[98] Instituto Alemão de Normalização. Tradução do autor.

[99] Informação e documentação - Critérios para arquivos digitais confiáveis. Tradução do autor.

[100] *Arquivos Digitais Confiáveis*. Tradução do autor.

> um alto grau de validade universal, adequação ao uso prático diário e também ampla aceitação dos resultados. O presente catálogo de critérios representa um marco importante no caminho para alcançar os objetivos do grupo de trabalho. As organizações de memória devem receber uma ferramenta bem construída, coordenada e prática para alcançar e provar sua confiabilidade. No entanto, a intenção é também apresentar a opção de documentar a confiabilidade por meio da certificação em um processo nacional ou internacional padronizado. O catálogo também suporta a participação ativa nos esforços de padronização internacionais existentes[101]. (BERGMEYER *et al*., 2009, p. 1).

Embora o Selo NESTOR possa ser obtido como uma solução independente, ele também enquadra-se no Quadro Europeu de Auditoria e Certificação. Além da Certificação Básica fornecida pelo Selo de Aprovação de Dados, o Selo NESTOR concede uma Certificação Estendida. (BERGMEYER *et al*., 2009).

Na Tabela 2, abaixo, apresentam-se as instituições certificadas com o Selo NESTOR - Versão Básica, até a data de publicação desta pesquisa.

TABELA 2 - Instituições Certificadas com o Selo NESTOR - Versão Básica

Instituição Certificada	**Ano**
Biblioteca de Informações Técnicas (TIB[102]) Hanover	2017
Centro de Informações de Economia de Leibniz (ZBW[103])	2017
Arquivamento de dados e serviços de rede (DANS[104])	2016
Biblioteca Nacional Alemã (para publicações em rede)	2016

FONTE: NESTOR, 2020. (Tradução nossa).

Em 2015 e 2016, os processos e sistemas de arquivamento digital de longo prazo na Biblioteca Nacional da Alemanha foram submetidos, segundo NESTOR, a uma autoavaliação estendida de acordo com a *DIN 31644*. Em 2016, as atividades na área de publicações on-line receberam o Selo NESTOR de Arquivos Digitais Confiáveis. Isso representa o nível de "Certificação Estendida" (NESTOR, 2020).

> Para a obtenção do *NESTOR Seal for Trustworthy Digital Archives,* o repositório a ser auditado/certificado deve requerer a avaliação por parte do

---

[101] Texto original: *This is the main focus of the work of the NESTOR working group "Trusted repositories - Certification". It identifies criteria which permit the trustworthiness of a digital repository to be evaluated, both at the organisational and technical levels. The criteria are defined in close collaboration with a wide range of different memory organisations, producers of information, experts and other interested parties. This open approach ensures a high degree of universal validity, suitability for daily practical use and also broad-based acceptance of the results. The present criteria catalogue represents an important milestone on the road towards achieving the working group's goals. The memory organisations should be given a well-constructed, coordinated and practical tool for achieving and proving their trustworthiness. However, the intention is also to present the option of documenting trustworthiness by means of certification in a standardised national or international process. The catalogue also supports active participation in existing international standardisation efforts.*

[102] *TIB Technische Informationsbibliothek Hanover.*

[103] *ZBW Leibniz-Informationszentrum Wirtschaft.*

[104] *Data Archiving and Networked Services*.

> Grupo NESTOR, e cada um das partes nomeará representantes para contatos. O NESTOR define o caléndario do processo, e o repositório começa por fazer a auto avaliação, utilizando o formulário de verificação e as instruções para cada critério. A aplicação de cada critério deve ser verificada para o caso em questão, podendo excluir-se alguns critérios desde que tal exclusão seja justificada devidamente. Depois de determinar quais são os critérios aplicáveis, o repositório deve responder, comprovando através de documentos e detalhando o cumprimento de cada requisito. Após a autoavaliação, a documentação é entregue ao responsável do designado pelo Grupo NESTOR, que verificará se a informação fornecida corresponde aos critérios, se é consistente, e se as soluções oferecidas são apropriadas para as tarefas e objetivos do repositório avaliado. Caso não haja questões, este emitirá um relatório, que será verificado pelo segundo revisor do NESTOR, que decidirá a atribuição do Certificado. Em seguida, o Grupo NESTOR e o repositório são informados, e caso este último não concorde com a decisão, pode apelar ao grupo de trabalho de certificação do NESTOR. O Selo tem validade a partir da publicação do relatório, das respostas e dos documentos no seu sítio *web* e após o NESTOR o acrescentar ao registro de repositórios certificados. O Selo indica o ano em que foi emitido e formalmente, a sua validade é indefinida, dependendo de futuras revisões e reavaliações. (CORUJO, 2014, p. 115).

4.2.2 Procedimento de autoavaliação para a obtenção do Selo NESTOR para Arquivos Digitais Confiáveis

Harmsen *et al.* (2013) explica os procedimentos para uma auto avaliação com o objetivo de obter o Selo NESTOR. Abaixo, apresentam-se esses procedimentos, no intuito de subsidiar bases para um procedimento semelhante para o RDC-Arq:

> 1. A instituição avaliada notifica o Grupo NESTOR de sua intenção; Ela planeja e nomeia duas pessoas de contato para o procedimento. A instituição deve especificar o objeto da avaliação com precisão. Se uma instituição opera uma série de arquivos, estes podem ser avaliados conjuntamente ou separadamente, o que pode resultar numa série de diferentes Selos NESTOR. Se avaliações a serem realizadas dentro de um arquivo forem múltiplas, estas devem ser ponderadas, descritas na íntegra no com base nos critérios relevantes, e avaliados. A instituição pode incluir os serviços entregues pelos prestadores de serviços na avaliação.
>
> 2. O Grupo NESTOR confirma o início o procedimento de avaliação para a instituição, nomeia uma ou mais pessoas que serão responsáveis pela revisão destes e define os prazos de processamento relevantes para ambas as partes. A auditoria completa não deve demorar mais de três meses. (HARMSEN *et al.*, 2013, p. 3).
>
> 3. O arquivo que deseja obter o Selo NESTOR começa sua autoavaliação. As ferramentas incluem um formulário de avaliação e as instruções e explicações relativas aos critérios individuais. A pessoa designada responsável pela avaliação pode ser contatada para questões de esclarecimento. A aplicabilidade de cada critério da norma deve ser primeiramente verificada para o caso em questão. Os critérios individuais podem ser excluídos: deve ser dada uma justificação suficiente se um critério é considerado não-aplicável. Uma vez que os critérios aplicáveis tenham sido determinados, o arquivo digital fornece informações sobre cada um deles. O arquivo digital avaliado fornece um relatório escrito suficientemente abrangente sobre o *status* de implementação de cada

> critério individual. Ele faz referência a documentos em que a situação particular está documentada, ou as anexa se não forem públicas disponíveis. (HARMSEN *et al.*, 2013, p. 4).

O arquivo realiza sua autoavaliação, atribuindo pontos com base no cumprimento da escla abaixo (Tabela 3):

TABELA 3 - Escala de avaliação - NESTOR

Status de aplicabilidade do critério	**Pontuação**	**Explicação sobre o *status* do critério**
Ainda não acionado	0	Ainda não existem planos de cumprimento ou documentos para o critério.
Planejado	3	Foi elaborado um plano escrito para o cumprimento do critério. O plano não se baseia apenas nas abordagens publicadas em outros lugares, também se refere à situação específica no arquivo.
Planejado em detalhes	6	Os planos foram preparados em detalhes. Todos os planos necessários, informações e aprovações foram fornecidas ou obtidas para implementação, que já foi iniciada.
Implementados	10	Os planos foram implementados de forma organizacional e/ou tecnicamente. As medidas foram incorporadas nas operações em andamento do arquivo.

FONTE: Harmsen (2013, p. 4, Tradução nossa). Adaptado.

> No caso de uma classificação de avaliação de 6 e 10 pontos, os documentos, geralmente, são autorizados e, em muitos casos, publicados. Se os documentos não puderem ser publicados devido a direitos autorais, segredos corporativos ou razões de segurança, eles devem ser disponibilizados para os auditores. A confidencialidade é assegurada durante a revisão. Documentos de trabalho que foram submetidos para avaliação mas ainda não foram publicados são suficientes para uma classificação de 3 pontos.
>
> Para obter o Selo NESTOR, os critérios de avaliação de 1 a 12, apresentados no Catálogo de Critérios para Repositórios Digitais Confiáveis do Grupo NESTOR, não podem ser excluídos da avaliação e, em cada caso, ao menos 10 pontos devem ser pontuados. Uma média de 7 pontos deve ser dada para os demais critérios aplicáveis. Esses requisitos mínimos podem mudar conforme os avanços surgem no arquivamento digital. O Grupo NESTOR deve atualizar as exigências em intervalos regulares de tempo. (HARMSEN *et al.*, 2013, p. 5).
>
> 4. Ao final da autoavaliação, o arquivo que deseja receber o Selo NESTOR apresenta sua documentação para a pessoa de contato do Grupo NESTOR. A autoavaliação e os documentos apresentados ou referenciados devem ser em alemão ou inglês. Os documentos serão então submetidos a uma verificação de plausibilidade, por um revisor do Grupo NESTOR.

Questionamentos de verificação de plausividade:

> -As informações fornecidas atendem aos critérios e correspondem às notas relacionadas? Estão completas e atualizadas? Estão claras e compreensíveis?
>
> -As informações são apresentadas de forma lógica, são internamente consistentes?
>
> -As soluções são apropriadas em termos dos objetivos do arquivo digital e tarefas?. (HARMSEN *et al.*, 2013, p. 5, Tradução nossa)[105].

Se o revisor chegar a conclusões diferentes sobre a situação em relação às do arquivo digital propriamente dito, o Repositório será solicitado a emitir uma declaração. Ao final da auditoria, o revisor redigirá um relatório e o encaminhará ao segundo revisor.

> 5. O segundo revisor verifica o trabalho do primeiro revisor e, em seguida, após consulta com o primeiro revisor, determina o total de pontos finais para a auto avaliação. Finalmente, o segundo revisor decide se o Repositório pode ser premiado ou não com o Selo NESTOR. Um relatório de revisão contendo um resumo dos resultados é escrito. Ele contém as seguintes informações: data da revisão, objeto de revisão, número de critérios aplicados, pontos alcançados no total e por critério, justificações para os critérios de exclusão. O Repositório avaliado e o Grupo NESTOR são informados. Se o arquivo não concorda com a decisão, pode interpor um recurso junto ao Grupo de Trabalho de Certificação NESTOR. Este grupo de trabalho decide em todas as disputas e se algum aspecto dos procedimentos não está claro. (HARMSEN *et al.*, 2013, p. 5).
>
> 6. O Selo é válido após uma avaliação positiva ser emitida, uma vez que o arquivo digital publicou o relatório de revisão, suas respostas de avaliação e todos documentos relevantes, juntamente com o Selo em uma posição facilmente localizáveis em seu *website* e adicionado ao registro de arquivos certificados pelo escritório administrativo NESTOR. O Selo inclui o ano de emissão. Formalmente, ele é válido indefinidamente. Entretanto, é provável que sua relevância diminua após alguns anos, a menos que uma nova revisão seja conduzida. No entanto, não há necessidade de repetir o procedimento. (HARMSEN *et al.*, 2013, p. 6).

Tendo em vista os procedimentos desenvolvidos pelo Grupo NESTOR, tenciona-se sugerir a utilização de procedimentos semelhantes para proceder a autoavaliação de um repositório arquivístico digital que pretende declarar-se confiável.

4.2.3 Critérios avaliativos para a Certificação com o Selo NESTOR

Harmsen *et al.* (2013) apresentam 34 critérios avaliativos para submissão junto aos arquivos digitais das instituições que desejam o selo NESTOR.

---

[105] Texto original: *• Does the information provided meet the criteria and correspond to the related notes? Is it complete and up-to-date? Is it clear and comprehensible?*
• Is the information presented in a logical form, is it internally consistent?
• Are the solutions appropriate in terms of the digital archive's targets and tasks?

Os critérios avaliativos para certificação com o Selo NESTOR apresentam a seguinte estrutura, mostrada na Tabela 4: - Estrutura dos critérios avaliativos para certificação com o Selo NESTOR

C1 Seleção de objetos de informação e suas representações
Em que medida o critério deve ser cumprido?
Explicação
Perguntas
Documentos

FONTE: Harmsen *et al.* (2013, adaptado pelo autor).

Abaixo, apresenta-se no Quadro 3, o critério C1 das *Notes on the individual criteria*[106], de Harmsen *et al.* (2013), a título de exemplo.

QUADRO 3 - Critério C1. *Notes on the individual Criteria*

C1 Seleção de objetos de informação e suas representações
Foram definidos critérios para a seleção de objetos de informação e suas representações no arquivo digital. A estrutura é fornecida por obrigações legais, pela função básica da instituição ou empresa, seus próprios alvos.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Isso diz respeito ao papel ou missão do arquivo digital. O tipo de informação digital pela qual o arquivo digital é responsável deve ser claro tanto interna quanto externamente. A seleção deve ser documentada de forma transparente, com base em critérios, diretrizes e perfis. A C1 faz parte da definição dos objetivos e tarefas do arquivo digital e, portanto, é crucial para avaliar sua confiabilidade, especialmente ao avaliar a adequação de cada atividade.
Perguntas
- Que critérios foram estabelecidos para selecionar os objetos de informação e suas representações? - Qual é a justificativa para esses critérios? - Como os critérios podem ser acessados, interna e externamente?
Documentos
Critérios publicados para a seleção dos objetos de informação e suas representações: base legal, diretrizes de coleta, catálogos e regras para avaliação e seleção.

FONTE: Harmsen *et al.* (2013, p. 7, Tradução nossa).

A utilização da ferramenta acima descrita auxilia a equipe de auditoria a produzir a documentação que fundamenta cada avaliação proferida, possibilitando aos revisores detalhar suas observações, justificando-as.

4.2.4 Estrutura Conceitual do Catálogo de Critérios para Repositórios Digitais Confiáveis NESTOR

O Catálogo de Critérios para Repositórios Digitais Confiáveis NESTOR dispõe seus atributos organizados em três seções (A, B C), apresentados no Quadro 4. Cada Seção é dividida em Grupos de Critérios com base no escopo de seus critérios, da seguinte forma:

[106] Notas sobre os critérios individuais. Tradução do autor.

QUADRO 4 - Estrutura Conceitual do Catálogo de Critérios para Repositórios Digitais Confiáveis NESTOR

Seções	Grupos de Critérios	N° de critérios	Quantidade total de critérios por Seção
A. Estrutura organizacional	1. No repositório digital, definiram-se os seus objetivos.	3	16
	2. No repositório digital, confere-se a sua(s) comunidade(s) designada(s) acesso adequado para as informações representadas pelos objetos digitais.	2	
	3. São observadas as regras legais e contratuais.	3	
	4. A forma organizacional é apropriada para o repositório digital.	6	
	5. No Repositório Digital, realiza-se o gerenciamento adequado da qualidade.	2	
B. Gerenciamento de Objetos	6. No repositório digital, assegura-se a integridade dos objetos digitais, durante todas as fases de processamento.	3	23
	7. O repositório digital garante a autenticidade dos objetos digitais durante todas as fases de processamento.	3	
	8. No repositório digital, tem-se um plano estratégico para as suas medidas de preservação técnicas (planejamento de preservação).	1	
	9. No repositório digital, aceitam-se objetos digitais dos produtores com base em critérios definidos.	3	
	10. O armazenamento de arquivo dos objetos digitais é realizado com as especificações definidas.	4	
	11. No repositório digital, permite-se o uso dos objetos digitais com base em critérios definidos.	2	
	12. O sistema de gerenciamento de dados é capaz de fornecer as funções de repositório digital necessárias.	7	
C. Infraestrutura e Segurança	13. A infraestrutura de TI é apropriada.	2	3
	14. A infraestrutura protege o repositório digital e seus objetos digitais.	1	
Total de Critérios			42

FONTE: Bergmeyer *et al.* (2009). Adaptado.

Cada critério do Catálogo da NESTOR é apresentado e, logo abaixo dele, são disponibilizadas explicações gerais sobre esse critério. A seguir, são apresentados exemplos, comentários e notas de diferentes áreas de aplicação, uma vez que um critério pode ser usado em repositórios de arquivos, bibliotecas, museus, entidades privadas prestadoras de serviços, dentre outras possibilidades. Ao final, são relacionadas referências literárias que convergem para informações no ínterim da ação discutida no critério.

Abaixo, na Tabela 5 apresenta-se uma síntese da estrutura do catálogo de critérios NESTOR:

TABELA 4 - Estrutura de um critério - Catálogo de Critérios NESTOR

Critério
Explicações gerais sobre este critério
Exemplos, comentários, notas de diferentes áreas de aplicação.
Literatura relacionada a este critério

FONTE: Bergmeyer *et al.* (2009). Adaptado.

Exemplo de Critério do Catálogo NESTOR.

QUADRO 5 - Critério do Catálogo NESTOR nº 14

Critério	**14 A infraestrutura protege o repositório digital e seus objetos digitais.**
Explicações gerais do critério	A infraestrutura deve proteger os objetos digitais de riscos baseados em sistemas e riscos externos. Perigos baseados em sistemas poderiam surgir, por exemplo, em razão dos problemas de *hardware* ou fracasso dos meios de armazenamento individual. Externamente, a primeira prioridade do Repositório Digital deve ser proteger contra ameaças naturais (por exemplo, fogo, água, atividade sísmica), e também contra os riscos provocados pelos seres humanos. Os objetos podem ser prejudicados diretamente por funcionários ou, por meio de programas nocivos contrabandeados para o sistema (por exemplo, vírus). Proteger os dados também envolve impedindo o envio não intencional de informações por programas (*trojans*) ou pessoas (espionagem). A proteção deve cobrir os objetos, as instalações utilizadas pelo Repositório Digital, o hardware, software e, não menos importante, o pessoal. Os diferentes riscos devem ser contrabalançados por um pacote técnico (por exemplo, programas de proteção antivirus) e medidas organizacionais (por exemplo, restrições de acesso).
Exemplos, comentários, notas de diferentes áreas de aplicação	Um incêndio que eclode no edifício principal da instituição que abriga o Repositório Digital não deve resultar em danos aos objetos ou perda de dados, pois deve haver um sistema de backup adequado em um local separado que possa assumir operações em caso de sinistro.
Literatura relacionada a este critério	BSI: Leitfaden IT-Sicherheit. IT-Grundschutz kompakt, 2007. BSI: IT-Grundschutz-Kataloge, 2007.

FONTE: Bergmeyer *et al.* (2009, p. 37, Tradução nossa.)

A disponibilização de explicações gerais sobre o critério, bem como a disponibilização de literatura relacionada ao critério e exemplos e comentários de diferentes áreas de aplicação proporcionam um ambiente que favorece ao intercâmbio de conhecimento entre profissionais de TI, equipe de preservação digital e os produtores de informação.

4.3 TRUSTWORTHY REPOSITORIES AUDIT & CERTIFICATION: CRITERIA AND CHECKLIST (TRAC)

O TRAC é uma prática recomendada desenvolvida pelo RLG/ NARA em 2007 e que, após aperfeiçoamentos sofridos, evoluiu para normativa ACTDR, que tornou-se o padrão internacional ISO 16363:2012, fornecendo às instituições diretrizes para a realização de auditorias internas para avaliar a confiabilidade dos repositórios digitais e cria uma

estrutura para suportar a certificação externa de repositórios digitais. O TRAC estabelece critérios, evidências, melhores práticas e controles que os repositórios digitais podem usar para avaliar suas atividades nas áreas de infraestrutura organizacional, gerenciamento de objetos digitais e infraestrutura técnica e gerenciamento de riscos. (WELCH; PHILLIPS, 2014).

Essa nova ferramenta de auditoria representa o trabalho de muitos especialistas, por meio de uma gama internacional de comunidades em organizações de pesquisa, governos, arquivos de dados e patrimônio cultural. Os membros foram escolhidos, tendo em vista sua experiência na construção e gerenciamento de repositórios digitais. Além disso, mais de um ano de rascunho público e discursos em conferências permitiram obter *insights* e contribuições inestimáveis da comunidade, tentando entender e utilizar a lista de verificação de auditoria. (OCLC, 2007).

Sobre a preservação a longo prazo, em repositórios digitais e sobre a necessidade de avaliação e certificação:

> A comunidade de preservação digital passou a não apenas reconhecer, mas abraçar o fato de que nem todos repositórios serão "iguais". Essa diversidade foi amplamente esclarecida pela proliferação de tipos de repositórios (repositórios institucionais, repositórios de acesso aberto, repositórios digitais, repositórios de preservação, arquivos digitais etc.) nos níveis local, regional, nacional e internacional. Em muitos desses repositórios, a preservação não é o objetivo principal ou a prioridade explícita. Com isso é fácil entender por que alguns repositórios podem não optar por buscar a certificação, assim como é fácil perceber por que outras pessoas devem se sentir compelidas (ou talvez obrigadas) a buscar certificação[107]. (OCLC, 2007, p. 5, Tradução nossa).

Os critérios do TRAC foram criados para serem aplicáveis a qualquer tipo de repositório ou arquivo digital. Em cada critério foram fornecidos exemplos ilustrativos, embora esses exemplos não devam ser interpretados como aplicações exaustivas. Esses critérios são aplicáveis a bibliotecas, museus, arquivos, arquivos de dados científicos, etc., bem como os dados extremamente heterogêneos produzidos e coletados por esse tipo de organização (OCLC, 2007).

Três organizações trabalharam para estabelecer um processo internacional unificado de certificação:

---

[107] Texto original: *"The digital preservation community has come to not only recognize but embrace the fact that not all repositories will be "equal." This diversity has been made abundantly clear by the proliferation of repository types (institutional repositories, open-access repositories, digital repositories, digital preservation repositories, digital archives, etc.) on local, regional, national, and international levels. For many of these repositories, preservation is not the primary purpose or explicit priority. With that understanding, it is easy to comprehend why some repositories may not choose to pursue certification, just as it is easy to see why others should feel compelled (or perhaps be compelled) to pursue certification."*

a) O *Center for Research Libraries*[108] (CRL), através do projeto Auditoria e Certificação de Arquivos Digitais, financiado por uma bolsa da Fundação Andrew W. Mellon;
b) O *Digital Curation Center*[109] (DCC), em conjunto com o projeto CRL e através de auditorias de testes independentes no Reino Unido;
c) O grupo de trabalho de certificação do NESTOR (*Network of Expertise in Long-Term Storage of Digital Resources*[110]), na Alemanha.

Ressalta-se que esses esforços para mesclar o desenvolvimento de um processo de certificação destacaram diferenças pequenas mas importantes entre os critérios nesta lista de verificação de auditoria e o Catálogo de Critérios NESTOR, por exemplo. Por enquanto, um conjunto único e padronizado de critérios e regras aplicáveis se mostrou impraticável por razões geopolíticas (OCLC, 2007).

As seguintes instituições foram auditadas e certificadas pela CRL, utilizando o TRAC:

TABELA 5 - Instituições auditadas e certificadas pela CRL utilizando o TRAC

Instituição Certificada	**Ano**
Canadiana.org	2014
Chronopolis	2010/2011
CLOCKSS	2013/2014
Hathitrust	2009/2010
Portico	2009
Scholars Portal	2013

FONTE: Center for Research Libraries (CRL, 2021, Tradução nossa).

A lista de verificação TRAC é dividida em três Seções, sendo que cada Seção corresponde a um Grupo de Critérios. Cada Grupo de Critérios apresenta uma quantidade de critérios constituintes, organizados conforme o Quadro 6:

[108] Centro de Bibliotecas de Pesquisa. Tradução do autor.
[109] Centro de Curadoria Digital. Tradução do autor.
[110] Rede de Especialização em Armazenamento de Longo Prazo de Recursos Digitais. Tradução do autor.

QUADRO 6 - Estrutura dos critérios - TRAC

Seções	Grupos de Critérios	Quantidade de critérios
A	Infraestrutura organizacional	24
B	Gerenciamento de objetos digitais	44
C	Tecnologias, infraestrutura técnica e segurança.	16

FONTE: OCLC (2007). Adaptado pelo autor.

Apresenta-se, no Quadro 7, a estrutura do Critério A1.1 da Lista de auditoria e Certificação TRAC, como exemplo de critério característico do TRAC.

QUADRO 7 - Estrutura de um critério da Lista de auditoria e Certificação TRAC

Seção	A Infraestrutura organizacional
Grupo	A1. Governança e viabilidade organizacional
Explicações sobre o Grupo	Independentemente do tamanho, escopo ou natureza do programa de preservação digital, um repositório confiável deve demonstrar um compromisso explícito, tangível e de longo prazo com o cumprimento das normas, políticas e práticas vigentes.
Critério	A1.1 O repositório tem uma declaração de missão que reflete um compromisso a longo prazo de retenção, gerenciamento e acesso à informação digital.
Explicações sobre o Critério	A declaração de missão do repositório deve ser claramente identificada e acessível aos depositantes e outras partes interessadas e conter um compromisso explícito de longo prazo.
Evidência	Declaração de missão para o repositório; declaração de missão para o contexto organizacional no qual o repositório se encontra; mandato legal ou legislativo; exigências regulatórias.

FONTE: OCLC (2007, Tradução nossa). Adaptado pelo autor.

Abaixo, apresenta-se a listagem de verificação (*checklist*) proposta pelo TRAC, consolidada no Quadro 8, e utilizada para as ações de autoavaliação, auditoria e certificação de Repositórios Digitais Confiáveis.

QUADRO 8- Criteria Checklist

Trustworthy Repositories Audit & Certification: Criteria Checklist					
Organização:		**Auditor:**		**Página:**	
Seção:		**Entrevistados:**		**Data:**	
Aspecto:					
Critério:	**Evidências (Documentos) Examinadas:**		**Descobertas e observações :**		**Resultado:**

FONTE: OCLC (2007, Tradução nossa).

Verificou-se que Online Computer Library Center (OCLC) não detalha os processos de autoavaliação, auditoria e certificação de repositórios digitais. Entretanto, as instituições certificadas disponibilizaram a documentação referente ao processo de suas certificações no síte do CRL.

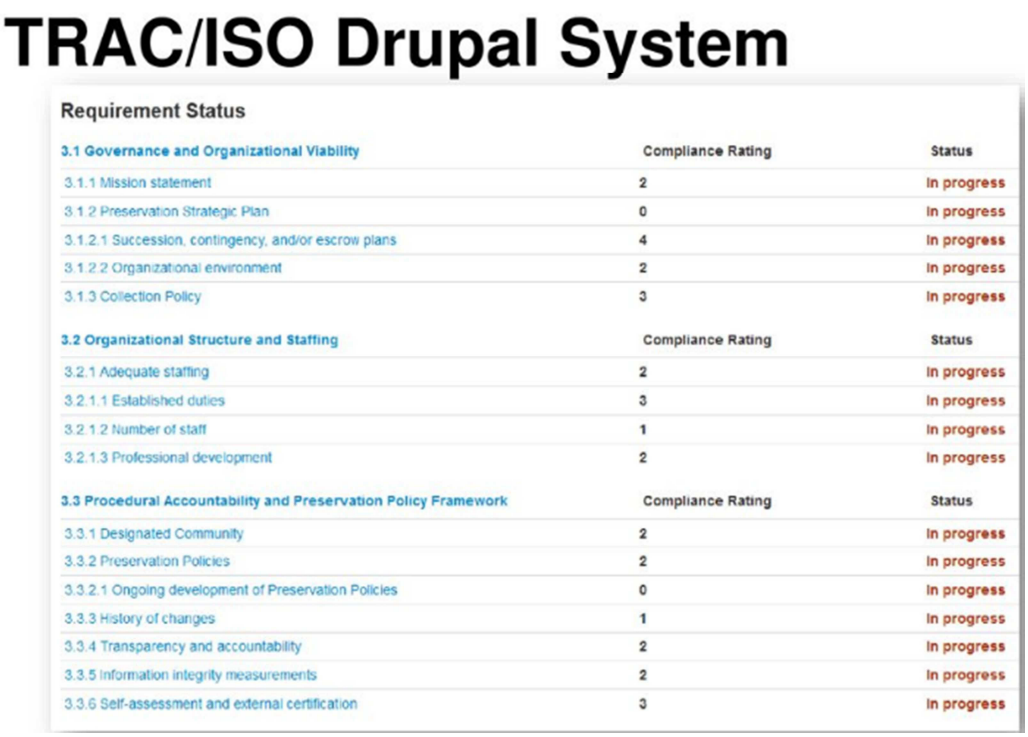
4.3.1 Ferramenta Drupal TRAC *Review*

A ferramenta Drupal TRAC *Review* foi desenvolvida pelo *Massachusetts Institute of Technology* (MIT) em um projeto liderado por Nancy McGovern, Diretora de Preservação de Bibliotecas de Digitais. Consiste uma ferramenta de auditoria para avaliar a confiabilidade, comprometimento e prontidão das instituições para assumir responsabilidades de preservação a longo prazo. (OCLC, 2007).

Hospedado pela Artefactual (mesma empresa que disponibiliza os softwares Archivematica e o ICA-Atom) para uso da comunidade, essa aplicação é baseada no *Trustworthy Repositories Audit & Certification -TRAC.* (OCLC, 2007).

A ferramenta *Drupal TRAC Review* fornece uma estrutura para avaliar a conformidade com os requisitos identificados no TRAC. Cada requisito do TRAC possui uma página na qual a instituição avaliada pode fornecer evidências de sua conformidade com os requisitos e uma classificação de conformidade é atribuída. A evidência de conformidade é fornecida na forma de políticas institucionais documentadas (THE UNIVERSITY OF BRITISH COLUMBIA LIBRARY - UBC, 2017 on-line). Na Figura 15, é apresentado o *status* da situação dos requisitos TRAC, utilizando a *ferramenta Drupal TRAC Review*.

FIGURA 15 - Drupal Trac Review Tool. Imagem da tela inicial



FONTE: TRAC review tool. @rchivematica, [S.l.], 2007.

Na ferramenta Drupal TRAC *Review,* definem-se cinco níveis de conformidade, apresentados na Tabela 7:

TABELA 6- Nível de Conformidade - Ferramenta Drupal TRAC *Review*

Nível de Conformidade	**Status de Conformidade**
0	Não-conforme
1	Ligeiramente conforme
2	Meio em conformidade
3	Em conformidade com a maioria
4	Totalmente em conformidade

FONTE: TRAC review tool. @rchivematica, [S.l.], 2007. Adaptado pelo autor.

Durante o desenvolvimento desta investigação, verificou-se que, embora OCLC (2007) não tenha definido níveis de conformidade para seus critérios, a Ferramenta Drupal TRAC Review preocupou-se com a natureza da binária do processo de auditoria e certificação desenvolvidos no TRAC, levando em conta a natureza de evolução continuada dos projetos de implementação típicos da área de TI.

4.4 AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES (ACTDR)

Desde que a lista de verificação TRAC foi atualizada por um grupo de trabalho e colaboradores liderados por David Giaretta, tornou-se o *Mission Operations Information Management Services Repository Audit and Certification*[111] (MOIMS-RAC), do Grupo de Trabalho do CCSDS. O grupo de trabalho e seus colaboradores trabalharam com a Organização Internacional de Padronização (ISO), para formalizar o TRAC como ISO 16363:2012 - *Audit and Certification of Trustworthy Digital Repositories*[112]. Em 14 de fevereiro de 2012, este trabalho atingiu a etapa 60:60, "*International Standard published*[113]". (WITT *et al*., 2012, p. 3).

> O ACTDR tem por objetivo realizar um processo contínuo de auditoria, julgando as áreas que necessitam ser melhoradas. O *status* de confiança não é atingido uma única vez, logo, será necessário manter um ciclo regular de auditoria e certificação, para que assim, possa ser demonstrada. (SANTOS, 2019, p. 168).

O ACTDR é uma recomendação técnica a ser usada como base para fornecer auditoria e certificação da confiabilidade dos repositórios digitais. Ele fornece uma

[111] Auditoria e Certificação do Repositório de Serviços de Gerenciamento de Informações de Operações de Missão. Tradução do Autor.
[112] Auditoria e Certificação de Repositórios Digitais Fidedignos. Tradução do autor.
[113] Norma Internacional publicada. Tradução do autor.

especificação detalhada dos critérios pelos quais os repositórios digitais devem ser auditados. O ACTDR faz uso de conceitos do Modelo de Referência *Open Archival Information Systems* (OAIS), e permite a avaliação e certificação de um repositório como sendo um Repositório Digital Confiável. (CCSDS, 2011).

O ACTDR inicia-se com uma introdução que explica o seu Escopo, seu Propósito e sua Aplicabilidade, assim como a estrutura e terminologia empregadas no documento. A segunda seção define um Repositório Digital Confiável e métricas de avaliação. As três últimas seções da ISO 16363 compreendem as métricas em si. Cada métrica inclui uma concisa declaração do critério, uma frase de apoio que explica a importância e a relevância do critério, um parágrafo que traz exemplos de evidências que poderiam ser utilizadas para demonstrar que o repositório cumpre o critério, e uma discussão mais longa que proporcione mais informações e contexto do critério, incluindo relações com ou dependências de outros critérios. (CCSDS, 2011).

Na Seção terceira, Infraestrutura organizacional, abordam-se questões como Governança e Estrutura organizacional, Pessoal, Responsabilidade Processual, Estrutura Política, Financeiro, Sustentabilidade e Contratos, Licenças e Responsabilidades. Na Seção 4, Gerenciamento de Objetos Digitais, avalia-se a aquisição de conteúdo, criação do Pacote de Informações de Arquivamento (AIP), planejamento de preservação, a preservação real das AIPs e a gestão da informação (metadados) e acesso. Finalmente, a seção 5 explica as métricas relacionadas à Infraestrutura Técnica e Gestão de Risco de Segurança. (CCSDS, 2011).

De acordo com Carvalho (2015), quando se trata de Níveis de maturidade, a norma ISO 16363 não apresenta, de momento, qualquer indicação relativamente ao nível de conformidade que um repositório deve apresentar em relação a cada um dos requisitos normativos. De acordo com CCSDS (2011), um repositório ou cumpre ou não cumpre um requisito, cabendo ao auditor determinar se as evidências apresentadas pelo repositório são suficientes para assegurar o seu cumprimento.

Abaixo, apresenta-se, na Tabela 8 a estrutura típica de um critério do ACTDR.

TABELA 7 - Estrutura de um critério no ACTDR

Seção
Categoria
Critério
Subcritério - Nível 1
Subcritério - Nível 2
Texto de suporte
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse critério
Discussão

FONTE: CCSDS (2011, Tradução nossa). Adaptado pelo autor.

A título de exemplo, apresenta-se o Critério 4.2.4 do ACTDR, na Quadro 9.

QUADRO 9 - Critério 4.2.4 do ACTDR

Seção	**4 Gerenciamento Digital de Objetos**
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs.
Subcritério	4.2.4.2 O repositório deve ter um sistema de serviços confiáveis de vinculação / resolução para encontrar o objeto identificado exclusivamente, independentemente de sua localização física.
Texto de suporte	Isso é necessário para que as ações relacionadas aos AIPs possam ser rastreadas ao longo do tempo, nas alterações do sistema e nas alterações de armazenamento.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação que descreve a convenção de nomenclatura e evidência física de sua aplicação (por exemplo, logs).
Discussão	Um repositório precisa garantir que exista uma convenção de nomenclatura padrão aceita que identifique seus materiais de forma exclusiva e persistente para uso dentro e fora do repositório. O requisito de 'visibilidade' aqui significa 'visível' para gerentes e auditores de repositório. Isso não implica que esses identificadores exclusivos precisem estar visíveis para os usuários finais ou que sirvam como o principal meio de acesso a objetos digitais. Idealmente, o ID exclusivo permanece enquanto o AIP; caso contrário, deve haver rastreabilidade. Na subseção 4.2.1, exige-se que os componentes de um AIP sejam adequadamente vinculados e identificados para o gerenciamento a longo prazo, mas não impõe restrições sobre como os AIPs são identificados com os arquivos. Assim, no caso geral, um AIP pode ser distribuído por muitos arquivos ou um único arquivo pode conter mais de um AIP. Portanto, identificadores e nomes de arquivos podem não corresponder necessariamente um ao outro. A documentação deve representar esses relacionamentos.

FONTE: CCSDS (2011, Tradução nossa). Adaptado pelo autor.

A lista de verificação do ACTDR é dividida em três seções, sendo que cada seção corresponde a um Grupo de Critérios. Cada Grupo de Critérios apresenta uma quantidade de critérios constituintes, organizados conforme a Tabela 9:

TABELA 8 - Estrutura dos critérios ACTDR

Seções	**Grupos de Critérios**	**Quantidade de critérios**
A	Infraestrutura organizacional	24
B	Gerenciamento de objetos digitais	60
C	Tecnologias, infraestrutura técnica e segurança.	24

FONTE: CCSDS (2011). Adaptado pelo autor.

De acordo com ISO (PRIMARY TRUSTWORTHY DIGITAL REPOSITORY AUTHORISATION BODY - PTAB, 2020), a primeira organização no mundo a receber o credenciamento ISO 16363 para Repositórios Digitais Confiáveis foi o *Primary Trustworthy*

Digital Repository Authorisation Body Ltd (PTAB), sediado em Dorset, Reino Unido, no ano de 2017.

> O PTAB está agora listado no Registro de Órgãos de Certificação do Conselho Nacional de Acreditação para Órgãos de Certificação (NABCB) sob o número de registro TD 001, após o extenso processo de acreditação. Como resultado, o PTAB está autorizado a auditar repositórios digitais em todo o mundo e, quando apropriado, certificar que eles são confiáveis. Os membros da equipe internacional da PTAB, cada um deles reconhecido por sua experiência em preservação digital, são autores da ISO 16363 e muitos também da ISO 14721 (OAIS), a norma fundamental para a preservação digital[114]. (PTAB, 2020).

Abaixo, apresenta-se, na Tabela 10, as únicas instituições certificadas utilizando ISSO 16363, até maio de 2021.

TABELA 9 - Instituições certificadas com a ISO 16363 pelo PTAB

A seguir, na Tabela12, apresentam-se as Instituições certificadas com a ISO 16363 pelo PTAB, até dezembro de 2020:Instituição	Data de certificação
INDIRA GANDHI NATIONAL CENTRE FOR THE ARTS. New Delhi, India	2017
UNITED STATES GOVERNMENT PUBLISHING OFFICE. Washington - DC. USA	2018

FONTE: PTAB (2020).

Durante a realização desta pesquisa, não foram encontradas publicações que detalhem o processo de auditoria e certificação utilizando a lista de critérios ACTDR.

4.4.1 Modelos de maturidade para Repositórios Digitais

Em busca de um estudo de caso que pudesse guiar futuras ações de implementação, auditoria e certificação, esta pesquisa encontrou o trabalho *Auditoria ISO 16363 a Repositórios Institucionais*, em que o pesquisador José Carvalho, da Universidade do Minho, em Portugal, disserta sobre sua experiência de auditoria em repositórios digitais utilizando a ISO 16363:2012.

A pesquisa realizou o diagnóstico empregando a ferramenta de análise de maturidade *Enterprise Content Management Maturity* Model (ECM3), algo que não fora até

[114] Texto original*: PTAB is now listed in the Register of Certification Bodies of National Accreditation Board for Certification Bodies (NABCB) under registration number TD 001 after the extensive accreditation process. As a result, PTAB is authorized to audit digital repositories worldwide and, when appropriate, certify that they are trustworthy. The PTAB international team members, each recognized for their expertise in digital preservation, authored ISO 16363 and many also authored ISO 14721 (OAIS), the fundamental standard for digital preservation.*

então comentado na literatura pesquisada no contexto brasileiro sobre auditoria e certificação de Repositórios Digitais.

Segundo Carvalho (2015), a norma ISO 16363:2012 não apresenta qualquer indicação relativa ao nível de conformidade que um repositório deve apresentar em relação a cada um dos requisitos normativos. Para a ISO 16363, um repositório ou cumpre ou não cumpre um dado requisito, cabendo ao auditor determinar se as evidências apresentadas pelo repositório são suficientes para assegurar o seu cumprimento.

O TRAC, publicação normativa que sucedeu à ISO 16363, também não faz menção à configuração de níveis de maturidade para seus critérios. Nesse ínterim, Carvalho (2015) relata que, para facilitar a realização do diagnóstico de conformidade, foi necessário adotar uma Escala de Maturidade que permitisse à equipe auditora identificar o nível de conformidade de cada repositório em relação do referencial normativo adotado e, com base nessa maturidade, elaborar um Plano de Ações de melhoria específico para cada repositório.

Um Modelo de Maturidade é, de acordo com Katuu (2013), uma ferramenta organizacional utilizada para desenvolver capacidades que tornam uma organização mais eficaz. Portanto, esses modelos buscam operacionalizar os fatores, habilidades e práticas que se acredita conduzirem a um sucesso nos negócios.

É uma coleção estruturada de elementos que descrevem características de processos eficazes e proporciona um lugar para começar, o benefício da experiência anterior, uma linguagem comum, uma estrutura para priorizar ações e uma forma para definir melhorias. Os modelos de maturidade são desenvolvidos com base nas organizações que não vão da capacidade zero para a capacidade ótima instantaneamente, mas com um progresso, ao longo de uma jornada de maturidade.

O Modelo de Maturidade ECM3 foi desenvolvido, segundo Katuu (2013), como um modelo aberto de fontes por indivíduos de uma série de empresas consultorias e que também servem como equipe de coordenação para a continuidade do desenvolvimento. O modelo é visto como uma estrutura para organizar os esforços das organizações para obter benefícios comerciais do ECM, bem como para manter a atenção do programa às partes interessadas. O modelo é capaz de fazer isso, porque pode ser aplicado para auditar, avaliar e explicar o estado atual dentro de uma organização, bem como fornecer um roteiro para o amadurecimento da capacidade de organização.

Entretanto, embora Carvalho (2015) tenha utilizado o ECM3 para auditar o Nível de Maturidade de repositórios digitais, Katuu (2013) esclarece que:

> O ECM3 foi projetado para avaliar os registros digitais dentro das aplicações ECM e, na maioria das vezes, estas aplicações não são projetadas a

> preservação de longo prazo. Isto porque as aplicações de preservação digital e as aplicações de ECM adeririam, em teoria, a diferentes requisitos funcionais. Para aplicações ECM, estes requisitos funcionais foram determinados principalmente dentro de jurisdições nacionais como a Austrália e os Estados Unidos. Além disso, existem diretrizes de ECM da União Européia e esforços para um conjunto global básico e genérico de requisitos funcionais pelo Conselho Internacional de Arquivos. Por outro lado, as aplicações de preservação digital, em sua maioria, aderem ao modelo de referência OAIS. Portanto, é prudente não esperar que as aplicações de ECM forneçam funcionalidade de preservação digital (KATUU, 2013, p. 5).

Um modelo mais apropriado, revela Katuu (2013), é um modelo que foi desenvolvido por Charles Dollar e por Lori Ashley e se intitula *Digital Preservation Capability Maturity Model* (DPCMM). O principal objetivo dessa ferramenta é ajudar os profissionais a identificarem, em um alto nível, as capacidades de sua organização em relação às capacidades ideais de preservação digital, a fim de traçar a evolução de gerenciamento desorganizado e indisciplinado de registros digitais para estágios cada vez mais maduros de capacidade de preservação digital.

4.4.2 Digital Preservation Capability Maturity Model (DPCMM)

O objetivo do DPCMM é, segundo Ashlley e Dollar (2015), fornecer aos profissionais um modelo de processo integrado e uma ferramenta de planejamento de casos comerciais para ajudar na avaliação comparativa e na melhoria das capacidades de preservação digital.

O DPCMM baseia-se nas funções e serviços de preservação identificados na ISO 14721, o Modelo de Referência de Sistemas de Informação de Arquivo Aberto (OAIS), bem como nos atributos especificados na ISO 16363, Auditoria e certificação de repositórios digitais de confiança (TDRs). Foi desenvolvido para analisar lacunas das atuais capacidades de preservação digital e para ajudar os profissionais e organizações a delinear um roteiro plurianual de melhorias a serem incrementadas.

O DPCMM é uma ferramenta flexível que pode ser adaptada aos requisitos e recursos específicos de qualquer organização, e tem em conta uma série de modelos de repositório potenciais e estratégias de implementação. A DPCMM identifica os principais requisitos de preservação digital que constituem a base para o debate e diálogo sobre o estado futuro desejado das capacidades de preservação digital e o nível de risco que a sua liderança está disposta a assumir no que diz respeito à proteção e acesso aos seus documentos oriundos de arquivos correntes e intermediários eletrônicos em longo prazo. (ASHLLEY; DOLLAR, 2015).

As principais normas internacionais que figuram de forma proeminente no DPCMM são:

a) ISO 14721 - *Space data and information transfer systems - Open archival information systems - Reference model*[115];
b) ISO 16363 - Space data and information transfer systems - Audit and certification of trustworthy digital repositories[116].

O DPCMM é baseado nas funções OAIS e em critérios de auditoria de repositório confiáveis (ISO 16363) que, quando combinados com as boas práticas aceitas pela comunidade, estabelecem um alto limite para as capacidades de preservação digital. As estratégias de preservação incluem a criação de objetos digitais "prontos para preservação", no momento da captura ou do recebimento, ou próximo ao momento da captura ou do recebimento, sempre que possível. O documento revisa, ainda, os metadados necessários como prova da precisão, integridade e confiabilidade dos Pacotes de Submissão de Informação, Pacotes de Arquivamento de Informaçãoe Pacotes de Disseminação de Informação. (ASHLLEY; DOLLAR, 2015).

4.4.3 Visão geral do Modelo de Maturidade de Capacidade de Preservação Digital

> A idéia de um *Capability Maturity Model*[117] (CMM) foi desenvolvida pelo Instituto de Engenharia de Software da Universidade Carnegie Mellon e utilizado na engenharia de software comercial nos anos 1990. Essencialmente CMM é uma ferramenta que ajuda as organizações a medir a maturidade de seu processo de desenvolvimento de software. A CMM coloca um esquema de pontuação simples a um tópico relativamente complexo e fornece um conjunto claro de passos para alcançar melhorias e desempenho sustentável ao longo do tempo. (PRESERVICA, 2015, p. 4).

Um Modelo de Maturidade da Capacidade (CMM) é, de acordo com Ashlley e Dollar (2015, p. 8). “um conjunto de níveis estruturados que descreve como as práticas, processos e comportamento de uma organização podem ser confiáveis e produzir de forma sustentável os resultados desejados.” O CMM identifica uma série de atividades associadas e métricas de base utilizadas para medir o desempenho em uma determinada área. Os estágios de maturidade são cumulativos: uma organização que atinge um estágio de

---

115 Dados espaciais e sistemas de transferência de informações - Sistemas de informação de arquivos abertos - Modelo de referência. Tradução do autor.
116 Sistemas de transferência de dados e informações espaciais - Auditoria e certificação de repositórios digitais confiáveis. Tradução do autor.
117 Modelo de maturidade da capacidade. Tradução do autor.

maturidade mais elevado deve implementar e sustentar todos os requisitos para aquele estágio, além dos requisitos para todos os estágios inferiores

O objetivo do DPCMM é ajudar os profissionais e suas respectivas organizações e repositórios de preservação a:

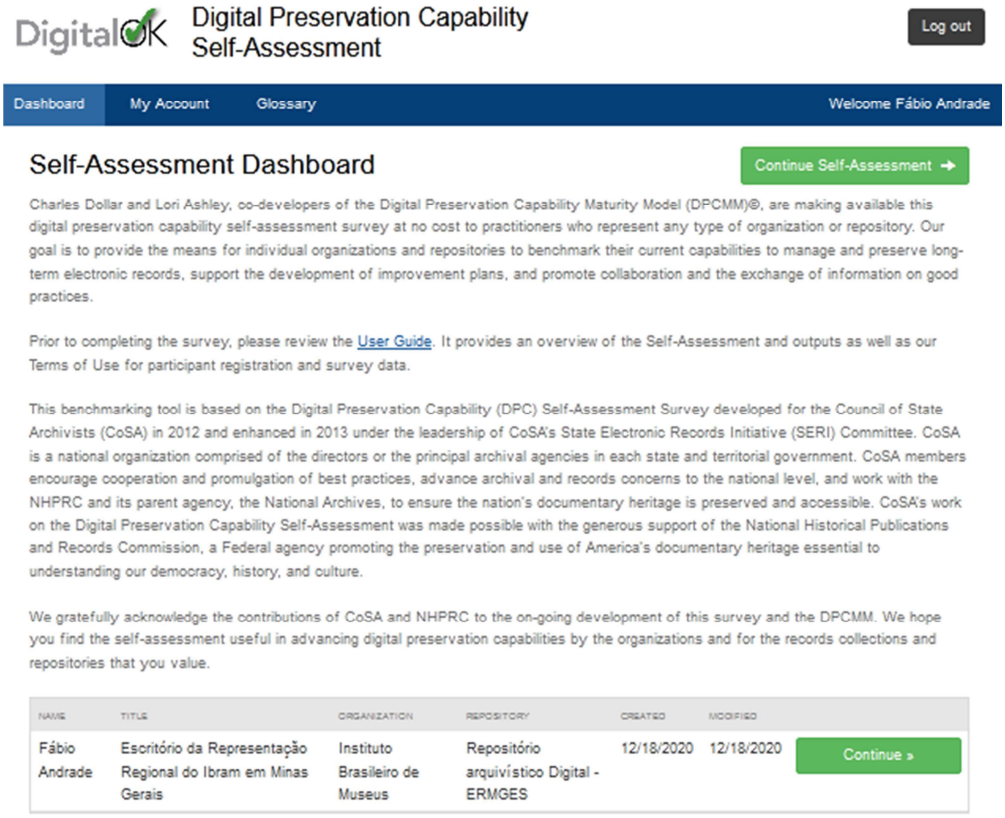
> - identificar em um alto nível onde um programa de gerenciamento de registros eletrônicos está em relação à capacidade ótima de preservação digital;
>
> - relatar lacunas nos níveis de capacidade e métricas de desempenho de preservação para educar e envolver os alocadores de recursos e outras partes interessadas; e
>
> - estabelecer prioridades para alcançar capacidades baseadas em padrões para preservar e garantir o acesso a registros eletrônicos de longo prazo. (ASHLLEY; DOLLAR, 2015, p. 8, Tradução nossa).

DPCMM é um *continuum* de maturidade de cinco níveis. Ele se baseia nas especificações funcionais da ISO 14721, nos critérios de auditoria e certificação do TRAC e da ISO 16363, e nas melhores práticas aceitas em repositórios operacionais de preservação digital. DPCMM é uma ferramenta baseada em sistemas para traçar um caminho evolutivo do gerenciamento desorganizado e indisciplinado de registros eletrônicos, ou da falta de uma abordagem sistemática de continuidade digital, para estágios cada vez mais maduros da capacidade de preservação digital. (ASHLLEY; DOLLAR, 2015).

No Apêndice E, apresenta-se uma versão traduzida do DPCMM*,* elaborada pelo autor, no decorrer desta pesquisa, para subsidiar possíveis ações de auditoria e certificação no RDC-Arq.

Ashley e Dollar (2015), desenvolvedores do Modelo de Maturidade de Capacidade de Preservação Digital (DPCMM), disponibilizaram uma pesquisa de autoavaliação de capacidade de preservação digital sem custo para os profissionais que representam qualquer tipo de organização ou repositório. O objetivo, segundo os autores, é fornecer os meios para que organizações individuais e repositórios possam comparar suas capacidades atuais para gerenciar e preservar registros eletrônicos de longo prazo, apoiar o desenvolvimento de planos de melhoria e promover a colaboração e a troca de informações sobre boas práticas. Abaixo, apresenta-se, na Figura 16, a imagem da ferramenta *Digital Preservation Capability Self-Assessment,* disponibilizado *on-line.*

FIGURA 16 - Digital Preservation Capability Self-Assessment

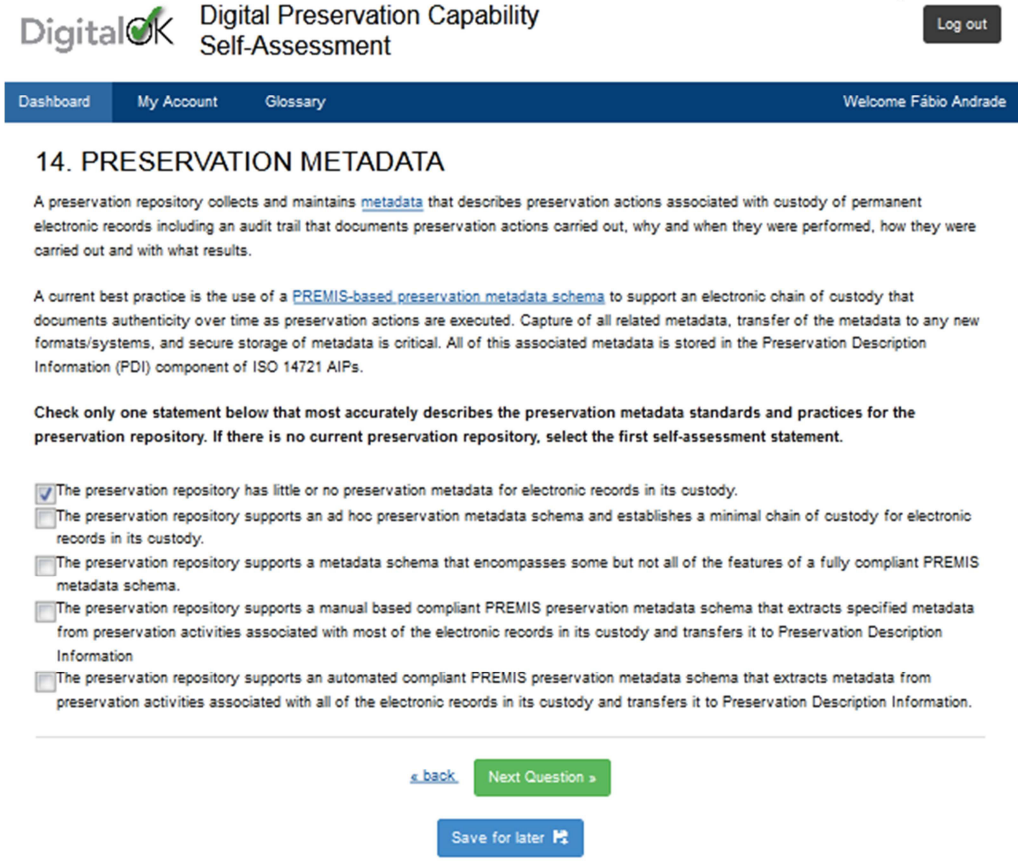


FONTE: Ashley e Dollar (2020).

Os autores disponibilizam um Guia do Usuário que se destina a ser usado em conjunto com a Ferramenta Autoavaliação da Capacidade de Preservação Digital (DPC). O documento fornece uma visão geral da pesquisa de autoavaliação do DPC e uma descrição de como utilizá-lo para produzir uma "pontuação" do estado atual capacidade de preservação digital de uma organização.

> Nosso objetivo é fornecer os meios para organizações individuais e para avaliar suas capacidades atuais de gerenciamento e preservação de registros eletrônicos por longos períodos, apoiar o desenvolvimento de planos de melhoria, e promover a colaboração e o intercâmbio de informações sobre boas práticas. O DPCMM se baseia em funções e serviços de preservação identificados na ISO 14721, o modelo de referência de Sistemas de Informação de Arquivo Aberto (OAIS), assim como os atributos especificados na ISO 16363, Auditoria e Certificação de Repositórios Confiáveis. (ASHLEY; DOLLAR, 2015).

FIGURA 17 - Ferramenta Auto Avaliação da Capacidade de Preservação Digital (DPC)

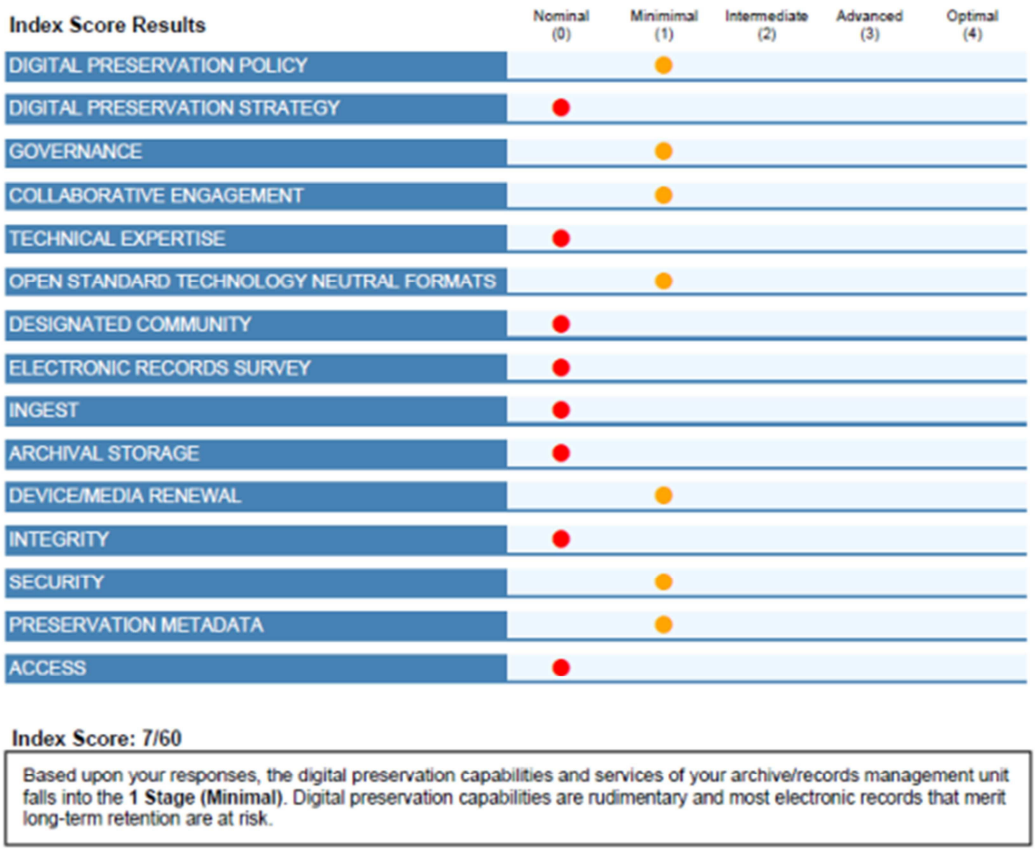


FONTE: Ashley e Dollar (2020).

A Ferramenta Auto Avaliação da Capacidade de Preservação Digital disponibiliza, em sua interface ao usuário, um ambiente denominado “Caixa-de-Areia”, onde é possível ter contato com formulários avaliativos e explicações sobre cada componente de relevância para a compreensão do critério, por parte do avaliador.

A autoavaliação da capacidade de preservação digital calcula um Índice de Pontuação (Figura 18) que se baseia em suas respostas para as declarações e a pesquisa lógica de pontuação. Esse índice de pontuação classifica as capacidades de preservação da organização e do repositório em relação ao cumprimento das capacidades mais elevadas de preservação digital associadas com as especificações da ISO 14721 e ISO 16363. (ASHLEY; DOLLAR, 2015).

FIGURA 18 - Resultados do Índice de Pontuação



FONTE: Ashley e Dollar (2020).

A FIGURA 19 - Resultados do Índice de Pontuação favorece aos avaliadores o entendimento ampliado da situação de capacidade de preservação digital quanto a cada um índices investigados, de forma que pode orientar onde serão mais necessários os esforços da equipe responsável pelo repositório digital.

5 METODOLOGIA

Para atender ao Objetivo Específico letra A: Analisar os critérios do Catalogue of Criteria for Trusted Digital Repositories (NESTOR), do Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) e Audit and Certification of Trustworthy Digital Repositories (ACTDR), comparando-os com os requisitos das Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq), observando as semelhanças e diferenças quanto aos agentes das ações de preservação, quanto às ações de preservação e quanto aos objetos digitais alvo dessas ações de preservação, elencadas em cada requisito; , serão analisados, por meio do Método Comparativo, as Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq), *Catalogue of Criteria for Trusted Digital* (NESTOR)*, o Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC) *e Audit and Certification of Trustworthy Digital Repositories (ACTDR)* por meio de quadros comparativos. Tais quadros proporcionarão a análise dos grupos de requisitos que apresentam funções afins. O intuito dessa análise é verificar as semelhanças e diferenças entre os requisitos dos três modelos. De acordo com Fachin (2005), o Método Comparativo consiste em investigar *coisas* ou fatos e explicá-los segundo suas semelhanças e suas diferenças. Ainda, segundo Fachin (2005), o método comparativo aborda, geralmente, duas séries ou fatos de natureza análoga, tornados de meios sociais ou de outra e área do saber, a fim de se detectar o que é comum a ambos.

Partindo da experiência propiciada pelos trabalhos publicados por Corujo (2014) e por Zazo e Lorenzo-Cáceres (2017) que se utilizaram de análise comparativa voltada para os aspectos da estrutura organizacional, gestão do objeto digital e infraestrutura técnica e segurança dos modelos TRAC, NESTOR e ACTDR/ ISO 16.363:2012, a presente pesquisa introduziu o RDC-Arq em um quadro comparativo que investigou a similaridade conceitual dos conjuntos de requisitos dos modelos internacionais supracitados. Os requisitos foram separados em três partes distintas, próximas de uma análise síntática, em que o sujeito da frase equivale, em tese, ao agente da ação de preservação, o verbo equivale à ação de preservação, e o objeto, seja direto ou indireto, contido no predicado, se equipara ao alvo ou objeto da ação de preservação elencada no requisito. A utilização de tal artifício justifica-se pelo fato de que a realização de uma análise sintática em cada requisito não proporcionaria a possibilidade de repetição exata da experiência, por outros pesquisadores, segundo prevê o Método Científico. Uma vez que se trata de uma comparação de traduções, em que o caráter subjetivo do tradutor pode comprometer a repetibilidade, a verificação e a organização sistemática das idéias provenientes dos textos produzidos, buscou-se caracterizar não o sujeito, mas sim, o agente que é o autor da ação de preservação. Da

mesma forma, não se comparou o verbo e sim o elemento motriz, caracterizado pela ação de preservação. De forma semelhante, não se classificou o objeto direto, indireto ou outros elementos do predicado, mas sim, o alvo ou objeto da ação de preservação.

Tal divisão busca tornar a comparação conceitual dos constituintes internos dos requisitos, uma vez que os requisitos são frutos de traduções textualmente diversas.

Os quatro modelos de requisitos estão organizados, cada um, em três seções de requisitos semelhantes, conforme se exemplifica, na Tabela 11:

TABELA 10 - Estrutura dos Modelos de Requisitos RDC-Arq, NESTOR, TRAC e ACTDR

Modelos de Requisitos	RDC-Arq	NESTOR	TRAC	ACTDR
Seção - A	II.2.1 Infraestrutura organizacional	A. Estrutura organizacional	A. Estrutura organizacional	3 Infraestrutura Organizacional
Seção - B	II.2.2 Gerenciamento do documento digital	B. Gerenciamento de Objetos	B. Gerenciamento de objetos digitais	4 Gerenciamento Digital de Objetos
Seção - C	II.2.3 Tecnologia, infraestrutura técnica e segurança	C. Infraestrutura e Segurança	C. Tecnologias, infraestrutura técnica e segurança.	5 Gestão de Riscos de Infraestrutura e Segurança

FONTE: Desenvolvido pelo autor.

Conforme pode ser observado, na Tabela 11, os quatro modelos de requisitos apresentam-se organizados, estruturalmente, de forma semelhante, no que se refere às funções que cada Seção de requisitos desempenha. Assim, tem-se, por hipótese, que tais Seções de requisitos, organizadas, de acordo com suas funções, podem ser comparadas entre si.

Pretende-se uma tabela para cada comparação, tendo por base os requisitos do RDC-arq. Serão analisadas as Seções, os Grupos e os Requisitos dos três modelos internacionais investigados (Lista de verificação TRAC, Catálogo de critérios NESTOR e Lista de Critérios ACTDR), de forma a agrupá-los, baseando-se em sua similaridade conceitual. Intenciona-se, assim, demonstrar-se, qualitativamente, a compatibilidade entre os modelos de requisitos, uma vez que todos se proclamam compatíveis com o Modelo de Referência OAIS.

A análise dos requisitos será realizada da seguinte maneira:

1 - Será realizada a tradução dos modelos de critérios internacionais NESTOR, TRAC e ACTDR adotando, como ferramenta de auxílio, o Tradutor Deepl. A DeepL é uma empresa alemã que tem por objetivo de eliminar barreiras lingüísticas em todo o mundo, utilizando inteligência artificial (DEEPL, 2020).

> Desde 2017, ela oferece DeepL Tradutor em www.DeepL.com, uma máquina sistema de tradução que, de acordo com testes cegos, consegue a melhor tradução qualidade em todo o mundo. Ela também fornece produtos profissionais para empresas, negócios pessoas, e tradutores. Até agora, mais de um bilhão de pessoas já usaram o DeepL's serviços.
>
> A excepcional qualidade da tradução automática da DeepL é o resultado de melhorias nos serviços proprietários que a equipe fez na matemática e na metodologia das redes neurais[118]. (DEEPL, 2020).

2 - Será efetuada a análise do requisito/ critério, no intuito de identificarem-se o Agente da ação de preservação, Ação de preservação, e Objeto da ação de preservação.

3 - Comparação: Nesse campo, serão analisados os elementos comparados (Agente da ação de preservação, Ação de preservação, e Objeto da ação de preservação), justificando o Resultado.

4 - Os resultados das comparações receberão três classificações:

- Similares;
- ISimilaridade parcial;
- Sem correspondências similares.

Salienta-se que os Modelos de Critérios são, todos eles, compatíveis com o Modelo de Referência OAIS.

No Quadro 10, apresenta-se o dispositivo a ser adotado para a efetivação da comparação.

QUADRO 10 - Comparação entre o RDC-Arq e modelos de requisitos internacionais

Modelos de Requisitos	RDC-Arq	Modelos de requisitos internacionais
Seção		
Grupo		
Requisitos em análise		
Agente da ação de preservação		
Ação de preservação		
Objeto da ação de preservação		
Comparação		
Resultado		

FONTE: Desenvolvido pelo autor.

[118] Texto original: *DeepL is a German company that has set itself the goal of eliminating language barriers worldwide by using artificial intelligence. Since 2017, it has offered DeepL Translator on www.DeepL.com, a machine translation system that, according to blind tests, achieves the best translation quality worldwide. It also provides professional products for companies, business people, and translators. So far, more than one billion people have used DeepL's services. The exceptional quality of DeepL's machine translation is the result of proprietary improvements the team has made in the mathematics and methodology of neural networks.*

Para atingir o Objetivo Específico letra B: Elaborar um modelo conceitual híbrido, fruto das análises dos três modelos de requisitos supracitados, de forma a propor um formulário para autoavaliação de repositórios arquivísticos digitais confiáveis, adaptado ao contexto brasileiro e que possa subsidiar futuras atualizações do RDC-Arq serão utilizadas as informações levantadas junto às comparações entre os modelos internacionais e o RDC-Arq, com o objetivo de construir um modelo conceitual híbrido forma a propor um formulário para autoavaliação de repositórios arquivísticos digitais confiáveis, adaptado ao contexto brasileiro e que possa subsidiar futuras atualizações do RDC-Arq;

Para satisfazer o Objetivo Específico letra C: Investigar como proceder a transmissão do Pacote de Submissão de informação ao RDC-Arq, observando o disposto no Decreto nº 10.278/2020 e, simultaneamente, apoiando-se nas experiências internacionais de instituições voltadas para a preservação digital, por longos períodos, objetivando a proposição de procedimentos técnicos apropriados à preservação arquivística digital no contexto brasileiro.será realizado um levantamento bibliográfico investigativo em publicações internacionais voltadas para a preservação digital em longo prazo sobre procedimentos para efetuar o envio de Pacotes de Submissão de Informação (SIP) a repositórios digitais confiáveis, observando do Decreto nº 10.278/2020, com o intuito de propor procedimentos técnicos apropriados à preservação arquivística digital, por longos períodos no contexto brasileiro.

6 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

No presente capítulo, apresentar-se-ão os resultados das investigações e levantamentos realizados, como forma de subsidiar as conclusões no capítulo posterior.

6.1 ANÁLISE SOBRE A COMPARAÇÃO ENTRE OS REQUISITOS DO RDC-ARQ E DO TRAC

Durante esta pesquisa, efetuou-se uma análise comparativa qualitativa e quantitativa entre os requisitos para a implementação de repositórios digitais confiáveis, de autoria do Conselho Nacional de arquivos, e os critérios do *Trustworthy Repositories Audit & Certification: Criteria and Checklist* - TRAC.

Abaixo, apresenta-se o Quadro 11, que traz a comparação entre os requisitos do RDC-Arq e os critérios do TRAC.

QUADRO 11 - Comparação entre os requisitos do RDC-Arq e os critérios do TRAC

RDC-Arq		**Critérios de auditoria e certificação - TRAC**		**Comparação**
Seção	Grupo	Seção	Grupo	
II.2.1 - Infraestrutura organizacional	a.	**A. Infraestrutura Organizacional**	A1.	Similares
	b.		A2.	Similares
	c.		A3.	O RDC-Arq não apresentou requisito correspondente ao critério A.3.7 do Manual TRAC. Os demais requisitos e critérios são Similares
	d.		A4.	O RDC-Arq não apresentou requisito correspondente para o critério A.4.5 do Manual TRAC. Os demais requisitos e critérios são Similares
	e.		A5.	Similares
II.2.2 – Gerenciamento do documento digital	a.	**B. Gestão de Objetos Digitais**	B1.	Similares
	b.		B2.	Similares
	c.		B3.	Similares
	d.		B4.	Similares
	e.		B5.	Similares
	f.		B6.	Similares
			B6.	Similares
II.2.3 – Tecnologia, infraestrutura técnica e segurança	a.	**C. Tecnologias, Infraestruturas Técnicas, e Segurança**	C1.	O RDC-Arq não apresentou requisito correspondente para o critério C1.10 do Manual TRAC. Os demais requisitos e critérios são similares.
	b.		C2.	Similares
	c.		C3.	Similares

FONTE: Desenvolvido pelo autor.

A comparação foi efetivada com base em sua similaridade conceitual, após análise do agente da ação de preservação, da ação de preservação e do objeto da ação de preservação entre os requisitos, identificados e destacados nos campos do quadro de análise e comparação.

Construiu-se uma tabela com os seguintes dados:

1- Quantidade total de requisitos / critérios total do RDC-Arq e do TRAC;

2- Quantidade de requisitos do RDC-Arq que desempenham ações de preservação similares quando comparados aos critérios do TRAC.

3 - Quantidade de requisitos do RDC-Arq que desempenham ações de preservação parcialmente similares quando comparados aos critérios do TRAC.

4- Quantidade de critérios do TRAC que não encontraram ações de preservação semelhantes entre os requisitos do RDC-Arq.

A fim de tornar os procedimentos de comparação mais transparentes e acessíveis, disponibilizamos o Apêndice H que traz o quadro completo de comparação entre os dois modelos supracitados.

QUADRO 12 - Resultado da comparação RDC-Arq e do TRAC

Modelo de requisitos/ critérios	RDC-Arq	TRAC
1- Quantidade total de requisitos / critérios	74	84
2- Quantidade de requisitos do RDC-Arq que desempenham ações de preservação similares quando comparados aos critérios do TRAC.	66	
3- Quantidade de requisitos do RDC-Arq que desempenham ações de preservação parcialmente similares quando comparados aos critérios do TRAC.	8	
4- Quantidade de critérios do TRAC que não encontraram ações de preservação semelhantes entre os requisitos do RDC-Arq.	4	

FONTE: Desenvolvido pelo autor.

Verificou-se que há grande similaridade conceitual entre os requisitos do RDC-Arq e os critérios do TRAC. Ou seja, esta pesquisa averiguou que todos os requisitos elencados no RDC-Arq estão integralmente contidos nos critérios do TRAC, mas que nem todos os requisitos do TRAC estão contidos no RDC-Arq.

Ainda assim, não significa que o RDC-Arq tenha simplesmente, adotado os conceitos dos critérios TRAC, sem alterá-los. Pelo contrário, verifica-se que o RDC-Arq adaptou vários critérios do TRAC ao contexto arquivístico, uma vez que os critérios TRAC foram desenvolvidos para repositórios digitais diversos, como bibliotecas, museus, bancos

de dados, entre outros. O RDC-Arq adequa, por assim dizer, os conceitos do TRAC ao contexto arquivístico, com suas peculiaridades intrínsecas.

Apesar do TRAC possuir dez critérios a mais que o RDC-Arq, essa diferença explica-se pelo fato do RDC-Arq mesclar, em vários casos, requisitos que equivalem a dois ou mais critérios do TRAC. Ainda assim, os requisitos propostos no RDC-Arq permanecem similares aos critérios equivalentes no TRAC.

Constatou-se, entretanto, que o RDC-Arq não adotou a totalidade dos critérios do TRAC. Abaixo, são apresentados os critérios do TRAC que não apresentam requisitos conceitualmente similares entre os requisitos do RDC-Arq. Esta pesquisa os concentrou no Quadro 13, a fim de analisá-los e tecer possíveis melhorias ao RDC-Arq, advindas desta análise.

QUADRO 13 - Requisitos TRAC que não apresentaram similaridade conceitual aos requisitos do RDC-Arq

Critérios de auditoria e certificação - TRAC
A. Infraestrutura Organizacional
A1. Governança e viabilidade organizacional
A3.7 O Repositório compromete-se a garantir a transparência e a responsabilidade em todas as ações de apoio à operação e gestão do repositório, especialmente às que afetam a preservação de conteúdos digitais ao longo do tempo.
A4.5 O Repositório compromete-se a acompanhar e a fazer pontes entre as lacunas de financiamento.
B. Gestão de Objetos Digitais
B6. Gerenciamento de acesso
B6.5 Sistema de gerenciamento de acesso ao repositório implementa integralmente a política de acesso.
C. Tecnologias, Infraestruturas Técnicas, & Segurança
C1. Infraestrutura do sistema
C1.10 O Repositório tem um processo para reagir à disponibilidade de novas atualizações de segurança de software com base numa avaliação de risco-benefício.

FONTE: Desenvolvido pelo autor.

Contribuições para o RDC-Arq

- Os requisitos do RDC-Arq poderiam receber notações (letras ou números) para facilitar sua identificação e localização.

- Acréscimo do campo “Evidências” na estrutura conceitual de cada requisito, com o objetivo de documentar e referenciar material levantado durante o processo de auditoria/ certificação.

- O Formulário de *checklist* do TRAC,apresentado no Quadro 14, é uma excelente ferramenta que poderia ser acrescentada ao RDC-Arq, com as necessárias adaptações pontuais.

QUADRO 14 - Trustworthy Repositories Audit & Certification: Criteria Checklist

Trustworthy Repositories Audit & Certification: Criteria Checklist					
Organização		**Auditor**		**Página**	
Seção		**Entrevistados**		**Data**	
Aspecto					
Critério	**Evidências Examinadas**		**Descobertas e observações**		**Resultado**

FONTE: OCLC (2007).

- Os requisitos do RDC-Arq, em alguns casos, poderiam ser divididos em dois ou mais requisitos, de forma a facilitar os processos de verificação de conformidade de requisitos, durante procedimentos de certificação, auditoria e implementação.

Segue, abaixo, a sugestão de divisão, no Quadro 15:

QUADRO 15 - Requisitos do RDC-Arq que poderiam ser divididos para equivalerem ao à Lista de Verificação TRAC

Modelo	**RDC-Arq**	**Sugestão**
Seção	**II.2.1 - Infraestrutura organizacional**	
Grupo	**a. Governança e viabilidade organizacional**	
Requisitos	a.1	Dividir em dois requisitos distintos
Grupo	**b. Estrutura organizacional e de pessoal**	
Requisitos	b.1	Dividir em três requisitos distintos
Grupo	**e. Contratos, licenças e passivos**	
Requisito	e.1	Dividir em cinco requisitos distintos
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	
Grupo	**f. Gerenciamento de acesso**	
Requisitos	f.4	Dividir em dois requisitos distintos

FONTE: Desenvolvido pelo autor.

Como pode ser observado no QUADRO 16, sugere-se dividir alguns dos requisitos do RDC-arq com o intuito de equipará-lo à estrutura originalmente apresentada pelo TRAC, de forma a propiciar a utilização da metodologia de auditoria e certificação desenvolvida por OCLC(2007).

QUADRO 16 - Comparação entre os requisitos RDC-Arq e Critérios TRAC para fins de adequação para a utilização da Ferramenta Drupal TRAC Review

Modelo	RDC-Arq		Critérios de auditoria e certificação - TRAC
Seção	II.2.1 - Infraestrutura organizacional		A. Infraestrutura Organizacional
Grupo	A. Governança e viabilidade organizacional		A1. Governança e viabilidade organizacional
Requisito	A1.1	Dividir A1.1 em dois requisitos	A1.1
			A1.2
Grupo	b. Estrutura organizacional e de pessoal		A2. Estrutura organizacional e pessoal
Requisito	B1.1	Dividir B1.1 em três requisitos	A2.1
			A2.2
			A2.3
Grupo	C. Transparência de procedimentos e arcabouço político		A3. Responsabilidade processual e enquadramento político
Requisito	C1.1	Ambos equivalem ao critério A3.1	A3.1
Requisito	C1.2		
Requisito	Sem correspondente similar no RDC-Arq		A3.7
Requisito	C1.9	Ambos equivalem ao critério A3.9	A3.9
Requisito	C1.10		
Grupo	d. Sustentabilidade financeira		A4. Sustentabilidade financeira
Requisito	Sem correspondente similar no RDC-Arq		A4.5
Seção	II.2.2 – Gerenciamento do documento digital		B. Gestão de Objetos Digitais
Grupo	**f. Gerenciamento de acesso**		**B6. Gerenciamento de acesso**
Requisito	Sem correspondente similar no RDC-Arq		B6.5 Sistema de gerenciamento de acesso ao repositório implementa integralmente a política de acesso.
Grupo	f. Gerenciamento de acesso		B6. Gerenciamento de acesso
Requisito	F2.4	Dividir F2.4 em dois requisitos	B6.4
			B6.5
Seção	II.2.3 – Tecnologia, infraestrutura técnica e segurança		C. Tecnologias, Infraestruturas Técnicas, e Segurança
Grupo	a. Infraestrutura de sistema		C1. Infraestrutura do sistema
Requisito	Sem correspondente similar no RDC-Arq		C1.10
Grupo	b. Tecnologias apropriadas		C2. Tecnologias adequadas
Requisito	B3.1	Dividir B3.1em dois requisitos	C2.1
			C2.2

FONTE: Desenvolvido pelo autor.

Diante das informações levantadas nesta pesquisa, concluiu-se que não será necessário propor um formulário para autoavaliação, auditoria e certificação voltada para RDC-Arqs, uma vez que, o RDC-Arq apresenta-se, conceitualmente, muito próximo da lista de TRAC. Dessa forma, após realizar a tradução da Lista de Verificação TRAC e compará-la aos requisitos do RDC-Arq, concluiu-se que pode ser utilizada a ferramenta *DRUPAL TRAC Review* em conjunto com os requisitos do RDC-Arq, tendo em mente que devem ser observados os critérios e requisitos acima destacados e reestrutudados conforme o Quadro 16.

Importante frisar que não devem ser considerados os critérios TRAC sem correspondentes conceituais similares no RDC-Arq, apresentados no Quadro 17, nessa proposição de utilização do da metodologia TRAC de autoavaliação, auditoria e certificação.

6.2 ANÁLISE SOBRE A COMPARAÇÃO ENTRE OS REQUISITOS DO RDC-ARQ E O *CATALOGUE OF CRITERIA FOR TRUSTED DIGITAL REPOSITORIES* - NESTOR

Durante esta pesquisa, efetuou-se uma análise comparativa qualitativa e quantitativa entre os requisitos para implementação de repositórios digitais confiáveis, de autoria do Conselho Nacional de arquivos, e os critérios do *Catalogue of criteria for trusted digital repositories* - NESTOR.

Abaixo, segue o Quadro 17 apresentando o resumo da análise efetuada.

QUADRO 17 - Comparação entre os Requisitos do RDC-Arq e Critérios NESTOR

(Continua)

RDC-Arq		Catalogue of criteria for trusted digital repositories NESTOR		Comparação
Seção	**Grupo**	**Seção**	**Requisitos**	
II.2.1 - Infraestrutura organizacional	**a. Governança e viabilidade organizacional**	**A. Infraestrutura Organizacional**		
	a1.		1.2 e 4.6	Similares
	b. Estrutura organizacional e de pessoal			
	b1.		4.3, 5.1 e 4.2	Similares
	c. Transparência de procedimentos e arcabouço político			
	c1		1.3	Similares
	c2.		-	Sem correspondências similares
	c3.		1.1	Similares
	c4.		-	Sem correspondências similares
	c5.		-	Sem correspondências similares
	c6.		-	Sem correspondências similares
	c7.		-	Sem correspondências similares
	c8.		-	Sem correspondências similares
	c9.		-	Sem correspondências similares
	c10.		-	Sem correspondências similares
	d. Sustentabilidade financeira			
	d1.		4.1	Similares
	d2.		-	Sem correspondências similares
	d3.		-	Sem correspondências Similares
	d4.		-	Sem correspondências similares
	e. Contratos, licenças e passivos		3.1, 3.2 e 12.6	Similares

QUADRO 17 - Comparação entre os Requisitos do RDC-Arq e Critérios NESTOR

(Continuação)

RDC-Arq		Catalogue of criteria for trusted digital repositories NESTOR		Comparação
Seção	**Grupo**	**Seção**	**Requisitos**	
II.2.2 – Gerenciamento do documento digital	**a. Admissão: captura de documentos digitais**	**B. Gestão de Objetos Digitais**		
	a.1		9.2.	Similares
	a.2		9.1	Similares
	a.3		7.1	Similares
	a.4		6.1	Similares
	a.5		9.3	Similares
	a.6		-	Sem correspondências similares
	a.7		1.1	Similares
	a.8		-	Sem correspondências similares
II.2.2 – Gerenciamento do documento digital	**b. Admissão: criação do pacote de arquivamento**	**B. Gestão de Objetos Digitais**		
	b.1		10.1	Similares
	b.2		10.1	Similares
	b.3		10.2	Similares
	b.4		-	Sem correspondências similares
	b.5		12.1	Similares
	b.6		-	ISem correspondências similares
	b.7		-	ISem correspondências similares
	b.8		12.3 e 12.5	Similares
	b.9		12.4 e 12.6	Similares
	b.10		2.2	Similares
	b.11		-	ISem correspondências similares
	b.12		6.1	Similares
	b.13		-	ISem correspondências similares
	c. Planejamento da preservação			
	c.1		8 e 4.4	Similares
	c.2		-	ISem correspondências similares
	c.3		4.5.	Similares
	c.4		-	ISem correspondências similares

QUADRO 17 - Comparação entre os Requisitos do RDC-Arq e Critérios NESTOR

(Continuação)

RDC-Arq		**Catalogue of criteria for trusted digital repositories NESTOR**		**Comparação**
Seção	**Grupo**	**Seção**	**Requisitos**	
II.2.2 – Gerenciamento do documento digital	**d. Armazenamento e preservação / manutenção do *AIP***	**B. Gestão de Objetos Digitais**		
	d1.		-	ISem correspondências similares
	d2.		10.4	Similares
	d3.		-	ISem correspondências similares
	d4.		6.2 e 7.2	Similares
	d5.		-	ISem correspondências similares
	e. Gerenciamento de informação			
	e1.		-	ISem correspondências similares
	e2.		12.2	Similares
	e3.		12.7	Similares
	e4.		12.7	Similares
	f. Gerenciamento de acesso			
	f1.		6.3	Similares
	f2.		-	ISem correspondências similares
	f3.		3.3	Similares
	f4.		6.3	Similares
	f5.		-	ISem correspondências similares
	f6.		-	ISem correspondências similares
	f7.		-	ISem correspondências similares
	f8.		-	ISem correspondências similares
	f9.		7.3	Similares

QUADRO 17 - Comparação entre os Requisitos do RDC-Arq e Critérios NESTOR

(Conclusão)

RDC-Arq		**Catalogue of criteria for trusted digital repositories NESTOR**		**Comparação**
Seção	**Grupo**	**Seção**	**Requisitos**	
II.2.3 – Tecnologia, infraestrutura técnica e segurança	**a. Infraestrutura de sistema**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**		
	a1.		-	Sem correspondências similares
	a2.		-	Sem correspondências similares
	a3.		-	Sem correspondências similares
	a4.		-	Sem correspondências similares
	a5.		6.2	Similares
	a6.		-	Sem correspondências similares
	a7.		-	Sem correspondências similares
	a8.		4.5	Similares
	a9.		4.5	Similares
	b. Tecnologias apropriadas			
	b1.		4.5	Similares
	c. Segurança			
	c1.		14	Similares
	c2.		13.2	Similares
	c3.		-	Sem correspondências similares
	c4.		-	Sem correspondências similares

FONTE: Desenvolvido pelo autor.

Construiu-se uma tabela com os seguintes dados:

1- Quantidade total de requisitos / critérios total do RDC-Arq e do NESTOR;

2- Quantidade de requisitos do RDC-Arq compatíveis com os critérios do NESTOR.

No intuito de tornar os procedimentos de comparação mais transparentes e acessíveis, disponibilizamos o Apêndice J, que traz o quadro completo de comparação entre os dois modelos supracitados.

QUADRO 18 - Resultado Quantitativo da Comparação entre os Requisitos do RDC-Arq e Critérios NESTOR

Modelo de requisitos/ critérios	RDC-Arq	NESTOR
1 - Quantidade total de requisitos / critérios total do RDC-Arq e do NESTOR	74	42
2 - Quantidade de requisitos do RDC-Arq compatíveis com os critérios do NESTOR.	39	
3 - Quantidade de Requisitos do RDC-Arq que não encontraram similaridade conceitual entre os Critérios do NESTOR.	37	
4 - Quantidade de Critérios NESTOR sem correspondentes nos requisitos RDC-Arq	06	

FONTE: Desenvolvido pelo autor.

Abaixo, são apresentados os critérios do NESTOR que não apresentam requisitos conceitualmente similares entre os requisitos do RDC-Arq. Esta pesquisa os reuniu na Tabela 12, a fim de analisá-los e tecer possíveis melhorias advindas dessa análise. São os seguintes:

TABELA 11 - Requisitos NESTOR sem correspondentes conceituais similares no RDC-Arq

Critérios para Repositórios Digitais Confiáveis - NESTOR
A. Estrutura Organizacional
2.1 O repositório digital garante que suas comunidade(s) designada(s) podem acessar os objetos digitais.
5.2 O repositório digital documenta todos os seus elementos com base em um processo.
B. Gerenciamento de objetos
10.3 O repositório digital garante o armazenamento e legibilidade dos pacotes de informação para arquivamento (AIPs).
11.1 O repositório digital define seus Pacotes de Disseminação de Informação (DIPs).
11.2 O repositório digital garante a transformação de pacotes de informação para arquivamento (AIPs) em Pacotes de Disseminação de Informação (DIPs).
C. Infraestrutura e Segurança
13.1 A infraestrutura de TI implementa os requisitos de gerenciamento de objetos.

FONTE: Desenvolvido pelo autor.

Contribuições para o RDC-Arq provenientes do NESTOR

A estrutura conceitual de apresentação dos critérios NESTOR apresenta um campo denominado “Literatura relacionada”, campo esse que poderia significar um grande melhoramento para um RDC-Arq, no sentido de prover fontes bibliográficas de relevância aos responsáveis pela implementação, auditoria e certificação de repositórios arquivísticos digitais.

6.3 ANÁLISE SOBRE A COMPARAÇÃO ENTRE OS REQUISITOS DO RDC-ARQ E O ACTDR

Durante esta pesquisa, efetuou-se uma análise comparativa qualitativa e quantitativa entre os requisitos para implementação de repositórios digitais confiáveis, de autoria do Conselho Nacional de arquivos, e os critérios do *AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES*- ACTDR.

Abaixo, apresenta-se o Quadro 18, que traz a comparação entre os requisitos do RDC-Arq e os critérios do ACTDR.

QUADRO 19 - Comparação entre os Requisitos do RDC-Arq e Critérios ACTDR

(Continua)

RDC-Arq		- ACTDR		Comparação
Seção	**Grupo**	**Seção**	**Grupo**	
II.2.1 - Infraestrutura organizacional	**a. Governança e viabilidade organizacional**	**3. Infraestrutura Organizacional**	**3.1. Governança e Viabilidade Organizacional**	
	a1.		3.1.1; 3.1.2; 3.1.2.1; 3.1.2.2	Similares
	b. Estrutura organizacional e de pessoal		**3.2. Estrutura Organizacional e Pessoal**	
	b1.		3.2.1; 3.2.1.2	Similares
	c. Transparência de procedimentos e arcabouço político		**3.3. Responsabilização Processual e Política de Preservação Estrutural**	
	c1		3.3.1	Similares
	c2.		3.3.2	Similares
	c3.		3.3.2.1	Similares
	c4.		-	Sem correspondências similares
	c5.		3.3.3	Similares
	c6.		-	Sem correspondências similares
	c7.		-	Sem correspondências similares
	c8.		3.3.5	Similares
	c9.		3.3.6	Similares
	c10.		-	Sem correspondências similares
	d. Sustentabilidade financeira		**3.4. Sustentabilidade Financeira**	
	d1.		3.4.1	Similares
	d2.		-	Sem correspondências similares
	d3.		*3.4.2*	Similares
	d4.		3.4.3	Similares

QUADRO 19 - Comparação entre os Requisitos do RDC-Arq e Critérios ACTDR

(Continuação)

RDC-Arq		***AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES* - ACTDR**		**Comparação**
Seção	**Grupo**	**Seção**	**Grupo**	
II.2.1 - Infraestrutura organizacional	**e. Contratos, licenças e passivos**	**3. Infraestrutura Organizacional**	**3.5 Contratos, Licenças e Passivos**	
	e1.		3.5.1; 3.5.1.3; 3.5.1.1; 3.5.1.2; 3.5.1.4.	Similares
II.2.2 – Gerenciamento do documento digital	**a. Admissão: captura de documentos digitais**	**4 Gestão de Objetos Digitais**	**4.1 Ingest: Aquisição de Conteúdo**	
	a1.		4.1.1 4.1.1.1 4.1.1.2	Similares
	a2.		4.1.2	Similares
	a3.		4.1.4	Similares
	a4		4.1.5	Similares
	a5.		4.1.6	Similares
	a6.		4.1.7	Similares
	a7.		-	ISem correspondências similares
	a8.		4.1.8	Similares
	b. Admissão: criação do pacote de arquivamento		**4.2 Ingest: Criação do AIP**	
	b1.		4.2.1 4.2.1.1	Similares
	b2.		4.2.1.2	Similares
	b3.		4.2.2	Similares
	b4.		4.2.3 4.2.3.1	Similares
	b5.		4.2.4 4.2.4.1 4.2.4.1.1	Similares
	b6.		4.2.4.1.2	Similares

QUADRO 19 - Comparação entre os Requisitos do RDC-Arq e Critérios ACTDR

(Continuação)

RDC-Arq		***AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES* - ACTDR**		**Comparação**
Seção	**Grupo**	**Seção**	**Grupo**	
II.2.2 – Gerenciamento do documento digital	b7.	**4 Gestão de Objetos Digitais**	4.2.4.1.3 4.2.4.1.4 4.2.4.1.5	Similares
	b8.		4.2.4.2	Similares
	b9.		4.2.5 4.2.5.1 4.2.5.2 4.2.5.3 4.2.5.4	Similares
	b10.		4.2.6 4.2.6.1 4.2.6.2 4.2.6.3	Similares
	b11.		4.2.8	Similares
	b12.		4.2.9	Similares
	b13.		4.2.10	Similares
	c. Planejamento da preservação		**4.3. Planejamento de Preservação**	
	c1.		4.3.1	Similares
	c2.		4.3.2 4.3.2.1	Similares
	c3.		4.3.3	Similares
	c4.		4.3.4	Similares
	d. Armazenamento e preservação / manutenção do *AIP*		**4.4. Preservação AIP**	
	d1.		-	ISem correspondências similares
	d2.		4.4.1	Similares
	d3.		4.4.1.1	Similares
	d4.		4.4.1.2	Similares
	d5.		4.4.2	Similares

QUADRO 19 - Comparação entre os Requisitos do RDC-Arq e Critérios ACTDR

(Continuação)

RDC-Arq		***AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES* - ACTDR**		**Comparação**
Seção	**Grupo**	**Seção**	**Grupo**	
II.2.2 – Gerenciamento do documento digital	**e. Gerenciamento de informação**	**4 Gestão de Objetos Digitais**	**4.5 Gestão da Informação**	
	e1.		4.5.1	Similares
	e2.		4.5.2	Similares
	e3.		4.5.3	Similares
	e4.		4.5.3.1	Similares
	f. Gerenciamento de acesso		**4.6 Gestão de Acesso**	
	f1.		4.6.1	Similares
	f2.		-	Sem correspondências similares
	f3.		-	Sem correspondências similares
	f4.		-	Sem correspondências similares
	f5.		4.6.1.1	Similares
	f6.		-	Sem correspondências similares
	f7.		-	Sem correspondências similares
	f8.		4.6.2.1	Similares
	f9.		4.6.2	Similares
II.2.3 – Tecnologia, infraestrutura técnica e segurança	**a. Infraestrutura de sistema**	**5 Gestão de Riscos de Infraestrutura e Segurança**	**5.1 Gestão de Riscos de Infraestrutura Técnica**	
	a1.		-	Sem correspondências similares
	a2.		5.1.1.1 5.1.1.1.1 5.1.1.1.2 5.1.1.1.3 5.1.1.1.4 5.1.1.1.5	Similares
	a3.		5.1.2	Similares
	a4.		5.1.2.1	Similares
	a5.		5.1.1.3	Similares
	a6.		5.1.1.3.1	Similares
	a7.		5.1.1.3.1	Similares
	a8.		5.1.1.5	Similares

QUADRO 18 - Comparação entre os Requisitos do RDC-Arq e Critérios ACTDR

(Conclusão)

RDC-Arq		***AUDIT AND CERTIFICATION OF TRUSTWORTHY DIGITAL REPOSITORIES* - ACTDR**		**Comparação**
Seção	**Grupo**	**Seção**	**Grupo**	
	a9.		5.1.1.6 5.1.1.6.1 5.1.1.6.2	Similares
II.2.3 – Tecnologia, infraestrutura técnica e segurança	a10.		5.1.1.4	Similares
	b. Tecnologias apropriadas		**5.1 Gestão de Riscos de Infraestrutura Técnica**	
	b1.		5.1.1.1.6 5.1.1.1.7 5.1.1.1.8	Similares
	c. Segurança		**5.2 Gestão de Riscos de Segurança**	
	c1.		5.2.1	Similares
	c2.		5.2.2	Similares
	c3.		5.2.3	Similares
	c4.		5.2.4	Similares

FONTE: Desenvolvido pelo autor.

Construiu-se a Tabela 13 com os seguintes dados:

a. Quantidade total de requisitos / critérios total do RDC-Arq e do ACTDR;
b. Quantidade de requisitos do RDC-Arq compatíveis com os critérios do ACTDR.
c. Quantidade de critérios do ACTDR que não encontraram similaridade conceitual entre os requisitos do RDC-Arq.
d. Quantidade de Critérios ACTDR sem correspondentes nos requisitos RDC-Arq.

A comparação foi efetivada com base na similaridade conceitual entre os requisitos do RDC-Arq e os critérios do ACTDR. Com o intuito de tornar os procedimentos de comparação mais transparentes e acessíveis, disponibilizamos o Apêndice I que traz o quadro completo de comparação entre os dois modelos supracitados.

TABELA 12 - Resultado Quantitativo da Comparação entre os Requisitos do RDC-Arq e Critérios ACTDR

Modelo de requisitos / critérios	RDC-Arq	ACTDR
1 - Quantidade total de requisitos / critérios total do RDC-Arq e do ACTDR	74	109
2 - Quantidade de requisitos do RDC-Arq conceitualmente similares com os critérios do ACTDR.	61	
3 – Quantidade de Requisitos do RDC-Arq que não encontraram similaridade conceitual entre os Critérios do ACTDR.	13	
4 - Quantidade de Critérios ACTDR que não encontraram similaridade conceitual entre os requisitos RDC-Arq	5	

FONTE: Desenvolvido pelo autor.

Foi verificado que há compatibilidade conceitual parcial entre os requisitos do RDC-Arq e os critérios do ACTDR. Ou seja, 61 dos 74 requisitos elencados no RDC-Arq estão integralmente contidos nos critérios ACTDR. No Quadro 19, apresentam-se os requisitos do RDC-Arq em que não verificou-se critério correspondente no ACTDR.

O ACTDR apresenta um número de critérios muito superior ao RDC-Arq, porém, essa diferença se explica da seguinte maneira:

a) O RDC-Arq mescla vários critérios do ACTDR em um único requisito, em alguns casos;
b) O ACTDR apresenta mais subdivisões de classificação de seus requisitos do que o RDC-Arq. Ou seja, enquanto o RDC-Arq tem três níveis na apresentação

de um requisito, o ACTDR tem, em alguns casos, 5 níveis para um critério, o que aumenta o seu detalhamento e aprofundamento explicativo.

QUADRO 18 - Requisitos do RDC-Arq sem critério correspondente no ACTDR

Modelo	**RDC-Arq**
Seção	**II.2.1 - Infraestrutura organizacional**
Grupo	**c. Transparência de procedimentos e arcabouço político**
Requisito	- documentar permissões legais - por meio de acordos de custódia, normas de procedimentos e outros - que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;
Requisito	- relacionar o registro histórico, acima referido, com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;
Requisito	- demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;
Requisito	-estar comprometido em notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu *status* de certificação (no caso de repositórios já certificados).
Grupo	**d. Sustentabilidade financeira**
Requisito	- revisão e ajustes anuais;
Seção	**II.2.2 – Gerenciamento do documento digital**
Grupo	**a. Admissão: captura de documentos digitais**
Requisito	- demonstrar em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório; e
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***
	- utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;
Grupo	**f. Gerenciamento de acesso**
Requisito	- 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;
Requisito	- concessão de 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;
Requisito	- 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;
Requisito	- demonstração de que o processo que gera o *DIP* 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);
Requisito	- demonstração de que o processo que gera o *DIP* 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);
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**
Grupo	**a. Infraestrutura de sistema**
Requisito	Um repositório deve possuir uma infraestrutura tecnológica robusta, de maneira a apoiar a confiabilidade dos *AIPs* nele mantidos. Para tanto, deve observar os seguintes aspectos: - funcionamento do repositório com base num sistema operacional e outros *softwares* de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;

FONTE: Desenvolvido pelo autor.

Critérios ACTDR sem correspondentes nos requisitos RDC-Arq

Com o intuito de analisar os critérios do ACTDR que não estão presentes no RDC-Arq, elaborou-se o Quadro 20, composto por critérios do ACTDR que não se encontram, conceitualmente, presentes no RDC-Arq. A intenção é subsidiar possíveis propostas de melhorias no RDC-Arq utilizando esses elementos díspares.

QUADRO 19 - Requisitos ACTDR sem correspondentes conceituais similares no RDC-Arq

ACTDR	
Seção	**3 Infraestrutura Organizacional**
Grupo	**3.1. Governança e Viabilidade Organizacional**
Requisito	3.1.3 O repositório deve ter uma Política de Coleta ou outro documento que especifique o tipo de informação à qual preservará, reterá, gerenciará e fornecerá acesso.
Requisito	3.2.1.1 O repositório deve ter identificado e estabelecido as tarefas que ele precisa executar.
Requisito	3.3.4 O repositório deve se comprometer com a transparência e a responsabilidade em todas as ações que suportam a operação e o gerenciamento do repositório que afetam a preservação do conteúdo digital ao longo do tempo.
Seção	**4 Gerenciamento Digital de Objetos**
Grupo	**4.3. Planejamento de Preservação**
Requisito	4.3.3.1 O repositório deve ter mecanismos para criar, identificar ou coletar qualquer Informação de Representação extra necessária.
Seção	**5 Gestão de Riscos de Infraestrutura e Segurança**
Requisito	**5.1 Gestão de Riscos de Infraestrutura Técnica**
Requisito	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.

FONTE: Desenvolvido pelo autor.

Observações / Contribuições para o RDC-Arq:

a) O ACTDR, em alguns casos, subdivide um critério em subcritérios de níveis 1 e 2, de forma a detalhar com maior profundidade um critério. Esse formato pode ser interessante a alguns requisitos do RDC-Arq que necessitem de maiores especificações;
b) O campo “Discussão”, presente na estrutura de apresentação dos critérios no ACTDR, pode ser uma melhoria a ser adotada no RDC-Arq, a fim de auxiliar no entendimento mais amplo dos requisitos, por parte dos responsáveis pela implantação, auditoria e certificação.

6.4 PROCEDIMENTOS PARA A TRANSMISSÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITALIZADOS DE UM PRODUTOR A UM ARQUIVO, EM CONFORMIDADE COM O DECRETO 10.278/2020

A seguir, apresenta-se uma proposição de procedimentos de transmissão de documentos arquivísticos digitalizados de um Produtor a um Arquivo, em conformidade com o Decreto 10.278/2020. Partindo do Modelo de Referência OAIS, do PAIMAS, e o *Into the Archive - a guide for the information transfer to a digital repository,* do Grupo NESTOR*,* pretende-se proporcionar aos Produtores de documentos arquivísticos digitalizados um conjunto de procedimentos técnicos arquivísticos e computacionais que possibilitem a transmissão desses documentos a um Arquivo, observando as determinações do Decreto 10.278/2020 e, ao mesmo tempo, assegurando a manutenção das qualidades arquivísticas dos documentos digitalizados, mantendo seu valor legal.

Ações de responsabilidade do Produtor do Pacote SIP

As ações elencadas, nesta proposta, iniciam-se partindo do pressuposto que o Produtor:

a) Digitalizou o documento arquivístico observando as orientações técnicas do anexo I do Decreto 10.278/2020, que prescreve os padrões técnicos mínimos para digitalização de documentos;
b) Assinou o documento digitalmente, utilizando certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

1º Ação: Verificação do formato do objeto digital

O Produtor deverá verificar o formato de documento arquivístico digitalizado a ser transmitido e convertê-lo ao formato adequado, quando necessário, observando o disposto no Decreto 10.278/2020, que estabelece, em seu anexo I, o formato do arquivo digital, a partir do tipo documental digitalizado. Os formatos de arquivo previstos no seu anexo I do referido Decreto são o PDF/A e o PNG[119].

Ocorre que o Decreto não define qual subtipo de PDF/A deve ser utilizado. Para tanto, esta pesquisa recorreu à *Orientação Técnica nº 4 - Recomendações de uso do PDF/A para Documentos Arquivísticos* que, de acordo CONARQ (2016), apresenta recomendações gerais sobre o uso do formato PDF/A na produção e no arquivamento de documentos

[119] Portable Network Graphics.

arquivísticos digitais, ou seja, nas idades corrente, intermediária e permanente, visando ao seu acesso e a sua preservação.

O formato PDF/A é utilizado, segundo o Decreto 10.278/2020, em documentos textuais manuscritos, impressos, coloridos ou em preto e branco.

Já o Formato PNG é utilizado para fotografias, cartazes, plantas e mapas.

Abaixo, apresentam-se orientações sobre digitalização de imagens em formatos PNG, TIFF e JPEG2000, efetuadas por CONARQ (2010):

> - O formato *Portable Network Graphics* (PNG), apresenta como vantagem a utilização de compressão sem perdas, além, de ser um formato padronizado pela *International Standard Organization* como ISO/IEC 15948:2003. Entretanto, é mais limitado na inserção de metadados embutidos.
>
> - O formato mais utilizado para os representantes digitais matrizes é o formato TIFF, que apresenta elevada definição de cores sendo amplamente conhecido e utilizado para o intercâmbio de representantes digitais entre as diversas plataformas de tecnologia da informação existentes.
>
> -O formato de arquivo digital JPEG 2000, tem sido apreciado para a geração de matrizes quando os originais em outro formato continuam a serem preservados, mas apresenta atualmente limitações em navegação WEB, devendo ser gerada uma imagem derivada de acesso em JPEG. Pode ser configurado para fazer a compressão sem perdas. Em relação ao PNG, o JPEG 2000 permite embutir mais metadados. É um formato padronizado pela *International Standard Organization* como ISO/IEC 15444-1:2000. (CONARQ, 2010).

Ferramentas para a verificação de formatos

O formato PNG pode ser validado por meio dos softwares DROID; JHOVE.

O formato PDF/A pode ser validado pelas ferramentas DROID; VERApdf

Não se recomenda a ferramenta JHOVE, pela ocorrência de falhas em seus processos de validação de PDF/A, apontados em algumas pesquisas (LINDLAR; TUNNAT, 2017; LINDLAR; TUNNAT; WILSON, 2017).

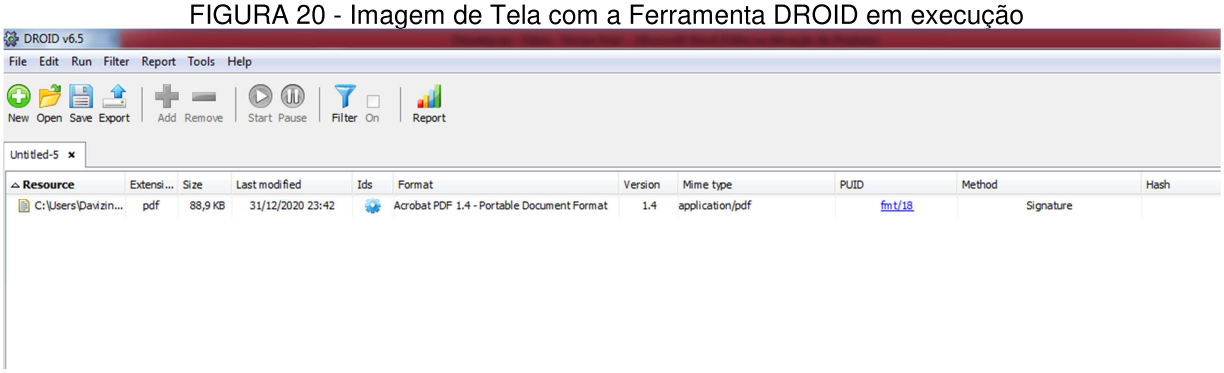
Justificativas Técnicas para a adoção das Ferramentas

> O DROID (*Digital Record Object IDentification*[120]) é uma ferramenta de identificação de formato de arquivo desenvolvida pelo Arquivo Nacional do Reino Unido. É amplamente utilizado em todo o mundo, em instituições de memória cultural, locais e departamentos do governo central e outros órgãos públicos, e tem sido incorporado em múltiplos produtos de preservação digital comerciais e de código aberto. A função central do DROID é a identificação precisa do formato do arquivo, mesmo que a extensão do arquivo esteja errada ou em falta. Sempre que possível, as

[120]Identificação de objetos de registro digital. Tradução do autor.

> identificações são feitas além do tipo amplo, até o nível da versão. DROID pode atualmente identificar mais de 1400 arquivos formatos, e este número está crescendo o tempo todo. Informações sobre formatos de arquivos, incluindo as assinaturas de identificação utilizadas pela DROID são mantidas no PRONOM[121], o Arquivo Nacional de Registro de Formato. (THE NATIONAL ARCHIVES, 2020, p. 1).

FIGURA 20 - Imagem de Tela com a Ferramenta DROID em execução



FONTE: Desenvolvido pelo autor.

PRONOM é um sistema de informação on-line sobre formatos de arquivos de dados e seus produtos de *software* de apoio. Desenvolvido originalmente para apoiar a adesão e a preservação, no longo prazo, dos registros eletrônicos mantidos pelo *The National Archives of United Kingdom*, o PRONOM está agora sendo disponibilizado como um recurso para qualquer pessoa que necessite ter acesso a esse tipo de informação (THE NATIONAL ARCHIVES, 2021).

> Além de identificar o formato de arquivo, o DROID também extrai outras informações sobre os arquivos varreduras, tais como, tamanho do arquivo, data da última modificação e caminho do arquivo. Estas informações são apresentadas em um perfil que pode ser analisado na tela na Interface Gráfica do Usuário (GUI[122]), utilizando filtragem, ou exportado para um arquivo CSV[123] (formato utilizado por processadores de tabelas). O DROID também examina os arquivos dentro de arquivos de contêineres, tais como arquivos 'zip[124]'. (THE NATIONAL ARCHIVES, 2020, p. 1).

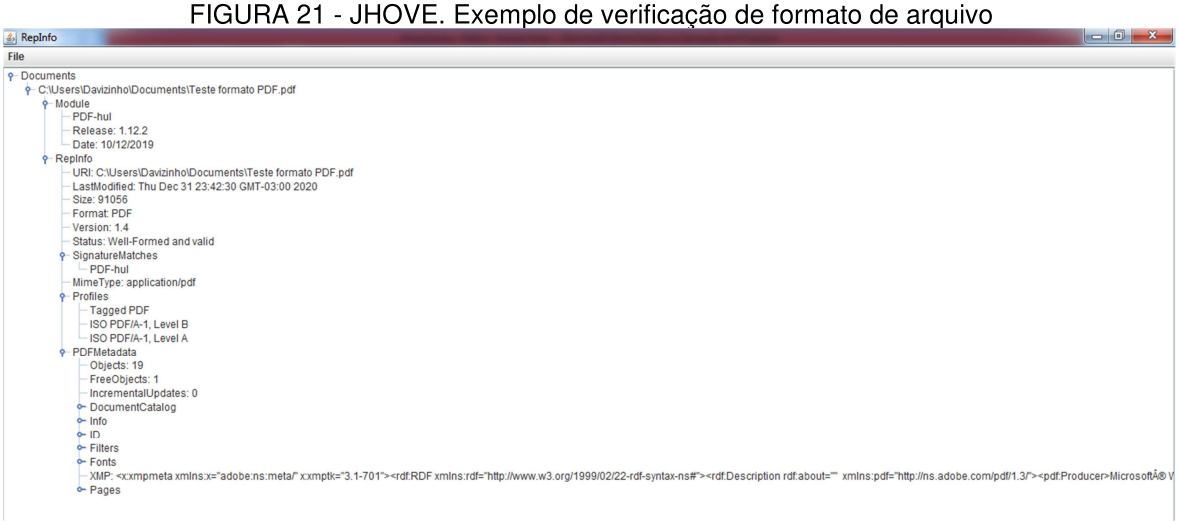
O JHOVE (*JSTOR/Harvard Object Validation Environment*[125]) é uma estrutura de software extensível para realizar a identificação de formatos, validação e caracterização de

---

[121] Public Record Office and Nom
[122] *Graphical User Interface*
[123] *Comma Separated Values* (CSV) é um formato de arquivo de texto que pode ser usado para trocar dados de uma planilha entre aplicativos.
[124] Formato de compressão de pacotes de dados.
[125] Ambiente de validação de objetos JSTOR/Harvard. Tradução do autor.

objetos digitais. A identificação de formato é o processo de determinação do formato ao qual um objeto digital está em conformidade (OPEN PRESERVATION FOUNDATION, 2015).

FIGURA 21 - JHOVE. Exemplo de verificação de formato de arquivo



FONTE: Desenvolvido pelo autor.

A validação do formato é o processo de determinação do nível de conformidade de um objeto digital com a especificação de seu suposto formato (OPEN PRESERVATION FOUNDATION, 2015).

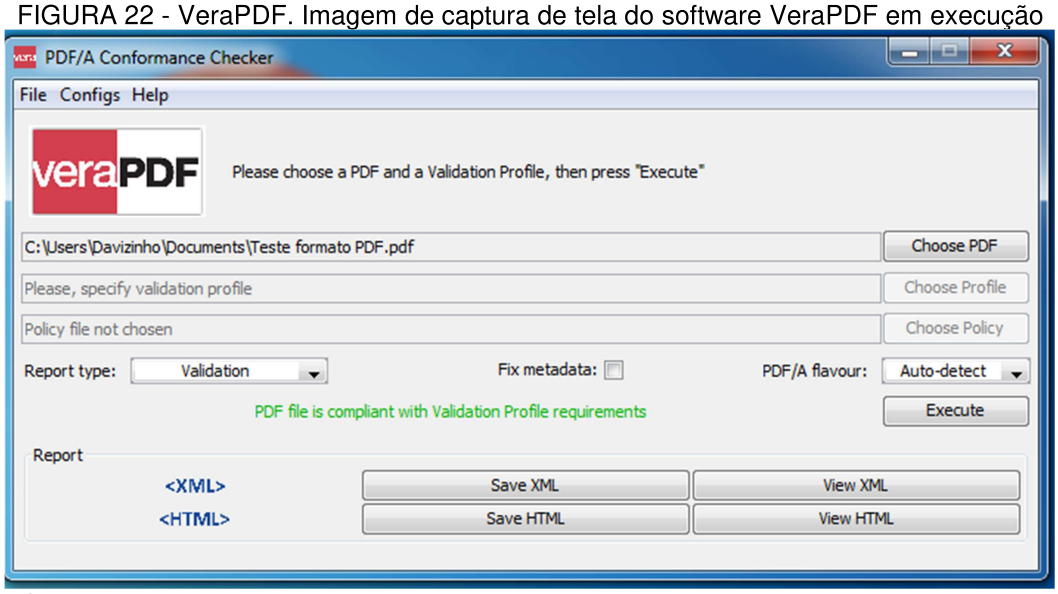
A conformidade do formato de validação é determinada em três níveis: 1) boa formatação, 2) validade e 3) consistência.

1) Um objeto digital é bem formatado se atender aos requisitos puramente sintáticos de seu formato;
2) Um objeto é válido se for bem formatado e atender aos requisitos semânticos de nível superior para a validade do formato;
3) Um objeto é consistente se for válido e sua informação de representação extraída internamente for consistente com a informação de representação fornecida externamente. (OPEN PRESERVATION FOUNDATION, 2015).

Entretanto, surgiram dúvidas, nos últimos anos, sobre a capacidade de validação de PDF/A utilizando a ferramenta JHOVE, conforme relatam Lindlar e Tunnat (2017), Lindlar, Tunnat e Wilson (2017), que concluíram, em suas pesquisas, que o software JHOVE não deve ser utilizado para a validação de documentos em formato PDF/A, por apresentar falhas no processo de validação.

O *software* VeraPDF Consortium fornece validação de PDF / A de código aberto desenvolvida com o suporte da indústria de PDF. O VeraPDF Conformance Checker usa a biblioteca VeraPDF Java, que fornece APIs e implementações para validação de PDF / A, verificação de política, reparo de metadados e relatórios. A interface gráfica do usuário (GUI) de *desktop* VeraPDF permite que os usuários executem o software em um computador *desktop* ou estação de trabalho. (VeraPDF, 2020).

FIGURA 22 - VeraPDF. Imagem de captura de tela do software VeraPDF em execução



FONTE: Desenvolvido pelo autor.

Compressão de arquivo sem perda de informação

O Decreto 10.278/2020 orienta que, na hipótese de necessidade de comprimir o arquivo, deve ser realizada compressão sem perda, de forma que a informação obtida, após a descompressão seja idêntica à informação antes de ser comprimida. Entretanto, o referido decreto não estabelece o algoritmo de compressão a ser utilizado, nem o *software* recomendado para tal tarefa.

A compressão de dados é definida, de acordo com Sharma e Naaz Mir (2018), como o processo de codificação de informações, usando menos bits do que a representação original das informações usaria. A compressão de dados é, frequentemente, conhecida como *bit-rate encoding* (codificação de taxa de bits) ou codificação da fonte.

A compressão de dados sem perda envolve, segundo Berz *et al.* (2015), uma transformação da representação do conjunto de dados original, de forma que é possível reproduzir exatamente o conjunto de dados originais, realizando uma transformação de descompressão. A compressão sem perda é utilizada na compressão de arquivos de texto, códigos executáveis, arquivos de processamento, arquivos de banco de dados, arquivos de

tabulação, e sempre que for importante que o original e os arquivos descompactados sejam idênticos.

Enfim, nesta pesquisa, recomenda-se que, até a definição um *software* capaz de realizar a compressão sem perda de dados, não devem ser utilizados softwares compressores nos pacotes SIPs produzidos para fins de procedimentos do Decreto 10.278/2020. É interessante que sejam realizados estudos para analisar e comparar algoritmos de compressão sem perda de *bits,* avaliando o tempo necessário para a execução de cada algoritmo, quando da compressão de objetos digitais de grande volume, bem como as perdas, se existirem.

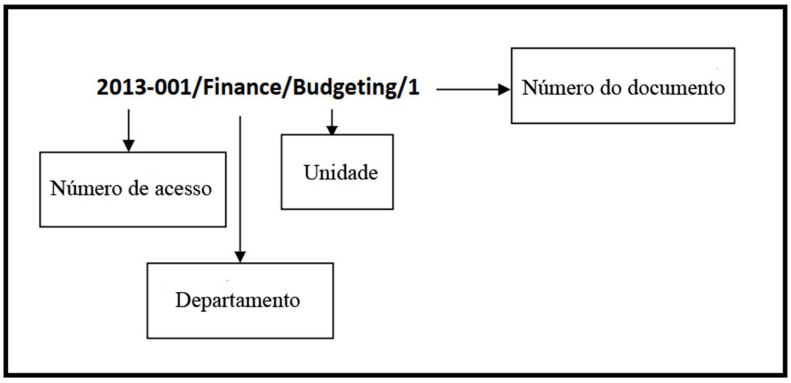
2ª Ação: O Produtor deverá identificar cada documento arquivístico digitalizado a ser transmitido através um identificador único persistente.

O Identificador Persistente é, de acordo com IRMT (2016), um número único que facilita gestão do registro digital e o vincula com seus metadados de suporte. Registros digitais e seus metadados de suporte são frequentemente armazenados em duas áreas separadas do repositório digital. O Identificador Persistente permite que esses dois elementos permaneçam conectados, garantindo a autenticidade e a confiabilidade dos registros digitais. Exemplos de registros persistentes:

> • the Uniform Resource Name (URN);
> • the persistent URL (PURL);
> • the Handle system;
> • the digital object identifier (DOI);
> • National Bibliography Numbers (NBNs);
> • the Archival Resource Key (ARK);
> • the Open URL (IRMT, 2016, p. 74).

Se a organização não tiver um *software* que crie um identificador persistente, um número único pode ser atribuído por um sistema de gerenciamento de registros ou de informações como uma medida provisória. Um método simplificado de atribuição de um identificador único é criar um que seja específico para a organização. Como mostrado no exemplo abaixo:

FIGURA 23 - Identificador Persistente

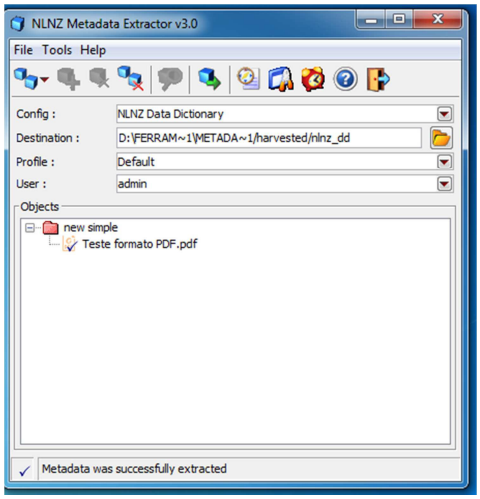


FONTE: IRMT (2016, p. 74, Tradução nossa). Adaptado.

Ação nº3: O Produtor deverá assegurar que cada documento arquivístico digitalizado a ser transmitido atenda aos elementos referentes aos metadados obrigatórios, conforme Anexo II do Decreto 10.278/2020.

Segundo Millar (2009b), o NLNZ *Metadata Extractor* foi desenvolvido pela Biblioteca Nacional da Nova Zelândia como uma ferramenta para a extração de metadados de uma série de formatos. O NLNZ *Metadata Extractor* extrai metadados de diferentes formatos de arquivo, incluindo documentos PDF, arquivos de imagem, arquivos de som, documentos textuais e outros. Os metadados coletados podem estar relacionados com o *hardware* ou *software* utilizado para criar o arquivo, a data e a hora em que foi criado, ou o nome ou título do responsável pela criação ou utilização do arquivo. O arquivo resultante da análise e coleta pelo NLNZ *Metadata Extractor* pode ser fornecido em formato XML ou outros formatos de código aberto para que as informações possam ser utilizadas para determinar critérios e ações de preservação.

FIGURA 24 - NLNZ Metadata Extractor



FONTE: Desenvolvido pelo autor.

Ação nº4: O Produtor deverá verificar cada documento arquivístico digitalizado a ser transmitido quanto à sua integridade.

Um *checksum* em um arquivo, de acordo com Digital Preservation Coalization (2020), é uma "impressão digital" pela qual mesmo a menor alteração no arquivo fará com que o checksum mude completamente. Os checksums são, normalmente, criados usando técnicas criptográficas e podem ser gerados usando uma gama de ferramentas de código aberto e prontamente disponíveis. É importante notar que embora os *checksums* possam ser usados para detectar se o conteúdo de um arquivo mudou, eles não dizem onde no arquivo ocorreu a mudança. Os *checksums* têm três usos principais:

> - Saber que um arquivo foi recebido corretamente de um proprietário de conteúdo ou fonte e depois transferido com sucesso para o armazenamento de preservação.
>
> - Saber que a fixidez do arquivo foi mantida quando esse arquivo está sendo armazenado.
>
> - Ser compartilhado com os usuários do Arquivo no futuro para que eles saibam que o arquivo foi corretamente recuperado do armazenamento e entregue a eles[126] (DIGITAL PRESERVATION COALIZATION, 2020).

A verificação de integridade pode ser realizada, por meio de *checksums*. A realização de um *checksum* gera um resumo numérico de um registro digital, denominado *hash*. O registro *hash* leva em consideração, no momento de sua criação, todos os *bits* que formam o objeto digital, e esse registro será armazenado no pacote SIP, o que permitirá que o receptor (nesse caso, o Arquivo da Instituição receptora do documento arquivístico digitalizado) verifique se o fluxo de *bits* recebido é exatamente o mesmo que o enviado. Se os registros tiverem sido corrompidos ou alterados de alguma forma durante o processo de transmissão, o *checksum* verificará que os resumos *hash* do Produtor e do Arquivo diferem e marcará o objeto digital como defeituoso.

O Decreto 10.278/2020 não estabeleceu qual o nível de complexidade de *hash* criptográfico deve ser utilizado para a verificação de integridade dos objetos arquivísticos digitalizados. Dessa forma, apresenta-se um quadro-resumo elaborado pelo *National Digital*

---

[126] Texto original: *Checksums have three main uses:*
- *To know that a file has been correctly received from a content owner or source and then transferred successfully to preservation storage*
- *To know that file fixity has been maintained when that file is being stored.*
- *To be given to users of the file in the future so they know that the file has been correctly retrieved from storage and delivered to them.*

Stewardship Alliance (NDSA) que exemplifica o nível de complexidade e esforço necessário correspondente a ser realizado pelo sistema computacional, algo que implicará em tempo demandado para a conclusão da verificação e no volume de informação processada.

QUADRO 20 - Nível de complexidade e esforço necessário correspondente realizado pelo sistema computacional

Instrumento de Fixidade	**Definição**	**Nível de esforço e retorno sobre o investimento**
Tamanho de arquivo esperado	O tamanho do arquivo que difere do esperado pode ser um indicador de problemas, por exemplo, destacando arquivos de zero *bytes*	Baixo nível de esforço e baixo nível de detalhes. O tamanho do arquivo é um metadado técnico gerado automaticamente e pode ser visualizado no Windows Explorer ou em outras ferramentas comuns.
Contagem esperada de arquivos	A contagem de arquivos que difere do esperado pode ser um indicador de que os arquivos são adicionados ou descartados do pacote.	Baixo nível de esforço e baixo nível de detalhes. A contagem de arquivos é frequentemente gerada automaticamente e pode ser visualizada no Windows Explorer ou em outras ferramentas comuns.
Cyclic Redundancy Check (CRC)	Verificação típica de erro na rede	Baixo nível de esforço e nível moderado de detalhes. Os valores das funções CRC, que são variáveis mas tipicamente 32 ou 64 bits, são relativamente fáceis de implementar e analisar.
Message-Digest algorithm 5 (MD5)	Função de *hash* criptográfico	Nível moderado de esforço e alto nível de detalhes. Os requisitos de CPU e processamento para calcular os valores de hash são baixos a moderados, dependendo do tamanho do arquivo. O tamanho de saída do valor de hash é o menor dos valores de hash criptográfico a 128 bits.
Secure Hash Algorithm 1 (SHA-1)	Função de *hash* criptográfico	Nível moderado de esforço, alto nível de detalhes e garantia de segurança adicional. Devido a seu maior valor de hash de saída de 160 bits, o SHA-1 requer mais tempo relativo para calcular para um determinado número de ciclos de processamento CPU e tempo de processamento do que o MD5.
Secure Hash Algorithm 256 (SHA-256)	Função de *hash* criptográfico mais segura	Alto nível de esforço e muito alto nível de detalhes, e garantia de segurança adicional. Com um valor de hash de saída de 256 bits, o SHA-256 requer mais tempo relativo para calcular para um determinado número de ciclos de processamento CPU e tempo de processamento do que o SHA-1.

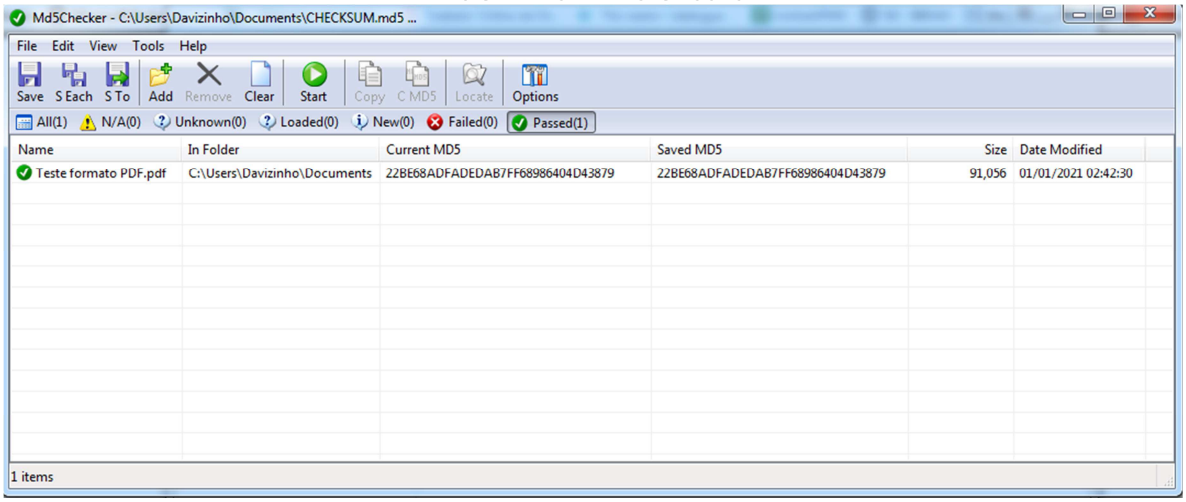
FONTE: National Digital Stewardship Alliance (NDSA, 2014, p. 5, Tradução nossa).

Os CRCs são úteis para gerar informações sobre fixidez e são usados frequentemente no nível de conjunto de dados estruturados , no interior do registro. Entretanto, como MD5, SHA1 e SHA256 são bastante superiores, sempre que os recursos permitem, pode ser melhor confiar em qualquer uma destas funções criptográficas de *hash* para a documentação completa de fixidade de nível de arquivo e objeto. Como observado, MD5, SHA1 e SHA256 são funções de *hash* criptográfico com diferentes tamanhos de soma de controle e com níveis crescentes de segurança. Em muitos casos, para fins de fixidez de dados, tanto MD5 quanto SHA1 são mais úteis do que SHA256 devido ao maior tempo de computação e requisitos de Unidade Central de Processamento (CPU) do computador para este último. Com o aumento dos níveis de segurança, aumenta o tempo e os recursos para calcular, portanto, dependendo da quantidade de dados em uma coleção e dos recursos

disponíveis, cada um tem um lugar em diferentes fluxos de trabalho de verificação de fixidez (NDSA, 2014).

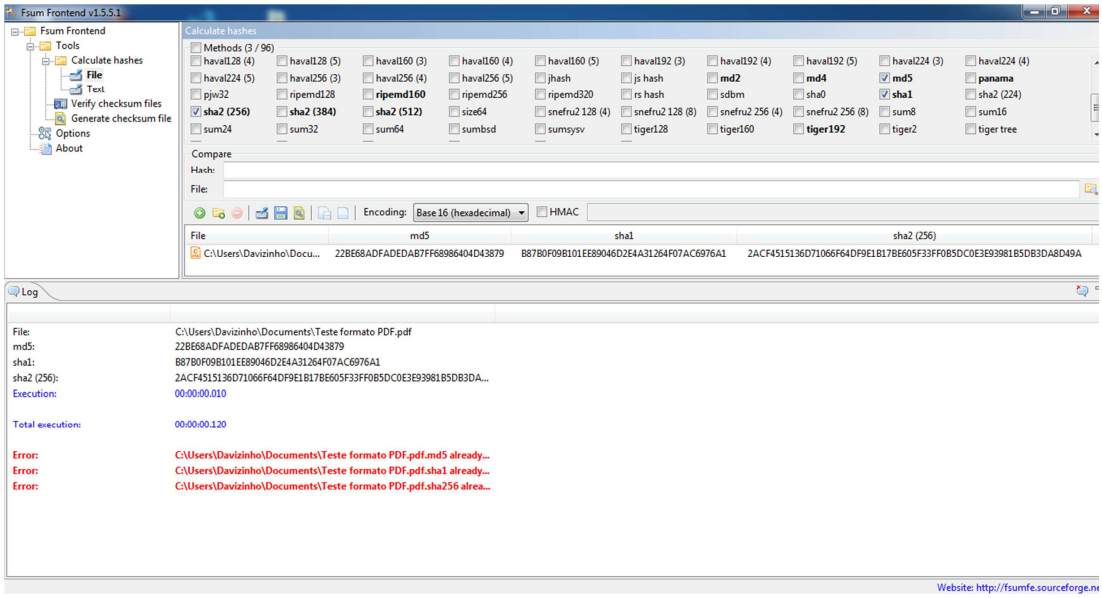
Ferramentas recomendadas para a verificação de integridade: Jacksum, Md5checker, FsumFrontend.

FIGURA 25 - MD5 Checker



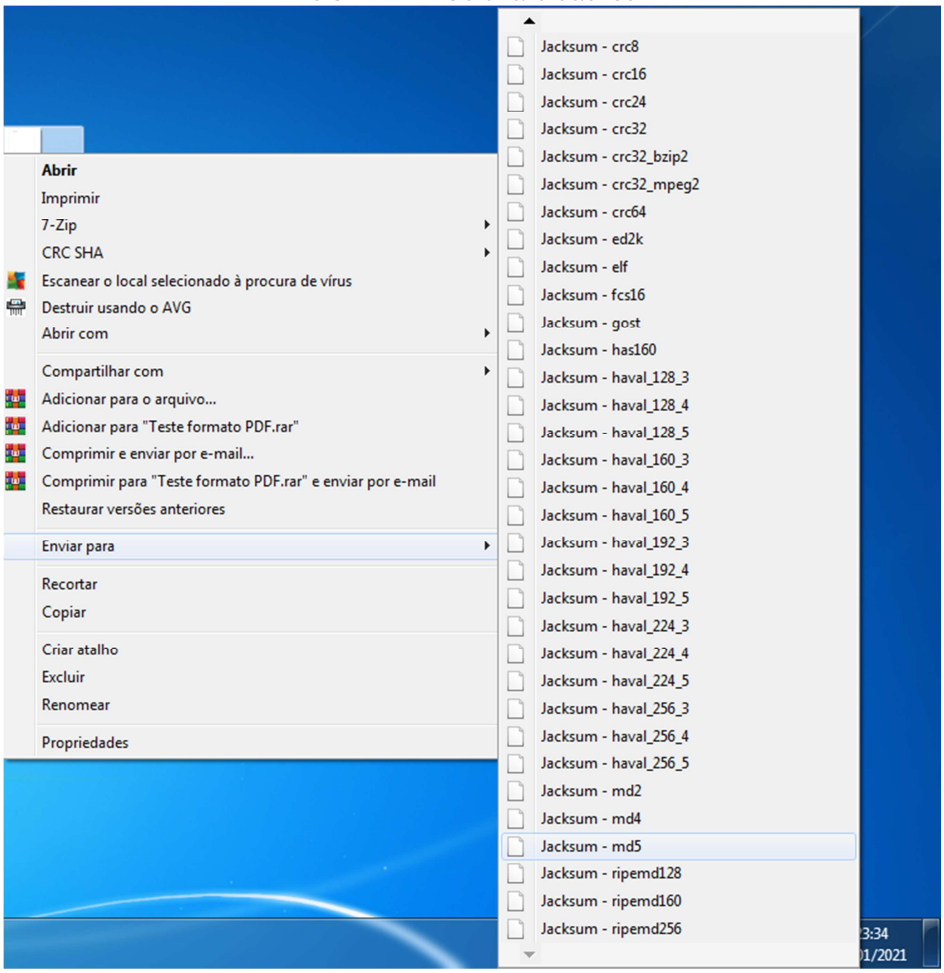
FONTE: Desenvolvido pelo autor.

FIGURA 26 - Fsum Frontend



FONTE: Desenvolvido pelo autor.

FIGURA 27 - *Software* Jacksum



FONTE: Desenvolvido pelo autor.

Ação nº5 - O Produtor deve ser realizar cópias de segurança dos documentos arquivísticos digitalizados a serem transmitidos.

Registros duplicados devem ser mantidos até que se saiba que o processo de transmissão foi bem sucedido, uma vez que podem ser necessários como cópias-mestras, caso ocorram erros, durante o processo, que comprometam a integridade dos dados do pacote SIP.

Recomenda-se que o Produtor mantenha as cópias-mestras do pacote SIP transmitido pelo mesmo prazo previsto na Tabela de Temporalidade Documental do Arquivo da Instituição receptora, preferencialmente, em um repositório arquivístico digital confiável, para fins de efetuar a validação do objeto transmitido, em caso de contestação, por alguma das partes, quanto à proveniência e autenticidade do documento arquivístico digitalizado transferido.

Ferramentas recomendadas: Não há necessidade de ferramentas para essa ação.

Ação nº6 - O Produtor deverá verificar cada documento arquivístico digitalizado a ser transferido quanto à existência de vírus e outras formas de códigos maliciosos, através varredura por *software* antivírus atualizado.

Malware é, de acordo com Monnappa (2018), um código que realiza ações maliciosas; podendo tomar a forma de um executável, *script*, código, ou qualquer outro *software*. Os atacantes usam *malware* para roubar informações sensíveis, espionar o sistema infectado, ou assumir o controle do sistema. Normalmente, ele entra em seu sistema sem consentimento do usuário e pode ser entregue, por meio de vários canais de comunicação, tais como e-mail, *web*, ou *drives* USB.

A seguir estão algumas das ações maliciosas realizadas por *malware*:

a) Perturbação das operações do computador;
b) Roubo de informações sensíveis, incluindo dados pessoais, comerciais e financeiros;
c) Acesso não autorizado ao sistema da vítima;
d) Espionagem das vítimas;
e) Envio de e-mails de *spam*;
f) Ataques de negação de serviço distribuído;
g) Bloqueio de arquivos no computador e solicitação de resgate para liberação do acesso.

Ferramentas recomendadas: Antivírus AVG, Avast, Panda.

Ação nº7 - O Produtor deverá verificar com o contato no arquivo da Instituição receptora as formas disponíveis para a transmissão do objeto digital, sob a forma de SIP, seguindo o padronizado no documento "Acordo de Submissão".

As formas de envio do podem incluir:

a) e-mail;
b) Link de upload;
c) Encaminhamento de mídia removível (pendrive, disco rígido externo).

É importante que o Produtor verifique a capacidade que a operadora de internet contratada disponibiliza para velocidade de conexão, bem como sua estabilidade no momento de transmissão, principalmente quando o pacote de informação alcançar um volume considerável.

Ferramentas recomendadas: Não há necessidade de ferramentas para essa ação.

Criação um Pacote SIP no *software* BAGGER

No intuito de auxiliar o Produtor a criar um Pacote de Submissão de Informação de forma padronizada e compatível com o Modelo de Referência OAIS e, ao mesmo tempo, capaz observar as determinações do Decreto 10.278/2020, apresenta-se como uma opção o software Bagger. Abaixo, seguem algumas explicações disponíveis no *Bagger GUI User Guide: How to Create and Validate Bags with Bagger* e no *BagIt File Packaging Format*.

FIGURA 28 - Imagem da Tela de inicialização do software Bagger

FONTE: Desenvolvido pelo autor.

O aplicativo BAGGER foi criado para a Biblioteca do Congresso dos EUA como uma ferramenta para produzir um pacote de arquivos de dados, de acordo com a especificação BagIt. (NC DEPARTMENT OF NATURAL AND CULTURAL - NCDCR, 2019).

BagIt é uma especificação, um formato hierárquico de embalagem de arquivo projetado para suportar armazenamento em disco ou em rede e transferência de arquivos digitais de conteúdo arbitrários. (ADAMS *et al.*, 2018).

Especificação do BagIt define uma convenção de layout de arquivo hierárquico projetada para apoiar o armazenamento e a transferência de conteúdo digital arbitrário. A

especificação surgiu de uma colaboração entre a Biblioteca do Congresso e a Biblioteca Digital da Califórnia e foi disponibilizada como um rascunho em 2008. A versão atual é de outubro de 2018. (ADAMS *et al.*, 2018).

Principais componentes, de acordo com (NCDCR, 2019):

a) Pacote

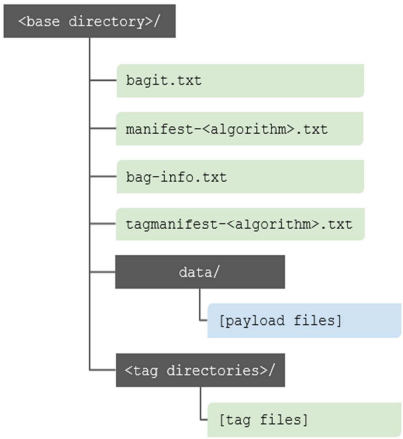
Um pacote consiste em uma “carga útil” e “tags” (etiquetas). O conteúdo da carga útil é o foco de custódia do pacote e é tratada como semanticamente opaco. As "*tags*" são arquivos de metadados destinados a documentar e facilitar o armazenamento e a transferência do pacote.

b) Manifest

Um arquivo de carga de “manifest” fornece uma lista completa de cada nome de arquivo de carga, juntamente com um *checksum* correspondente para permitir a verificação da integridade dos dados.

Um ou mais arquivos de carga de “manifest” de *tag* opcionais fornecerão uma listagem completa de cada nome de arquivo de *tag* com um *checksum* correspondente.

FIGURA 29 - Estrutura da especificação BagIt



FONTE: ADAMS *et al.*, 2018

Outros arquivos de *tags:*

a) O arquivo "bagit.txt" é um arquivo de *tag* obrigatório que contém a versão BagIt que o pacote utiliza e a codificação dos caracteres do arquivo de *tag*;

b) O arquivo "bag-info.txt" é um arquivo de *tag* opcional que contém elementos de metadados que descrevem o pacote e a carga útil;
c) Os elementos de metadados contidos no arquivo "bag-info.txt" são destinados principalmente ao uso humano;
d) *payload files* consiste na carga útil.

c) Validação

Um pacote completo deve atender aos seguintes requisitos:

a) Os elementos necessários devem estar presentes (declaração do pacote, diretório de carga útil, *manifest* de carga útil);
b) Todo arquivo listado em cada etiqueta e manifesto de carga útil deve estar presente.

Um pacote válido deve atender aos seguintes requisitos:

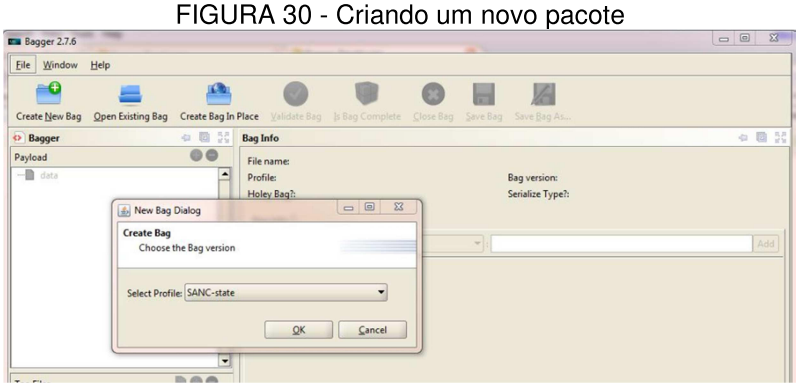
a) O Pacote deve estar completa;
b) Todo o *checksum* em cada etiqueta e *manifest* de carga útil foi verificado com sucesso.

d) Criando um novo pacote

Na tela principal do aplicativo Bagger, clique em "*Create New Bag*".

Surgirá uma pequena caixa de diálogo que lhe pede para selecionar um perfil. Cada perfil corresponde a um modelo de metadados de um determinado órgão americano. Clique OK.

FIGURA 30 - Criando um novo pacote

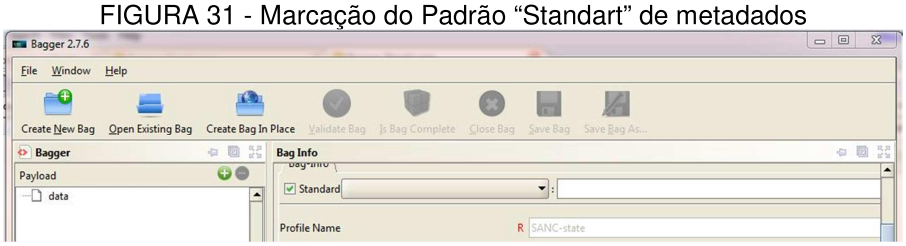


FONTE: Desenvolvido pelo autor.

O painel do lado direito da interface mostra uma lista de metadados a serem preenchidos. Os campos marcados com um "R" vermelho são obrigatórios.

A caixa “*Standart*”, com um letra “V” verde, permite a escolha de campos metadados específicos pré-configurados a inserir. Se desmarcada, permite que sejam criados novos campos de metadados.

FIGURA 31 - Marcação do Padrão “Standart” de metadados



FONTE: Desenvolvido pelo autor.

e) Adicionando carga ao Pacote

Para adicionar arquivo, há dois caminhos: Clique no botão verde “Adicionar dados” ou vá para Arquivo> depois, Adicionar dados...

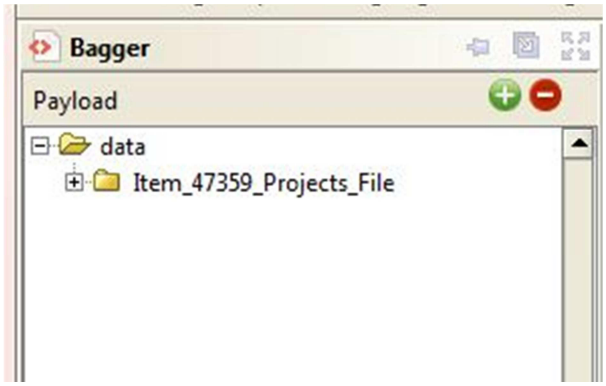
FIGURA 32 - Adição de Carga ao Pacote

FONTE: Desenvolvido pelo autor.

Selecione o botão “Open” para colocar suas seleções no Pacote. (Observação: Quando você clica em “Open”, nada acontece com os arquivos). Eles continuarão em seus locais de origem, sem nenhuma alteração. Você está simplesmente preparando uma lista, e ainda pode adicionar e remover arquivos, livremente, nesta etapa.

Os novos arquivos aparecerão na seção “Payload” à esquerda:

FIGURA 33 - Adição de Carga ao Pacote



FONTE: Desenvolvido pelo autor.

f) Salvando o Pacote

- Clique no botão "*Save Bag As*".

- Certifique-se de que o manifesto de etiquetas e as caixas de manifesto de carga útil estejam marcados e ajustados para o algoritmo desejado:

- Clique no botão "*Browse*" e navegue até a pasta desejada no disco rígido externo. Na caixa "File name", digite o nome do Pacote. Este será o título da pasta que carrega o Pacote.

Observação: Use o botão "*Browse*" para navegar para o local correto e depois digite o nome do pacote, em vez de simplesmente digitar o caminho no campo "*Save in*", como Bagger encontrará um erro e não será capaz de salvar a pacote.

Siga essas regras ao nomear um pacote:

a) Sempre termine o nome do pacote com _bag;
b) Substituir todos os espaços vazios por sublinhados (Easley_Exec_Orders em vez de Easley Exec Orders).

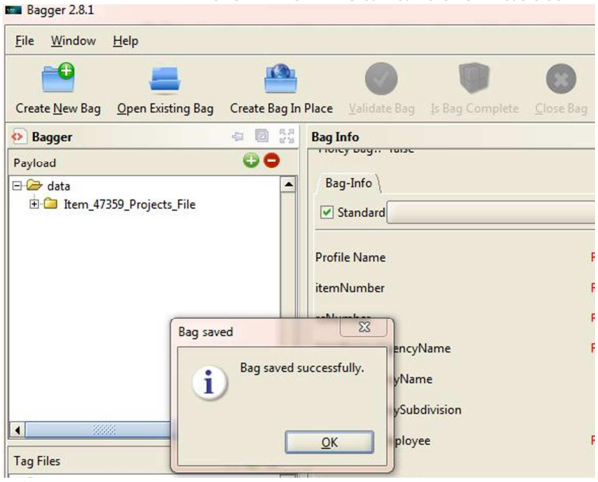
Clique OK para começar a guardar o pacote. Depois de clicar em OK, Bagger irá primeiro verificar os arquivos originais, depois copiar os arquivos para o disco rígido.

Nota: Após clicar em OK para salvar a pacote, se você passar o cursor sobre o Bagger, o cursor aparecerá ocupado. Isso irá continuar até que o Bagger tenha terminado o *checksum* dos arquivos. Quando o Bagger começar a copiar os arquivos, uma barra de progresso surgirá e o cursor voltará ao normal. Não se preocupe se o Bagger permanecer

com a barra de progresso por um longo período de tempo. Significa que está sendo realizado o*checksum* dos arquivos.

Uma vez que o pacote tenha sido salvo, uma janela *pop-up* aparecerá:

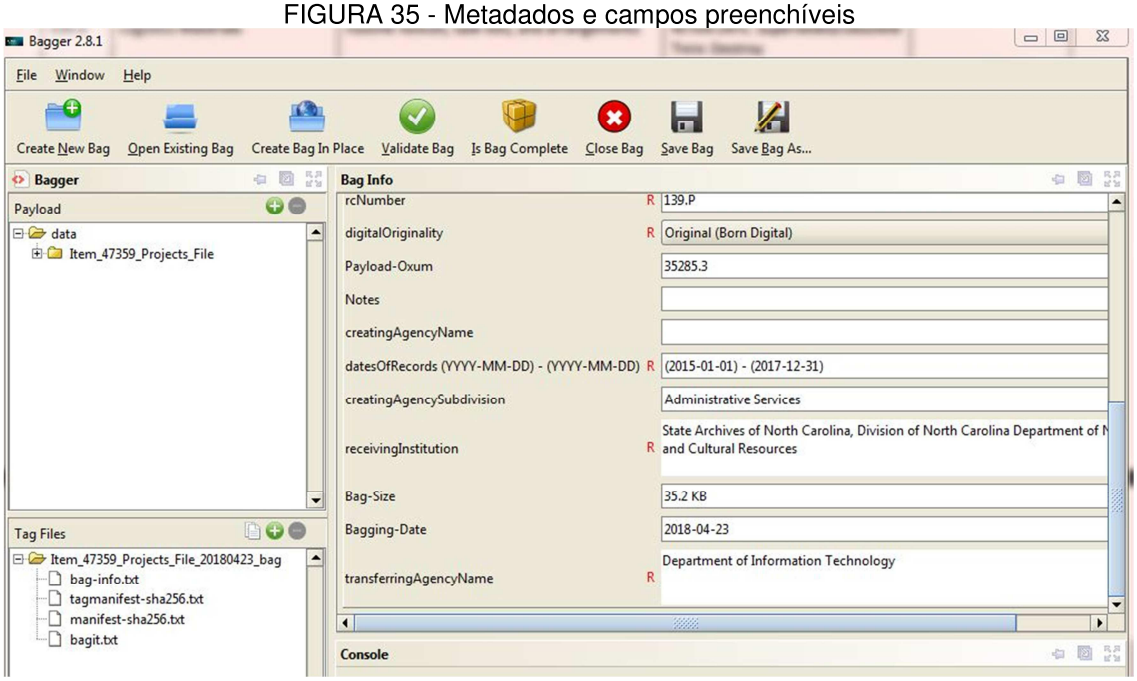
FIGURA 34 - Salvando o Pacote



FONTE: Desenvolvido pelo autor.

Clique em OK na janela pop-up. A janela pop-up irá desaparecer e a janela principal exibirá informações sobre o novo pacote:

FIGURA 35 - Metadados e campos preenchíveis



FONTE: Desenvolvido pelo autor.

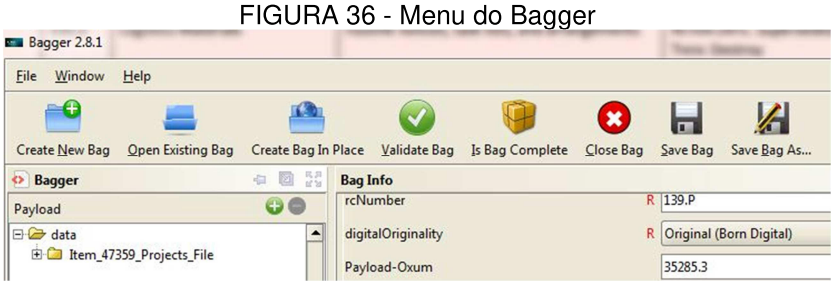
g) Registro do tamanho do pacote

Na FIGURA 34 , é possível notar duas informações importantes:

a) o tamanho do Pacote, que pode ser encontrada no Bagger como "*Bag-Size*" (tamanho do pacote);

b) o número de arquivos na carga útil do pacote, que pode ser encontrado no Bagger nos numerais após o período, no "Payload-Oxum". Por exemplo, na tela copiada abaixo, o payload-oxum era 35285.3. Assim, havia 3 arquivos neste pacote.

FIGURA 36 - Menu do Bagger



FONTE: Desenvolvido pelo autor.

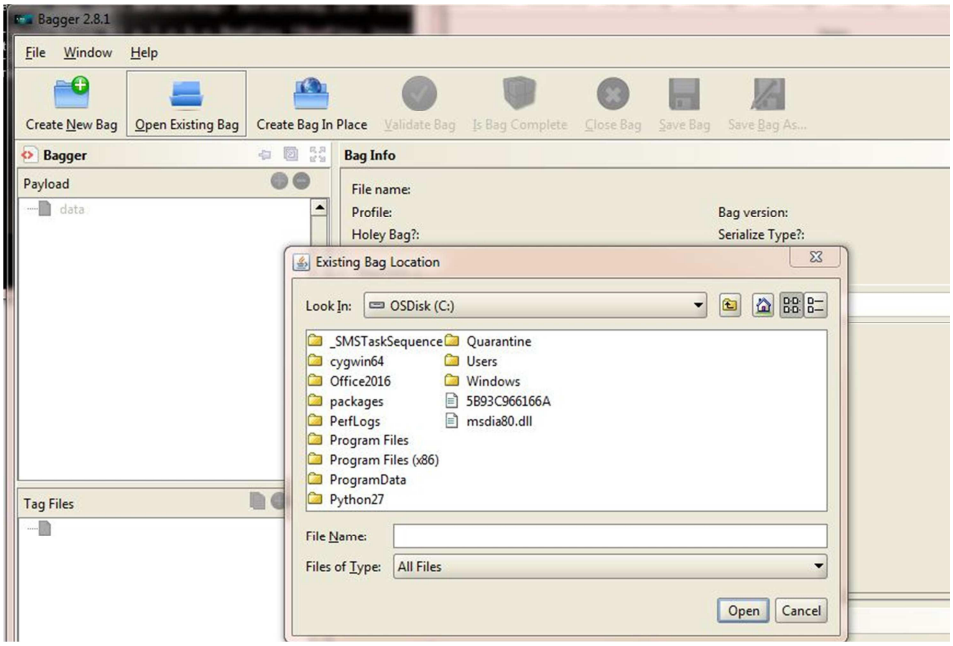
h) Validação de uma pacote

Imediatamente após a criação de um pacote, é recomendada a sua validação para autenticar que o pacote foi criada com sucesso.

i) Abrindo um pacote existente

Na tela principal do Bagger, clique em “Open Existing Bag”. Uma janela pop-up aparecerá:

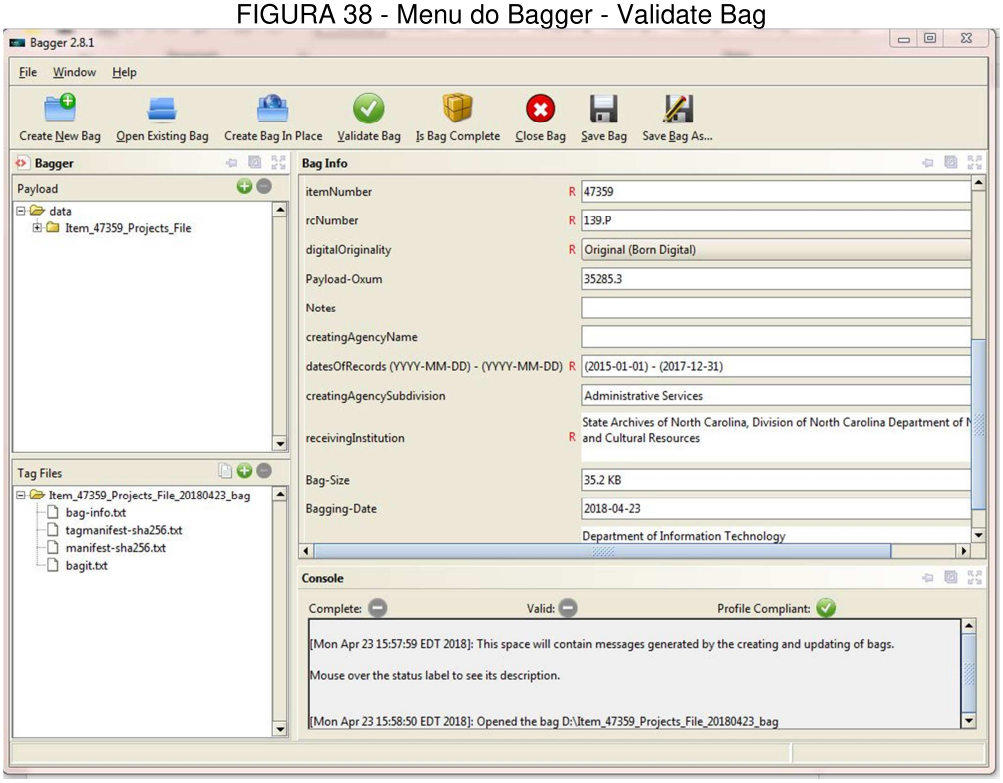
FIGURA 37 - Buscando o pacote no local selecionado



FONTE: Desenvolvido pelo autor.

Navegue até o pacote que você gostaria de validar e clique em "*Open*". O pacoteaparecerá na tela principal:

FIGURA 38 - Menu do Bagger - Validate Bag



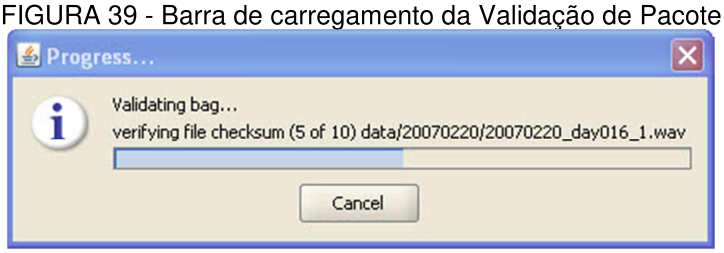
FONTE: Desenvolvido pelo autor.

j)Validar o pacote

Clique em “*Validate Bag*”. O empacotador começará imediatamente a validar a pacote.

Uma janela *pop-up* pode aparecer mostrando o progresso do Bagger:

FIGURA 39 - Barra de carregamento da Validação de Pacote



FONTE: Desenvolvido pelo autor.

l) Verificar resultados

Uma vez concluída a validação, aparecerá uma janela *pop-up* que diz “**Validation successful**”. Clique em OK.

FIGURA 40 - Validação realizada com sucesso

FONTE: Desenvolvido pelo autor.

Observe que a pacote agora tem marcas de verificação verdes, indicando que ela está completa e válida.

m) Fechar Bagger

Após validar a pacote, você pode fechar o empacotador usando o canto superior direito ou clicando em Fechar pacote:

FIGURA 41 - Fechando o pacote

FONTE: Desenvolvido pelo autor.

Procedimentos de responsabilidade do Arquivo da Instituição receptora do pacote SIP

Ação nº1: Recepção e varredura por antivírus

Receber o pacote SIP transmitido pelo Produtor e promover a análise por varredura, por meio do software antivírus e quarentena por trinta dias em área de armazenamento seguro, antes de ser efetuada a admissão (*ingest*) no RDC-Arq.

O registro digital precisa ser colocado em quarentena para garantir que outros registros ingeridos não serão infectados com nenhum vírus ou código malicioso. Todo

registro transmitido a um repositório arquivístico digital confiável deve ser colocado em quarentena em um servidor separado ou em localização na rede, por até trinta dias antes de ser realmente admitido no repositório. Esse tempo é necessário para que programas de varredura de vírus atualizem seus de bancos de dados de detecção de vírus, garantindo assim que todos os vírus possam ser detectados e removidos. (IRMT, 2016).

Ferramentas recomendadas: Antivirus AVG, Avast, Panda.

Ação nº2 - Validação do Pacote SIP por meio de comparação *checksum* do pacote SIP transferido.

O processo de validação irá analisar a integridade dos dados que compõem os objetos digitais do pacote SIP, realizando *checksums* e gerando *hashes* criptográficos que serão comparados aos gerados pelo produtor. Se forem idênticos, o objeto digital transmitido pelo Produtor será idêntico recebido pelo Arquivo, indicando que a cadeia de *bits* original foi mantida integra.

Ferramentas recomendadas: Md5checker, Fsum Frontend

Ação nº3 - Verificação de funcionalidade, integridade, formato

Os registros deverão ser novamente testados para assegurar que qualquer redução ou alteração na funcionalidade, ou perda de conteúdo, estrutura ou formato, sejam detectados antes do *ingest* no RDC-Arq

Ferramentas recomendadas para verificar a funcionalidade: Leitores de PDF (Exemplos: Foxit Reader, Acrobat Reader) e software de imagem que leia PNG (Exemplo: Irfan view).

Ferramentas recomendadas para verificar a integridade: Md5checker, FsumFrontend.

Ferramentas recomendadas para verificar a formato: DROID; VERApdf.

Se a funcionalidade dos registros não puder ser atestada, o processo de preservação terá de ser repetido em novas duplicatas dos registros da fonte.

Serão verificados também, pelo Arquivo, se o formato do arquivo do objeto digital está em conformidade com o Decreto 10.278/2020.

Caso sejam detectadas inconsistências, o Arquivo deverá contatar o Produtor e orientar novo envio de SIP, com as necessárias correções, até que seja alcançado êxito na transmissão de um objeto digital integro e em conformidade com as normativas.

Ação nº4 - Identificação de cada documento arquivístico digitalizado a ser transmitido através um identificador único persistente.

As plataformas de preservação arquivística digital Archivematica e RODA possuem funcionalidades capazes de gerar identificadores únicos persistentes aos documentos arquivísticos digitais que são admitidos no processo de *ingest*.

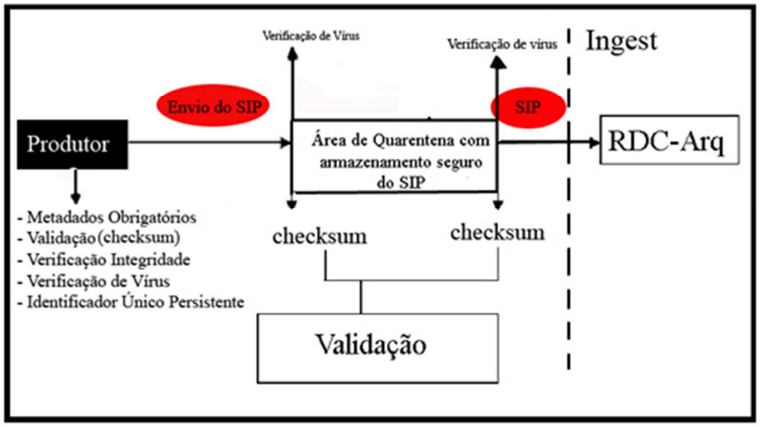
Ação nº5 - Execução de nova verificação de integridade e nova varredura por software antivírus antes da efetivação do *ingest*

O Arquivo deverá, ao final do período de quarentena, executar novo checksum e nova varredura por software antivírus, antes de permitir o ingest do objeto digital no RDC-Arq. Essas ações garantem a segurança do RDC-Arq quanto a códigos maliciosos e vírus e asseguram que o objeto digital apresenta-se integro após o período de quarentena, pronto para o ingest no RDC-Arq.

Ferramentas recomendadas para verificação de integridade: Md5checker, Fsum Frontend.

Ferramentas recomendadas para verificação de códigos maliciosos: AVG, Avast, Panda.

FIGURA 42 - Processo de transmissão do pacote SIP do Produtor ao Arquivo



FONTE: IRMT (2016, p. 75). Adaptado.

7 CONCLUSÃO

Na presente pesquisa, realizaram-se as análises e investigações que buscaram cumprir o Objetivo Geral e os Objetivos Específicos, elencando abaixo as conclusões abstraídas.

Para cumprir o Objetivo Específico a) Analisar os critérios do Catalogue of Criteria for Trusted Digital Repositories (NESTOR), do Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) e Audit and Certification of Trustworthy Digital Repositories (ACTDR), comparando-os com os requisitos das Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq), foram realizadas comparações entre os requisitos do RDC-Arq e critérios Catalogue of Criteria for Trusted Digital Repositories (NESTOR), do Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) e Audit and Certification of Trustworthy Digital Repositories (ACTDR), observando as semelhanças e diferenças quanto aos agentes das ações de preservação, quanto às ações de preservação e quanto aos objetos digitais alvo dessas ações de preservação, elencadas em cada requisito.

Verificou-se que o RDC-Arq baseou-se nos critérios da lista TRAC para elaborar os requisitos para preservação arquivística digital por longos períodos, adaptada ao contexto brasileiro. É importante ressaltar que o RDC-Arq, em várias ocasiões, reestrutura os critérios TRAC de modo a aproximá-lo ao contexto arquivístico, visto que o TRAC visa a alcançar não só acervos arquivísticos, mas também acervos de bibliotecas, museus, bancos de dados de instituições de pesquisa, entidades comerciais e não-comerciais. No Apêndice H, apresenta-se o Quadro Comparativo integral entre os requisitos do RDC-Arq e os critérios TRAC.

Diante das análises realizadas, esta pesquisa conclui que a metodologia TRAC é aquela que exige menor esforço técnico para ser adaptada às Diretrizes do RDC-Arq, no intuito de tornar esta última apta a efetuar autoavaliação, auditoria e certificação em repositórios arquivísticos digitais.

É importante também assinalar a necessidade de utilizar uma metodologia de avaliação de maturidade apropriada a repositórios arquivísticos digitais. A importância dessa avaliação advém do fato de que os requisitos, conforme apresentados no TRAC e no RDC-Arq, apresentam natureza binária. É necessário determinar em que estágio de implementação um dado requisito se encontra, com o objetivo de fornecer aos administradores uma noção exata do estágio em que se encontra e das ações necessárias

para efetivá-lo em sua completude, dimensionando os custos, pessoal, prazos, meios disponíveis, por exemplo.

Verificou-se que OCLC (2007) não detalha o processo de auditoria. Entretanto, as instituições certificadas disponibilizam a documentação referente ao processo de suas certificações.

A ferramenta *DRUPAL TRAC Review*, desenvolvida pelo *Massachusetts Institute of Technology* (MIT) em um projeto liderado por Nancy McGovern, Diretora de Preservação de Bibliotecas de Digitais, consiste em uma ferramenta de auditoria para avaliar a confiabilidade, comprometimento e prontidão das instituições para assumir responsabilidades de preservação em longo prazo. Essa ferramenta, em razão de suas características *open-source,* pode ser trabalhada por pesquisadores e ter seu código-fonte alterado. Dessa forma, pode ser traduzida e adaptada ao RDC-Arq, observando as alterações em critérios pontuados nesta pesquisa. Assim, conclui-se que esta é a maneira mais rápida e sem custos para tornar o RDC-Arq apto para autoavaliação e certificação.

Verificou-se que os critérios do Catálogo de Critérios NESTOR apresentam uma abrangência conceitual mais ampla que os demais modelos de requisitos investigados, neste estudo. Apesar do número reduzido de critérios, se comparado aos demais modelos de requisitos e critérios, um critério NESTOR pode encaixar-se, conceitualmente, em mais de um requisito do RDC-Arq. No Apêndice J, apresenta-se o Quadro Comparativo integral entre os requisitos do RDC-Arq e os critérios NESTOR, traduzidos.

Outra observação é que os critérios NESTOR são definidos com maior precisão em relação aos critérios do RDC-Arq, pois elas incluem elementos como título do critério, explicação geral sobre o critério, exemplos, comentários e notas para o uso em diferentes áreas de aplicação (arquivos, bibliotecas, museus, etc.), e bibliografia relacionada com o critério.

Verificou-se que Grupo NESTOR disponibiliza vasta documentação em seu website, com literatura relativa à temática da preservação digital por longos períodos em língua germânica e com algumas publicações em língua inglesa. Esse grupo não apresentou nenhum software específico para a mensuração da sua maturidade, entretanto, apresentou, em sua metodologia de auditoria e certificação, meios de verificar o estágio de maturidade de implementação de requisitos.

Observou-se que o Grupo de Trabalho NESTOR desenvolveu procedimentos de autoavaliação para a obtenção do Selo NESTOR para Arquivos Digitais Confiáveis. Denominados Critérios avaliativos para a Certificação com o Selo NESTOR, Harmsen *et al.*

(2013) apresentam 34 critérios avaliativos para submissão junto aos arquivos digitais das instituições que desejam o selo NESTOR.

Concluiu-se, nesta pesquisa que, embora os critérios NESTOR não sejam tão conceitualmente similares aos requisitos do RDC-Arq quanto os critérios TRAC, o Catálogo de Critérios NESTOR apresenta elementos que podem ser aproveitados em futuras atualizações das Diretrizes do RDC-Arq como os campos bibliográficos, notas de aplicação e comentários e exemplos.

No presente estudo, verificou-se que há similaridade conceitual parcial entre os requisitos do RDC-Arq e os critérios do ACTDR. Concluiu-se que, apesar de aparentemente requerer um maior esforço para que sejam empreendidas ações de autoavaliação, auditorias e certificação, no ACTDR, apresentam-se critérios bastante detalhados, o que auxilia no entendimento e avaliação dos critérios. No Apêndice I, apresenta-se o Quadro Comparativo integral entre os Requisitos do RDC-Arq e os critérios ACTDR, traduzidos.

Verificou-se também que o ACTDR dispõe de uma ferramenta de avaliação de maturidade dos requisitos denominada *Digital Preservation Capability Maturity Model* (DPCMM). O objetivo do DPCMM é, segundo Ashlley e Dollar (2015), fornecer aos profissionais um modelo de processo integrado e uma ferramenta de planejamento de casos comerciais para ajudar na avaliação comparativa e na melhoria das capacidades de preservação digital. Para auxiliar, neste processo, Ashlley e Dollar (2020) desenvolveram e disponibilizaram, gratuitamente, a ferramenta *Digital Preservation Capability Self-Assessment,* que fornece os meios para que organizações individuais e repositórios possam comparar suas capacidades atuais para gerenciar e preservar registros eletrônicos de longo prazo, apoia o desenvolvimento de planos de melhoria e promove a colaboração e a troca de informações sobre boas práticas. (ASHLLEY; DOLLAR, 2020).

Por fim, conclui-se que, pelo fato do ACTDR ser a base conceitual da Norma ISO 16363, a observação de seus critérios por um repositório digital torna-o mais próximo da certificação num padrão internacional amplamente aceita. Entretanto, é necessário fazer adaptações ao RDC-Arq, semelhantes às desenvolvidas por Santos (2018) em seu trabalho denominado *Manual para Auditoria de Repositórios Arquivísticos Digitais Confiáveis*, visando a tornar um RDC-Arq auditável segundo os parâmetros da ISO 16363.

Não se encontraram publicações que detalhassem o processo de certificação utilizando a lista de critérios ACTDR. Entretanto, verificou-se, de acordo com ISO (PTAB, 2020), que a primeira organização no mundo a receber o credenciamento ISO 16363 para

Repositórios Digitais Confiáveis é o *Primary Trustworthy Digital Repository Authorisation Body Ltda* (PTAB).

O modelo desenvolvido por Ashley e Dollar (2015) intitulado *Digital Preservation Capability Maturity Model* (DPCMM), demonstrou ser uma opção viável para auxiliar os profissionais a identificar, em um alto nível, as capacidades de sua organização em relação às capacidades ideais de preservação digital, a fim de traçar a evolução de gerenciamento desorganizado e indisciplinado de registros digitais para estágios cada vez mais maduros de capacidade de preservação digital. (KATUU, 2013).

Os mesmo autores do DPCMM elaboraram e disponibilizaram, gratuitamente, a ferramenta *Digital Preservation Capability Self-Assessment, cujo* objetivo, segundo Ashley e Dollar (2015), é fornecer os meios para que organizações individuais e repositórios possam comparar suas capacidades atuais para gerenciar e preservar registros eletrônicos a longo prazo, apoiar o desenvolvimento de planos de melhoria e promover a colaboração e a troca de informações sobre boas práticas.

Quanto ao cumprimento do Objetivo Específico b) Elaborar um modelo conceitual híbrido, fruto das análises dos três modelos de requisitos supracitados, de forma a propor um formulário para autoavaliação de repositórios arquivísticos digitais confiáveis, adaptado ao contexto brasileiro e que possa subsidiar futuras atualizações do RDC-Arq, concluiu-se que não será necessário propor um formulário para autoavaliação e auditoria voltada para RDC-Arqs, uma vez que, o RDC-Arq apresenta-se, conceitualmente, muito semelhante à lista de critérios TRAC. Dessa forma, após realizar a tradução da Lista de Verificação TRAC e compará-los aos requisitos do RDC-Arq, concluiu-se que pode ser utilizada a ferramenta *DRUPAL TRAC Review* em conjunto com os requisitos do RDC-Arq, tendo em mente que devem ser observados os critérios e requisitos abaixo destacados.

Por fim, para cumprir o objetivo específico letra c: Investigar como proceder a transmissão do Pacote de Submissão de informação ao RDC-Arq, observando o disposto no Decreto nº 10.278/2020 e, simultaneamente, apoiando-se nas experiências internacionais de instituições voltadas para a preservação digital, por longos períodos, objetivando a proposição de procedimentos técnicos apropriados à preservação arquivística digital no contexto brasileiro, verificou-se que o Decreto 10.278/2020 não especificou o tipo de PDF/A que deve ser utilizado quando da captura pelo aparelho de digitalização. Essa questão deve ser abordada, sendo que há diferentes tipos de PDF/A, com características distintas. Nesta pesquisa, julga-se que sejam observadas as recomendações da Orientação Técnica nº 4 -

Recomendações de uso do PDF/A para Documentos Arquivísticos que, de acordo com CONARQ (2016), apresenta recomendações gerais sobre o uso do formato PDF/A na produção e no arquivamento de documentos arquivísticos digitais.

Quanto à compressão de arquivo sem perda de informação, o Decreto 10.278/2020 não definiu os algorítimos de compressão para essa tarefa. Assim, recomenda-se que, até que se definam os algorítimos de compressão adequados, por meio de experimentos científicos, os arquivos e pacotes de submissão de informação não sejam comprimidos.

Quanto às funções de *hash* criptográficos a serem adotadas, não se definiu, no Decreto 10.278/2020, quais as funções de hash criptográfico permitidas, nem as situações em que cada uma deva ser utilizada, ou em que casos serão necessários níveis mais elevados de colisão criptográfica.

O Decreto 10.278/2020 não faz menção à utilização dos formatos ***T**agged **I**mage **F**ile **F**ormat* (TIFF) e JPEG2000, sendo que ambos apresentam vantagens e pontos fracos que podem influenciar diretamente a preservação por longos períodos.

Quanto aos metadados necessários à preservação digital, por longos períodos, o Decreto 10.278/2020 estabeleceu metadados mínimos obrigatórios, porém, seu número é muito reduzido em relação aos padrões de metadados de preservação digital existentes, o que permite concluir, sem mesmo que seja feita uma investigação, que esses metadados são insuficientes para a preservação arquivística digital por longos períodos.

Desta feita, nesta pesquisa, recomenda-se que sejam utilizados, desde a captura e criação do objeto digital pelo Produtor, os padrões de metadados citados abaixo e que deverão ser previamente estabelecidos no Acordo de Aceitação, estabelecidos entre Produtor e Arquivo, com o intuito de prover o objeto arquivístico digital de metadados adequados à sua descrição, gestão, preservação e difusão:

a) Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos -E-Arq - Brasil. Observar os metadados relativos ao Documento; Classe; Agente; Componente Digital e Ação de Preservação. Sugere-se, aqui, que cada instituição estabeleça, por meio de seu corpo arquivístico, os metadados que deverão compor, obrigatoriamente, o objeto arquivístico digital.
b) Metadados da Norma Brasileira de Descrição Arquivística (NOBRADE) - Utilizar, ao menos, os metadados obrigatórios reomendados pela publicação;

Quanto aos softwares criadores de Pacotes de Submissão de Informação,foi analisado o software Bagger.

O Bagger apresenta-se em língua inglesa e verificou-se uma versão em alemão, denominada Sigfried.

Para a inserção de metadados, são oferecidos formulários pré-definidos, mas nenhum com padrões internacionais. Os metadados foram criados, por exemplo, pelo *Indiana Archives and records administration,*da *Indiana University*.

O Bagger apresenta uma função de Validação do pacote SIP, sem necessidade de produzir classificação em formato JAVAScript Object Notation - JSON. Os metadados podem ser introduzidos um a um, no formulário-padrão. O Bagger apresenta, também, uma configuração de Pacotes SIPs: BagIt.

Recomenda-se, ainda, que o Bagger seja traduzido para a língua portuguesa, ação suportada pelo seu código-fonte aberto.

Enfim, espera-se que esta pesquisa auxilie os arquivistas nas atividades de autoavaliação, auditoria e futuras ações de certificação de repositórios arquivísticos digitais confiáveis brasileiros, pautadas nas experiências e técnicas apresentadas por modelos internacionais de auditoria e certificação de repositórios digitais. Tencionou-se aqui, também, sugerir procedimentos para a transmissão de documentos arquivísticos digitalizados, observando o imposto pelo Decreto 10.278/2020 e, ao mesmo tempo, utilizando métodos internacionalmente consagrados por instituições de preservação digital no longo prazo.

REFERÊNCIAS

ADAMS, C. *et al.* **The BagIt file packaging format (V1.0)**. Califórnia: IETF Trust, 2018. Disponível em: <https://tools.ietf.org/html/rfc8493^>. Acesso em: 18 jan. 2021.

ARELLANO, Miguel Ángel Márdero. **Critérios para a preservação digital da informação científica.** 2008. 356f. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília.

ARELLANO, Miguel Ángel Márdero. Preservação de documentos digitais. **Ciência da Informação**, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004.

ASHLEY, Lori; DOLLAR, Charles. **Digital Preservation Capability Maturity Model (DPCMM).** [S.l.: s.n.], 2015. 62 p. Disponível em: http://static1.squarespace.com/static/52ebbb45e4b06f07f8bb62bd/t/559bf956e4b06cac7e905011/1436285270565/DPCMM+Background+and+Performance+Metrics+v2.7_July+2015.pdf. Acesso em: 15 jan. 2021.

ASHLEY, Lori; DOLLAR, Charles. Digital preservation capability self-assessment. **DigitalOK**, [s.n.], 2020. Disponível em: <http://www.digitalok.org//Login.aspx>. Acesso em: 15 jan. 2021.

ASSOCIATION FOR LIBRARY COLLECTIONS & TECHNICAL SERVICES (ALCTS). **Definitions of digital preservation**. Washington: ALCTS, 2007. Disponível em: <http://www.ala.org/alcts/resources/preserv/defdigpres0408>. Acesso em: 27 nov. 2020.

BAGGIO, Claudia Carmem; FLORES, Daniel. Documentos Digitais: preservação e estratégias. **BIBLOS - Revista do Instituto de Ciências Humanas e da Informação**, Rio Grande, v. 27, n. 1, p. 11-24, jan./jun. 2013.

BARBEDO, Francisco; CORUJO, Luís; SANT'ANA, Mário. **Recomendações para a produção de Planos de Preservação Digital**. Lisboa: DGARQ, 2011. 111p.

BEAGRIE, Neil *et al.* **Digital preservation policies study**. **Part 1:** final report. [S.l.]: HEFCE, 2008. 60p.

BERG-CROSS, Gary *et al.* **Data Foundation and Terminology DFT 3:** snapshot of DFT Core Terms. [S.l.]: Research Data Alliance, 2015. 19p.

BERGMEYER, Winfried et al. **Catalogue of criteria for trusted digital repositories:** version 2. Frankfurt am Main: Nestor Working Group Trusted Repositories Certification, 2009. 53p.

BERZ, Dominic *et al.* Comparison of lossless data compression methods. **Technical Reports in Computing Science**, Kempten, n. CS-07, p. 1-12, 2015.

BRASIL. Decreto 10.278 de 18 de março de 2020. Regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais. **Diário Oficial da União**, DF, mar. 2020.

Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10278.htm>. Acesso em: 15 jan. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o código civil. Brasília: Presidência da República, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em: 15 jan. 2021.

BRASIL. Lei nº 13.874, de 20 de setembro de 2019. Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado; altera as Leis nºs 10.406, de 10 de janeiro de 2002 (Código Civil), 6.404, de 15 de dezembro de 1976, 11.598, de 3 de dezembro de 2007, 12.682, de 9 de julho de 2012, 6.015, de 31 de dezembro de 1973, 10.522, de 19 de julho de 2002, 8.934, de 18 de novembro 1994, o Decreto-Lei nº 9.760, de 5 de setembro de 1946 e a Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943; revoga a Lei Delegada nº 4, de 26 de setembro de 1962, a Lei nº 11.887, de 24 de dezembro de 2008, e dispositivos do Decreto-Lei nº 73, de 21 de novembro de 1966; e dá outras providências. **Diário Oficial da União**, DF, set. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm>. Acesso em: 15 jan. 2021.

BRITZ, Marjie. **Computer forensics and cyber crime:** an introduction. 3.ed. Clemson: Pearson, 2013. 408p.

CAPLAN, Priscilla; KEHOE, William; PAWLETKO, Joseph. Towards Interoperable Preservation Repositories (TIPR). **International Journal of Digital Curation**, Bath, v. 5, n. 1, p. 34-45, Mar. 2010.

CARVALHO, José. Auditoria ISO 16363 a repositórios institucionais. In: CONGRESSO NACIONAL BAD, 12., 2015, Évora. **Anais...** Évora: BAD, 2015. p. 29-39.

CENTER FOR RESEARCH LIBRARIES (CRL). **Certification and assessment of digital repositories.** Chicago: CRL, 2021. Disponível em: <https://www.crl.edu/archiving-preservation/digital-archives/certification-assessment>. Acesso em: 15 jan. 2021.

CHEN, Su-Shing. The paradox of digital preservation. **Computer**, Oxford, v. 34, n. 3, p. 24-28, Mar. 2001.

CHOY, Sara C. C. *et al.* **Guidelines for the selection of digital heritage for long term preservation**. Washington, DC: UNESCO, 2016. 19p.

COMMITTEE ON ELECTRONIC RECORDS. **Guide for managing electronic records from an archival perspective**. Paris, France: ICA, 1997. 58p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos. **Orientação Técnica nº 4, outubro de 2016.** Rio de Janeiro: CONARQ, 2016. 13p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Carta para a Preservação do Patrimônio Arquivístico Digital:** preservar para garantir o acesso. Rio de Janeiro: CONARQ, 2004. 5p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: CONARQ, 2005. 232p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Glossário:** documentos arquivísticos digitais. Rio de Janeiro: CONARQ, 2020. 62p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Orientação Técnica nº 3:** cenários de uso de RDC-Arq em conjunto com o SIGAD. Rio de Janeiro: Arquivo Nacional, 2015b. 8 p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Requisitos para a Implementação de Repositórios Arquivísticos Digitais Confiáveis - RDC-Arq.** Rio de Janeiro: CONARQ, 2015a. 31p.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Resolução nº 31, de 28 de abril de 2010. Dispõe sobre a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes. **Diário Oficial da União**, DF, 3 maio 2010. Seção 1, nº 82.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Audit and certification of trustworthy digital repositories.** Washington: CCSDS Secretaria, 2011. 77p.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **CCSDS charter.** Washington: CCSDS, 2004a. Disponível em: <https://public.ccsds.org/about/charter.aspx>. Acesso em: 14 jan. 2021.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **CCSDS histroy.** Washington: CCSDS, 2020. Disponível em: <https://public.ccsds.org/about/history.aspx>. Acesso em: 14 jan. 2020.

CONSULTIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS**).** **Producer-archive interface methodology abstract standard**. Washington: CCSDS Secretaria, 2004b. 72p.

CONSULTIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS). **Reference model for an Open Archival Information System (OAIS).** Washington: CCSDS Secretaria, 2012. 135p.

CORUJO, Luis Miguel Nunes. **Repositórios digitais e confiança**: um exemplo de repositório de Preservação Digital: o RODA. 2014. 255f. Dissertação (Mestrado em Ciências da Documentação e Informação) - Faculdade de Letras, Universidade de Lisboa, Lisboa.

DEEPL. 2020. Disponível em: <www.DeepL.com>. Acesso em: 16 jan. 2021.

DELMAS, Bruno. Por uma Diplomática contemporânea: novas aproximações. In: CAMARGO, Ana Maria de Almeida et al. **Dar nome aos documentos:** da teoria à prática / apresentação de Danielle Ardaillon. São Paulo: Instituto Fernando Henrique Cardoso, 2015. p. 32-56.

DIGITAL PRESERVATION COALITION (DPC). **Fixity and checksums**. Glasgow: DPC, 2020. Disponível em: <https://www.dpconline.org/handbook/technical-solutions-and-tools/fixity-and-checksums>. Acesso em: 15 jan. 2021.

DOBRATZ, Susanne; SCHOGER, Astrid. Digital Repository Certification: a report from Germany. **RLG DigiNews**, Berlin, p. 1-8, 2005.

DOBRATZ, Susanne; SCHOGER, Astrid; STRATHMANN, Stefan. The NESTOR Catalogue of Criteria for trusted digital repository evaluation and certification. **Digital Curation & Trusted Repositories**, Cincinnati, v. 8, n. 2, 2007. Disponível em: <https://journals.tdl.org/jodi/index.php/jodi/article/view/199/180>. Acesso em: 14 fev. 2020.

DURANTI, Luciana (Ed.). **The long-term preservation of authentic electronic records**: findings of the InterPARES Project. [S.l.]: Archilab, 2005. 364p.

DURANTI, Luciana. Registros documentais contemporâneos como provas de ação. **Estudos Históricos**, Rio de Janeiro, v. 7, n. 13, p. 49-64, 1994.

DURANTI, Luciana. The long-term preservation of accurate and authentic digital data: the interpares project. **Data Science Journal**, Taipei, v. 4, p. 106-118, Oct. 2005.

EISENHOWER, Dwight D. **Crusade in Europe**. Melbourne: William Heineman, 1948. 634p.

FACHIN, Odília. **Fundamentos de metodologia**. 5.ed. rev. e atual. São Paulo: Saraiva, 2005. 200p.

FARIA, Luís Francisco da Cunha Cardoso de. **Automated watch for digital preservation**. 2017. 156f. Thesis (Doctoral Program on Informatics) - Universidade do Minho, Minho.

FERREIRA, Miguel. **Introdução à preservação digital**: conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. 88p.

FLORES, Daniel; HEDLUND, Dhion Carlos. A preservação do patrimônio documental através da produção de instrumentos de pesquisa arquivísticos e da implementação de repositórios arquivísticos digitais. **Série Patrimônio Cultura e Extensão Universitária**, Brasília, n. 3, p. 3-31, fev. 2014.

FLORES, Daniel; PRADEBON, Daiane Segabinazzi; CÉ, Graziella. Análise do conhecimento teórico-metodológico da preservação digital sob a ótica da OAIS, SAAI, ISO 14721 e NBR 15472. **Brazilian Journal of Information Science**: research trends, São Paulo, v. 11, n. 4, p. 72-80, 2017.

GARRETT, John; WATERS, Donald. **Preserving digital information.** Alexandria: Commission on Preservation and Access and The Research Libraries Group, 1996. 64p.

GAVA, Tânia Barbosa Salles; FLORES, Daniel. Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. **Informação & Informação**, Londrina, v. 25, n. 2, p. 74-99, abr./jun. 2020.

GIARETTA, David *et al.* Audit and Certification of Trustworthy Digital Repositories - lessons learned. In: CONFERENCE ON ADDING VALUE AND PRESERVING DATA, 9., 2018, Harwell. **Proceedings…** Harwell: STFD, 2018. p. 163-167.

GONÇALEZ, Paula Regina Ventura Amorim. Recomendações para certificação ou medição de confiabilidade para repositórios arquivísticos digitais confiáveis com ênfase no acesso. **Revista Informação & Informação**, Londrina, v. 22, n. 1, p. 215-241, jan./abr. 2017.

HARMSEN, Henk *et al.* Explanatory notes on the NESTOR Seal for Trustworthy Digital Archives. **NESTOR Seal**, Leibniz, 2013. Disponível em: <https://files.dnb.de/NESTOR/zertifizierung/notes_NESTOR_Seal.pdf>. Acesso em: 15 jan. 2021.

HEDSTROM, Margaret. Digital preservation: a time bomb for digital libraries. **Computers and the Humanities**, Osprey, v. 31, n. 3, p. 189-202, 1997.
HERRERA, Antonia Heredia. **Archivística general:** teoría y práctica. 5. ed. Sevilha: Diputación provincial de Sevilla, 1991. 478p.

HERRERA, Antonia Heredia. Arquivos, documentos e informação. In: DEPARTAMENTO DO PATRIMÔNIO HISTÓRICO. **O direito à memória:** patrimônio histórico e cidadania. São Paulo: DPH, 1992. p. 113-120.

HISTORY ASSOCIATES INCORPORATED (HAI). **Preventing data loss:** steps toward long-term digital preservation. Rockville: HAI, 2020. Disponível em: <https://www.historyassociates.com/preventing-data-loss/>. Acesso em: 18 jan. 2021.

HOBSBAWM, Eric. **Era dos extremos:** o breve século XX (1914-1991). São Paulo: Companhia das Letras, 1995. 245p.
INDOLFO, Ana Celeste; LOPES, Vera Hess. Entrevista com Luciana Duranti. **Acervo**, Rio de Janeiro, v. 28, n. 2, p. 11-18, jul./dez. 2015.

INFLATION calculator. **Dollar Times**, Seattle, 2021. Disponível em: <https://www.dollartimes.com/inflation/>. Acesso em: 15 mar. 2020.

INNARELLI, Humberto Celeste. **Gestão da preservação de documentos arquivísticos digitais:** proposta de um modelo conceitual. 2015. 348f. Tese (Doutorado em Ciência da Informação) - Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo.

INTERNATIONAL COUNCIL ON ARCHIVES - ICA. **Documentos de arquivo electrónicos:** manual para arquivistas. Paris: ICA, 2005. 74p. (Estudo, nº 16).

INTERNATIONAL COUNCIL ON ARCHIVES (ICA). **Guide for managing electronic records from an archival perspective**. Paris: ICA, 1997. 55p.

INTERNATIONAL RECORDS MANAGEMENT TRUST (IRMT). **Digital preservation in lower resource environments:** a core curriculum. Paris: ICA, 2016. 94p.
INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). **The InterPARES Glossary.** Vancouver: InterPARES, 2001a. Disponível em: <www.interpares.org>. Acesso em: 27 nov. 2020.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). **Digital Records Pathways:** topics in digital preservation: module 1: introduction - a framework for digital preservation. Vancouver: InterPARES/ICA, 2012. 63p.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). **TR04 Assessing Information Systems:** a template for analysis. Vancouver: InterPARES, 2018. 10p.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). Authenticity task force report. In: _____. **The long-term preservation of authentic electronic records:** findings of the interpares project interpares. Vancouver: InterPARES, 2020c. Disponível em: http://www.interpares.org/book/interpares_book_d_part1.pdf>. Acesso em: 14 jan. 2021.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (InterPARES). Introduction. In: _____. **The long-term preservation of authentic electronic records:** findings of the interpares project interpares. Vancouver: InterPARES, 2001b. Disponível em: <http://www.interpares.org/book/interpares_book_c_intro.pdf>. Acesso em: 14 jan. 2021.

KAHN, Robert; WILENSKY, Robert. A framework for distributed digital object services. **International Journal on Digital Libraries**, Berlin, v. 6, n. 2, p. 115-123, 2006.

KALLINIKOS, Jannis; AALTONEN, Aleksi; MARTON, Attila. A theory of digital objects. **First Monday**, Washington, v. 15, n. 6-7, p. 1-28, June 2010.

KATUU, Shadrack. The utility of maturity models: the ECM Maturity Model within a South African context. In: BECKER, Christoph; CARDOSO, Elsa. CAPABILITY ASSESSMENT AND IMPROVEMENT WORKSHOP (CAIW), 2013, Lisboa. **Proceedings…** Lisboa; [s.n.], 2013. p. 1-8.

KING, Joseph. **Viking Lander Biology Data Restored by NSSDC and Planetary Data System (PDS)**. Washington: NASA, 2001. Disponível em: <https://nssdc.gsfc.nasa.gov/nssdc_news/sept00/viking_lander.html>. Acesso em: 18 jan. 2021.

LAVOIE, Brian F. **The Open Archival Information System (OAIS) Reference Model:** introductory guide. 2.ed. Glasgow: DPC, 2014. 33p.

LEE, Christopher A. **Defining digital preservation work:** a case study of the development of the reference model for an open archival information system. 2005. 325f. Dissertation (Doctor of Philosophy) - University of Michigan, Michigan.

LIBRARY OF CONGRESS. **PREMIS Data Dictionary for Preservation Metadata, version 3.0.** Washington, 2015. Disponível em: <https://www.loc.gov/standards/premis/v3/index.html>. Acesso em: 14 jan. 2021.

LINDLAR, Michelle; TUNNAT, Yvonne. How valid is your validation? A closer look behind the curtain of JHOVE. **International Journal of Digital Curation**, Bath, v. 12, n. 2, p. 286-298, 2017.

LINDLAR, Michelle; TUNNAT, Yvonne; WILSON, Carl. A PDF Test-Set for Well Formedness Validation in JHOVE - The Good, the Bad and the Ugly. In: INTERNATIONAL CONFERENCE ON DIGITAL PRESERVATION (iPRES2017), 14., 2017, Kyoto. **Proceedings…** Kyoto: iPRES, 2017. p. 1-11.

MARX, Fritz Morstein. The role of records in administration. **The American Archivist**, Chicago, v. 10, n. 3, p. 241-248, July 1947.

MILLAR, Laura (Ed.). **Module 1:** understanding the context of electronic records management. London: IRMT, 2009a. 73p.

MILLAR, Laura (Ed.). **Module 4:** preserving electronic records. London: IRMT, 2009b. 57p.

MOGOLLÓN, Juan Bernardo Montoya; RODRÍGUEZ, Sonia Maria Troitiño. Diplomática Forense: revisão histórica para a abordagem do documento nato-digital de arquivo. **Investigación Bibliotecológica**, México, v. 33, n. 78, p. 47-62, Enero/Mar. 2019.

MONNAPPA, K. A. **Learning malware analysis:** explore the concepts, tools, and techniques to analyze and investigate Windows malware. Birmingham: Packt Publishing, 2018. 512p.

MOORE, Reagan. Towards a theory of digital preservation. **The International Journal of Digital Curation**, San Diego, v. 3, n. 1, p. 63-75, June 2008.

MUNDET, José Ramón Cruz; CARRERA, Carmen Díez. Sistema de Información de Archivo Abierto (OAIS): luces y sombras de un modelo de referencia. **Investigación Bibliotecológica**: archivonomía, bibliotecología e información, México, v. 30, n. 70, p. 221-247, Sept./Dic. 2016.

NASA. **MARS 2020 mission**. Washington: NASA, 2020a. Disponível em: <https://mars.nasa.gov/mars2020/>. Acesso em: 18 jan. 2021.

NASA. **Viking 1 Lander**. **NSSDCA/COSPAR ID:** 1975-075C. Washington: NASA, 2020b. Disponível em: https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id= 1975-075C. Acesso em: 18 jan. 2021.

NATIONAL DIGITAL STEWARDSHIP ALLIANCE (NDSA). **Checking your digital content:** how, what and when to check fixity?. Arlington: NDSA, 2014. 7p.

NC DEPARTMENT OF NATURAL AND CULTURAL RESOURCES. **Bagger GUI user guide:** how to create and validate Bags with Bagger. Estados Unidos: NC, 2019. 25p.

NESTOR. **Network of expertise in long-term storage of digital resources.** [S.l.: s.n.], 2020. Disponível em: <https://www.langzeitarchivierung.de/Webs/nestor/EN/Zertifizierung/nestor_Siegel/siegel.html>. Acesso em: 18 jan. 2021.

NEVES, João Emmanuel D'Alkmin; INNARELLI, Humberto Celeste. Preservação digital: a gestão arquivística de documentos digitais em sua fase permanente. **Revista Tecnológica da Fatec Americana**, Americana, v. 1, n. 1, p. 65-77, mar. 2014.

ONLINE COMPUTER LIBRARY CENTER (OCLC). **Trustworthy repositories audit & certification**: criteria na checklist. Chicago: CRL, 2007. 88p.

OPEN PRESERVATION FOUNDATION. **JHOVE. Software.** Leeds: Open Preservation Foundation, 2015. Disponível em: <http://jhove.openpreservation.org/>. Acesso em: 15 jan. 2021.

PRESERVICA. **Achieving a step change in digital preservation capability:** an assessment of preservica using the digital preservation capability maturity. Boston: Preservica, 2015. 15p.

PRIMARY TRUSTWORTHY DIGITAL REPOSITORY AUTHORISATION BODY (PTAB). **Which repositories are TRUSTWORTHY?.** [S.l.]: PTAB, 2020. Disponível em: <http://www.iso16363.org/>. Acesso em: 15 jan. 2021.

RAMALHO, José Carlos *et al.* RODA-in: a generic tool for the mass creation of submission information packages. In: IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES (CISTI), 12., 2017, Lisboa. **Proceedings...** Lisboa: CISTI, 2017. p. 2316-2324.

RESEARCH LIBRARIES GROUP (RLG). **Attributes of a trusted digital repository:** meeting the needs of research resources. Mountain View, CA: The Research Libraries Group, 2001. 52p.

RLG/OCLC WORKING GROUP ON DIGITAL ARCHIVE ATTRIBUTES. **Trusted digital repositories:** attributes and responsibilities. Dublin: OCLC, 2002. Disponível em: <http://www.rlg.org/longterm/repositories.pdf>. Acesso em: 14 jan. 2021.

ROCHA, Cláudia Lacombe; SILVA, Margareth da. Padrões para garantir a preservação e o acesso aos documentos digitais. **Acervo**, Rio de Janeiro, v. 20, n. 1-2, p. 113-124, jan./dez. 2007.

ROGERS, Corinne. A literature review of authenticity of records in digital systems from ‘machine-readable’ to records in the cloud. **Acervo**, Rio de Janeiro, v. 29, n. 2, p. 16-44, jul./dez. 2016.

RONDINELLI, Rosely Curi. **O documento arquivístico ante a realidade digital**: uma revisão conceitual necessária. Rio de janeiro: Editora FGV, 2013. 280p.

SAMPAIO, Érika Maria Nunes; ABREU, Jorge Phelipe Lira de; REIS, Raquel Dias Silva. Perspectivas da preservação da memória digital brasileira a partir da experiência do Arquivo Nacional. **Revista do Arquivo**, São Paulo, v. 2, n. 6, p. 47-62, abr. 2018.

SANTOS, Henrique Machado dos. Auditoria de repositórios arquivísticos digitais confiáveis. **Informação em Pauta**, Fortaleza, v. 4, n. 2, p. 156-172, jul./dez. 2019.

SANTOS, Henrique Machado dos; FLORES, Daniel. Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 20, n. 2, p. 198-218, abr./jun. 2015.

SANTOS, Henrique Machado dos. **Manual para auditoria de repositórios arquivísticos digitais confiáveis.** 2018. 284f. Dissertação (Mestrado em Patrimônio Cultural) - Centro de Ciências Sociais e Humanas, Universidade Federal de Santa Maria, Santa Maria.

SARAMAGO, Maria Lurdes. Metadados para preservação digital e aplicação do modelo OAIS. **Actas do Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas**, Lisboa, n. 8, p. 1-6, 2004.

SCHLIEDER, Sarah. **NASA's viking data lives on, inspires 40 years later.** Washington: NASA, 2016. Disponível em: <https://www.nasa.gov/feature/goddard/2016/nasas-viking-data-lives-on-inspires-40-years-later>. Acesso em: 18 jan. 2020.

SCHELLENBERG, Theodore Roosevelt. **Arquivos modernos:** princípios e técnicas. Rio de Janeiro: Editora FGV, 1974. 383p.

SHARMA, Vipul; NAAZ MIR, Roohie. Digital preservation and data compression. **International Journal of Computer Science and Technology**, London, v. 9, n. 2, p. 32-43, Apr./June 2018.

THAN, Ker. Life on mars found by NASA's viking mission?. **National Geographic News**, Saint Louis, Apr. 2012. Disponível em: <https://www.nationalgeographic.com/news/2012/4/120413-nasa-viking-program-mars-life-space-science/>. Acesso em: 18 jan. 2021.

THE NATIONAL ARCHIVES. **DROID:** how to use it and how to interpret your results. [S.l.]: Crown, 2011. 36p.

THE NATIONAL ARCHIVES. **DROID:** user guide. [S.l.]: Crown, 2020. 22p.
THE NATIONAL ARCHIVES. **The technical registry PRONOM**. [S.l.: s.n.], 2021. Disponível em: <www.nationalarchives.gov.uk/help/PRONOM/faq.htm#faq1>. Acesso em: 15 jan. 2021.

THE UNIVERSITY OF BRITISH COLUMBIA LIBRARY (UBC). Digital Preservation Compliance Tracking System. **Digitalizacion Centre**, British, 2017. Disponível em: https://wiki.ubc.ca/images/7/7d/Impact-Assessment_2017-18.pdf. Acesso em: 1 dez. 2020.

THIBODEAU, Kenneth. Overview of technological approaches to digital preservation and challenges in comming years. In: THE STATE OF DIGITAL PRESERVATION: AN INTERNATIONAL PERSPECTIVE, 2002, Washington. **Proceedings…** Washington: Institutes for Information Science, 2002. p. 1-31.

THOMASSEM, Theo. Uma primeira introdução à arquivologia. **Arquivo & Administração**, Rio de Janeiro, v. 5, n. 1, p. 5-16, 2006.

THOMAZ, Kátia de Pádua. **A preservação de documentos eletrônicos de caráter arquivístico:** novos desafios, velhos problemas. 2004. 388f. Tese (Doutorado em Ciência da Informação) - Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte.

THOMAZ, Katia de Pádua; SOARES, Antônio José. A preservação digital e o modelo de referência open archival information system (OAIS). **DataGramaZero - Revista de Ciência da Informação**, Rio de Janeiro, v. 5, n. 1, p. 1-17, fev. 2004.

TOGNOLI, Natália Bolfarini. **A construção teórica da Diplomática:** em busca de uma sistematização de seus marcos teóricos como subsídio aos estudos arquivísticos. 2013. 162 f. Tese (Doutorado em Ciência da Informação) - Faculdade de Filosofia e Ciências, Universidade Estadual Paulista Júlio de Mesquita Filho, Marília.

TOGNOLI, Natália Bolfarini. Diplomática: dos diplomas aos documentos digitais. **Revista do Arquivo**, São Paulo, v. 2, n. 6, p. 34-46, abr. 2018.

TRAC review tool. **@rchivematica**, [S.l.], 2007. Disponível em: <https://www.archivematica.org/en/docs/archivematica-1.6/getting-started/other-resources/trac/>. Acesso em: 15 jan. 2021.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO). **Guidelines for the preservation of digital heritage**. Australia: Information Society Division, 2003. 177p.

URI, John. **45 years ago:** viking 1 and 2 off to mars. Washington: NASA Johnson Space Center, 2020. Disponível em: <https://www.nasa.gov/feature/45-years-ago-viking-1-and-2-off-to-mars>. Acesso em: 18 jan. 2020.

VeraPDF. **Desktop GUI quick start guide**. 2020. Disponível em: <https://docs.verapdf.org/gui/>. Acesso em: 15 jan. 2021.

WELCH, Todd; PHILLIPS, Kelly. **Trustworthy Repositories:** Audit and Certification (TRAC) Cline Library Internal Audit. Oxford: Spring, 2014. 95p.

WITT, Michael *et al.* **ISO 16363:** trustworthy digital repository certification in practice. Purdue: Purdue University, 2012. 4p.

ZAZO, José Luis Bonal; LORENZO-CÁCERES, María del Pilar Ortego de. Criterios de certificación y auditoría de repositorios digitales seguros en archivos. In: VAQUINHAS, Nelson; CAXIAS, Marisa; VINAGRE, Helena. **Da produção à preservação informacional:** desafios e oportunidades. Évora: Publicações do Cidehus, 2017. p.529-550.

APÊNDICE A - CATÁLOGO DE CRITÉRIOS PARA REPOSITÓRIOS DIGITAIS CONFIÁVEIS NESTOR - GRUPO DE TRABALHO REPOSITÓRIOS DE CONFIANÇA - CERTIFICAÇÃO[127]

A. Estrutura Organizacional

O repositório digital atua dentro de uma estrutura organizacional que é determinada por objetivos definidos, condições legais e recursos humanos e financeiros disponíveis.

1. O repositório digital definiu os seus objetivos.

   O repositório digital deve ter uma concepção clara dos seus objetivos. Ele determinou quais tarefas cumpre, e quais os princípios que observa em fazê-lo. Isso é crucial, como confiabilidade não é um termo absoluto, mas sim depende dos objetivos do repositório digital em particular. Seguindo o princípio da adequação, avaliação dos critérios individuais é sempre baseada nas metas específicas. O repositório digital garante que os seus objetivos são transparentes para que os outros - especialmente os usuários e produtores - possam avaliar a confiabilidade por si (As metas são muitas vezes publicadas sob a forma de uma Política).

1.1. O repositório digital desenvolveu critérios para a seleção dos seus objetos digitais.

O repositório digital deve ter estabelecido quais objetos digitais se enquadram no seu âmbito. Este é geralmente determinado pela área de tarefas gerais da instituição ou é estipulado por leis. O repositório digital desenvolveu diretrizes de coleta, critérios de seleção, critérios de avaliação ou de geração de patrimônio. Os critérios podem ser baseados em conteúdo, formais ou qualitativos.

1.2. O repositório digital assume a responsabilidade pela preservação no longo prazo da informação representada pelos objetos digitais.

O repositório digital declara, explicitamente, a sua responsabilidade para a preservação, em longo prazo, dos objetos digitais ingeridos como descrito no

ponto 1.1. Preservação em longo prazo aqui significa a retenção permanente da usabilidade das informações representadas pelos objetos digitais (conforme o modelo de informação OAIS).

1.3. O repositório digital definiu suas comunidade(s) designadas(s)

A definição geral do quadro para um repositório digital envolve a definição de comunidade(s) designada(s). Isso inclui conhecimento específico das exigências da comunidade(s) designada(s) que influenciam a seleção dos serviços a serem prestados. Se a comunidade(s) designada(s) ou suas necessidades mudam com o tempo, o repositório digital deve responder adaptando seus serviços.

2. O repositório digital confere a suas comunidade(s) designada(s) acesso adequado para as informações representadas pelos objetos digitais.

O repositório digital deve considerar sua principal tarefa o uso atual e futuro da informação representada pelos objetos digitais por parte de suas comunidade(s) designada(s). O uso dos objetos digitais baseia-se em sua preservação, a sua acessibilidade e na manutenção da capacidade de interpretá-los. O uso pode ser adequado, apesar de poder ser restringido, decorrente das razões legais (conforme 3.3.) ou nem todas as propriedades do original serem preservadas (conforme 9.2.).

2.1. O repositório digital garante que suas comunidade(s) designada(s) podem acessar os objetos digitais.

O repositório digital deve garantir que usuários autorizados tenham acesso aos objetos digitais. Isso inclui possibilidades de pesquisa apropriadas. Ao determinar seu portfólio de serviços, o repositório digital leva as necessidades de suas comunidade(s) designada(s) em conta. O repositório digital anuncia com antecedência as suas condições de utilização e quaisquer custos que possam surgir, listando estes de forma transparente.

2.2. O repositório digital garante que as comunidade(s) designada(s) podem interpretar os objetos digitais.

O repositório digital deve tomar medidas adequadas para garantir que os objetos digitais possam ser interpretados numa base de longo prazo, criando

assim os requisitos básicos para o uso adequado. Isso inclui a capacidade de interpretar o conteúdo e metadados.

No sentido de garantir isso, o repositório digital deve levar as necessidades de suas comunidade(s) designada(s) em conta. Quanto mais especializada(s) as comunidade(s) designada(s), mais *know-how* designado e equipamentos técnicos (por exemplo, um determinado *software*) são necessários, ou quanto maior for a vontade de organizar equipamento adicional (instalação de *plug-ins*) deve ser. Alterações no ambiente técnico ou na(s) comunidade(s) designada(s) podem influenciar a capacidade de interpretar os objetos. O repositório digital, portanto, deve verificar, em intervalos regulares, utilizando procedimentos adequados, se os objetos ainda podem ser interpretados pela(s) comunidade(s) designada(s).

3. São observadas as regras legais e contratuais.

As ações do repositório digital devem ser baseadas em normas legais. Estas abrangem a aquisição dos objetos digitais e também seu arquivamento e uso. Aqui, o repositório digital deve encontrar um equilíbrio entre os interesses legítimos dos produtores, os dos utilizadores e também, se for o caso, dos indivíduos em causa (no caso de dados relacionados à pessoa).

3.1. Existem contratos legais entre os produtores e o repositório digital.

A fim de assegurar o planejamento e segurança jurídica do repositório digital, sempre que possível, deve-se concluir acordos formais com os produtores ou fornecedores. A natureza e âmbito da prestação são reguladas, como são as obrigações do repositório digital de arquivo, as condições de utilização e, quando aplicáveis, os custos. Os acordos legais devem ser complementados com disposições de execução concretas. Se não for possível concluir um acordo formal, deve ser dada razão para isso.

3.2. No desempenho das suas tarefas de arquivamento, o repositório digital age com base em acordos legais.

O repositório digital deve observar disposições legais e obrigações contratuais em consideração quanto ao seu armazenamento de arquivos e o uso de medidas de preservação.

As restrições impostas ao armazenamento de arquivos por direitos autorais podem, por exemplo, ser contrariadas por acordos explícitos sobre o direito de armazenamento múltiplo, ações de alteração de arquivo, etc.

3.3. Com relação ao uso, o repositório digital age com base em acordos legais.
O repositório digital deve observar disposições legais e obrigações contratuais em consideração em relação ao uso de objetos digitais. Se isso resulta em uso restrito, a razão para a restrição deve ser documentada.

4. A forma organizacional é apropriada para o repositório digital.
O repositório digital deve ser organizado de tal forma que ele possa cumprir as suas metas de curto, médio e longo prazo. A sua eficácia e sustentabilidade podem ser avaliadas por usuários e produtores. Essa avaliação baseia-se nos seguintes pontos.

4.1 O financiamento adequado do repositório digital é garantido.
O repositório digital deve ser capaz de fundamentar a sua afirmação de que os serviços propostos podem ser financiados, tanto a curto quanto a longo prazo.

4.2 Número suficiente de pessoal devidamente qualificado disponível.
As qualificações e formação do pessoal devem ser adequadas para as metas, tarefas e processos do repositório digital. Esquemas adequados devem estar previstos para garantir a formação adequada e formação contínua em longo prazo. O número de funcionários deve ser suficiente para permitir que todos os processos necessários sejam totalmente preenchidos. O planejamento de longo prazo do repositório digital inclui recursos de pessoal.

4.3 Existem estruturas organizacionais adequadas para o repositório digital.
A estrutura organizacional deve ser adequada para as metas, tarefas e processos do repositório digital. Os processos e a destinação de pessoal e outros recursos são estruturados de tal forma que as metas definidas podem ser cumpridas.

4.4 O repositório digital se compromete com o planejamento de longo prazo.

O repositório digital deve se comprometer com o planejamento preventivo, incluindo tarefas iminentes ou esperadas, além de especificar os prazos em que elas serão concluídas. A gestão deve ter estruturas e procedimentos para o adequado planejamento estratégico. A base para o planejamento de longo prazo é o monitoramento de mudanças legais e sociais, as demandas e expectativas dos grupos-alvo [no OAIS: "Monitorar as Comunidade(s) Designado(s)"] e todos os desenvolvimentos técnicos (no OAIS: "Monitorar Tecnologias") relevantes para a preservação sustentada e uso adequado das informações representadas pelos objetos digitais. O planejamento também inclui garantir os recursos necessários.

4.5. O repositório digital reage a mudanças substanciais

Alterações substanciais são aquelas após as quais os objetivos não podem mais ser cumpridos, a menos que reajam ou, pelo menos, carreguem um risco aumentado. As alterações substanciais podem ser técnicas, organizacionais ou comunitárias.

Para isso, a administração deve incorporar um elemento do processo que monitore mudanças, avalie possíveis efeitos no cumprimento de tarefas e planos, implemente e monitore quaisquer alterações necessárias.

4.6 A continuidade das tarefas de preservação é assegurada mesmo para além da existência do repositório digital.

O repositório digital deve ter feito planos de contingência. Nesse caso, o trabalho de preservação deve ser continuado em um quadro organizacional diferente, garantindo, assim, que as tarefas definidas possam ser realizadas na sua totalidade. Onde isto não for possível, quaisquer restrições devem ser documentadas. O repositório digital deve tomar precauções para garantir que o processo de transição possa ser definido, planejado e implementado em tempo hábil. A documentação adequada é a base para o sucesso de um possível processo de transição.

5 O repositório digital realiza o gerenciamento adequado da qualidade.

O gerenciamento da qualidade deve garantir que as metas do repositório digital sejam atingidas. As metas gerais devem ser divididas em metas e objetivos específicos. Para isso, devem ser estabelecidas estruturas de processo adequadas, que são monitoradas pelo sistema de gestão da qualidade.
A gestão da qualidade deve ser um processo transversal que abranja todos as partes do repositório digital.

5.1 Todos os processos e responsabilidades foram definidos.
O sistema de gestão da qualidade deve garantir que todos os processos e suas interações estejam definidos, em particular, que indivíduos específicos estão responsavelmente designados para todos os processos. Isso também se aplica a processos externos (terceirizados).
5.2 O repositório digital documenta todos os seus elementos com base em um processo.
Os elementos incluem: metas, planos, especificações, implementações, processos, software, objetos e metadados, etc. O sistema de gestão da qualidade deve incluir um procedimento adequado para documentação, ou seja, um sistema para gerenciar todos os documentos necessários. O repositório digital deve estabelecer regras relativas à completude, correção, validade, compreensibilidade e acessibilidade da documentação, implemente estes e monitorar a sua observância.Isso evita que o conhecimento esteja ligado a certos indivíduos.

B. Gerenciamento de objetos
O repositório digital deve analisar seus objetivos e estratégias, e especificar todos os requisitos dos objetos relacionados para o gerenciamento de objetos digitais, durante o ciclo de vida dos objetos no repositório digital. As principais fases correspondem no modelo de referência da OAIS aos processos ("entidades funcionais") de armazenamento de ingestão, arquivamento, incluindo a implementação de medidas de preservação e acesso. Adições a essas funções podem se tornar necessárias, dependendo dos objetivos do repositório digital. O gerenciamento de objetos é baseado no modelo de informação do modelo de referência do OAIS e define os pacotes de submissão de informação informativos (SIPs) apropriados, pacotes de informação para arquivamento (AIPs) e pacotes de disseminação de informação (DIPs).

A integridade e autenticidade das informações a serem recebidas são conceitos centrais de confiabilidade. Integridade e autenticidade devem, portanto, ser de forma abrangente asseguradas em todas as fases pelas quais o repositório digital assumiu a responsabilidade. O pré-requisito para isso é garantir a integridade e autenticidade dos objetos digitais que representam informações que estão sendo preservadas (conforme 6 e 7). O repositório digital realiza o planejamento das medidas de arquivamento dos objetos-base em longo prazo para preservar a informação (em OAIS: Planejamento de Preservação) (conforme 8). Normas especificadas para ingestão, armazenamento e uso de arquivos, e padrões para os próprios objetos e suas transformações são outros indicadores de confiabilidade (conforme 9, 10 e 11). O repositório digital realiza um trabalho transparente, baseado em metadados para gerenciamento de dados para reconstrução de informações utilizáveis a partir dos objetos digitais para as comunidades designadas e para cumprir os requisitos de integridade, autenticidade e uso legalmente aprovado das informações (conforme 12).
Os requisitos de administração de objeto são os pré-requisitos para o planejamento e operação da infraestrutura técnica e sistema de segurança (conforme 13, 14).

6. O repositório digital assegura a integridade dos objetos digitais durante todas as fases de processamento.

Integridade aqui se refere, em primeiro lugar, à integralidade dos objetos digitais e em segundo lugar a sua intacto.

Os critérios para a integridade são as características de um objeto digital definida como digno de preservação (conforme 9.2.).

Os riscos para a integridade são colocados pela atividade humana (intencional ou acidental), imperfeição técnica ou roubo de infraestrutura técnica.

No repositório digital, deve-se tomar precauções tanto técnicas quanto organizacionais para se garantir a integridade.

O repositório digital deve operar um sistema de gerenciamento de dados adequado para preservar a integridade para os processos de ingestão, armazenamento de arquivos e acesso. O repositório digital também deve tomar precauções quanto à integridade da própria gestão de dados.

Em casos excepcionais, a integridade pode ser comprometida, caso em que esta deve ser adequadamente documentada.

6.1 Ingestão: o repositório digital garante a integridade dos objetos digitais.

Para isso, o repositório digital especifica uma interface claramente identificada para o produtor e o armazenamento de arquivos. Isso inclui a transformação a partir de pacotes de submissão de informação em pacotes de informação para arquivamento. A interface permite que o produtor e a administração de repositório digital verifiquem e mantenham a integridade dos objetos digitais.

6.2 Armazenamento de arquivos: o repositório digital garante a integridade dos objetos digitais.

Aqui o repositório digital deve especificar todas as funções de armazenamento de arquivos que são necessárias para verificar e manter a integridade dos objetos digitais pela administração do repositório digital. As funções incluem a gravação de pacotes de informação para arquivamento em mídias de armazenamento, armazenamento permanente, restauração dos pacotes de informações para arquivamento e todas as alterações nas AIPs.

6.3 Acesso: o repositório digital garante a integridade dos objetos digitais.

Para isso, o repositório digital especifica uma interface claramente identificada para o usuário e a loja de arquivos. Isso inclui a transformação de pacotes de arquivos em pacotes de acesso. A interface permite ao usuário e à administração do repositório digital para verificar e manter a integridade dos objetos digitais.

7 O repositório digital garante a autenticidade dos objetos digitais durante todas as fases de processamento.

Autenticidade aqui significa que o objeto é genuíno, ou seja, que ele representa o que ele afirma representar. Um aspecto chave é que o objeto em questão era criado pela fonte dada e no momento dado. A autenticidade também inclui documentação completa de todas as transformações aos objetos, realizadas para o propósito de preservação.

O repositório digital deve documentar se a autenticidade não puder ser demonstrada em um objeto particular. Uma vez que o objeto tenha sido recebido pelo repositório digital, o repositório digital assume a responsabilidade pela sua autenticidade.

O repositório digital deve operar um sistema de gerenciamento de dados adequado para a preservação da autenticidade nos processos de ingestão, armazenamento de

arquivos e acesso. Isto é fornecido, em particular, pela documentação de todas as alterações dos objetos (incluindo metadados) (ver 12.4).

7.1 Ingestão: o repositório digital garante a autenticidade dos objetos digitais.

O repositório digital deve especificar métodos para avaliar e proteger a autenticidade dos pacotes de apresentação.

7.2 Armazenamento de arquivo: o repositório digital garante a autenticidade dos objetos digitais.

O repositório digital deve especificar métodos que garantam a autenticidade dos objetos durante a implementação das medidas de preservação em longo prazo, ou documentar o grau de autenticidade (conforme. 10.4 e 12.4).

7.3 Acesso: o repositório digital garante a autenticidade dos objetos digitais.

O repositório digital deve garantir a autenticidade dos pacotes de acesso e permitir ao usuário para determinar o grau de sua autenticidade. Além disso, o repositório digital deve autenticar, ele mesmo, ao usuário como fornecedor dos pacotes de acesso.

8 O repositório digital tem um plano estratégico para as suas medidas de preservação técnicas (planejamento de preservação).

A fim de cumprir a sua responsabilidade para a preservação da informação, o repositório digital deve ter um plano estratégico, abrangendo todas as tarefas pendentes ou esperadas, e o tempo de sua realização. Esse planejamento estratégico (conforme 4.4) deve ser especificado no nível do objeto. Tais medidas devem manter o ritmo com a evolução técnica em curso (mudanças para suportes de dados, formatos de dados, as demandas dos usuários etc.).

As medidas para a preservação física dos dados (integridade, autenticidade), a sua acessibilidade e a preservação da sua facilidade de interpretação devem ser usadas para a preservação, em longo prazo, das informações representadas por objetos digitais. Medidas de preservação de longo prazo abrangem tanto conteúdo quanto metadados.

Veja 10.4 sobre a implementação das medidas de preservação em longo prazo.

9 O repositório digital aceita objetos digitais dos produtores com base em critérios definidos.

As linhas gerais de recolhimento, os critérios de seleção, os critérios de avaliação ou critérios para a geração de herança (conforme 1.1) e os objetivos gerais da conservação de longa duração devem ser especificados em nível do objeto.

A transferência pode ser efetuada por apresentação dos objetos para o repositório digital pela emissora ou por meio da coleta manual ou automática, por parte do repositório digital.

9.1 O repositório digital especifica seus pacotes de submissão de informação (SIP).

O repositório digital deve especificar, ou concordar com os produtores ou fornecedores, que objetos digitais e metadados devem ser ingeridos no repositório digital (na unidade conceitual de um pacote de submissão de informações). Esses acordos devem permitir a transferência ou a coleção a ser automatizada, e fluxos de trabalho para apresentação para o repositório digital devem ser implementados.

Essas especificações são a base para a verificação da qualidade dos objetos de transferência.

9.2 O repositório digital identifica quais características dos objetos digitais são significativas para a preservação da informação

Na determinação do escopo das características a serem preservadas, um equilíbrio devem ser atingido entre as metas relativas às possibilidades técnicas e os custos de preservação, em longo prazo, por um lado, e as necessidades da(s) comunidade(s) designada(s), por outro lado.

Pode ser eficaz a obtenção de diferentes representações de um objeto de informação, a fim de preservar o maior número possível de características.

9.3 O repositório digital tem controle técnico dos objetos digitais, a fim de levar a cabo medidas de preservação no longo prazo.

Muitos objetos digitais contêm características técnicas que restringem seu uso, seja por razões comerciais ou legais. Para a preservação, em longo prazo, dos objetos digitais, é crucial que o repositório digital seja capaz de

abrir e processar os objetos sem restrições. Todas as restrições técnicas de uso devem, portanto, ser removidas antes da submissão ao repositório digital.

10 O armazenamento de arquivo dos objetos digitais é realizado com as especificações definidas.

No coração de um repositório digital é a implementação do real processo de arquivamento. Este abrange a definição dos pacotes de arquivo, armazenamento dos AIPs e implementação das medidas de preservação no longo prazo.

10.1 O repositório digital define seus pacotes de informação de arquivamento (AIPs).

Pacotes de informação para arquivamento são unidades conceituais que consistem em dados de conteúdo e todos os metadados necessários para a preservação em longo prazo (conforme 12). A definição dos pacotes de informação para arquivamento deve incluir a determinação das estruturas de pacotes e de objetos utilizados, mais locais de armazenamento adequados e formatos.

A seleção dos pacotes de informação para arquivamento deve depender dos tipos de objetos (por exemplo de *script* digital ou clipe de animação 3D) e as características dos objetos a serem preservados.

Formatos abertos, divulgados e utilizados, frequentemente, são preferidos como formatos de pacotes de arquivamento, partindo do princípio de que estes terão uma vida mais longa, e é mais provável que hajam técnicas e ferramentas para converter ou emulando-os, já que eles são apoiados, por um amplo círculo dos usuários.

10.2 O repositório digital se encarrega de transformar os pacotes de submissão de informação (SIP) em pacotes de informação para arquivamento (AIPs).

Como parte do processo de ingestão, os SIPs devem ser transferidos para AIPs e os metadados de preservação específicos para preservação no longo prazo, adicionados. Isso pode envolver conversão de formato.

10.3 O repositório digital garante o armazenamento e legibilidade dos pacotes de informação para arquivamento (AIPs).

O repositório digital deve usar os métodos adequados para garantir que os pacotes de informação para arquivamento estejam corretamente armazenados e possam ser lidos, usando meios disponíveis no sistema. Legibilidade aqui refere-se à capacidade para ler os meios de armazenamento e a sequência de bits.
Veja 6.2 sobre como garantir a integridade dos pacotes de informações de arquivo.

10.4 O repositório digital implementa estratégias para a preservação no longo prazo dos pacotes de informação para arquivamento (AIPs).
As medidas de preservação, a longo prazo, especificadas no ponto 8 devem ser implementadas. Um tempo (ou ocasião) deve ser definido, quando cada pacote de informações para arquivamento deve ser verificado para saber se um passo preservação a longo prazo - por exemplo, a migração ou a emulação de um software à disposição - devem ser realizadas. Se necessária, a medida relevante deve ser realizada e documentada (conforme 12.4).

11 O repositório digital permite o uso dos objetos digitais com base em critérios definidos.
As finalidades de uso descritas no ponto 2 devem ser especificadas no nível do objeto. Os objetos podem ser utilizados por indivíduos, mas também por sistemas clientes. As possibilidades de busca e acesso aos pacotes de acesso devem ser definidas. Cada busca deve resultar em uma resposta clara do sistema. Se o repositório digital é parte de um arquivo maior, as conexões entre objetos digitais e analógicos que pertencem um ao outro também devem ser dados. Isso se aplica, em particular, para as partes constituintes de objetos híbridos.
Pacotes de acesso são unidades de informação que os usuários recebem como resposta
para consultas ao repositório digital .

11.1 O repositório digital define seus Pacotes de Disseminação de Informação (DIPs).
O repositório digital deve definir seus Pacotes de Disseminação de Informação (DIPs) dependo da(s) comunidade(s) designada(s) e os pacotes

de informação para arquivamento (AIPs). Uma pré-condição para isto é a determinação da aplicação de referência ambiente no qual os objetos podem ser usados. Um pacote de informações de arquivo pode ser oferecido em diferentes pacotes de difusão de informação, dependendo do contexto de utilização. Uso da informação representada pelos objetos digitais, na maioria dos casos, não significa que o acesso à informação arquivística nos próprios pacotes, em vez do uso de cópias ou derivados (possivelmente em combinação com outras informações), que ajuda na interpretabilidade. Esta poderia ser realizada por meio de uma descrição técnica, *software* adicional ou *software* de emulação.

Para trocar dados com outros repositórios digitais, ou para migrar os dados para uma infraestrutura técnica diferente é necessário transformar partes ou todo o conteúdo do repositório digital em um formato de exportação padronizado documentado. A informação pode assim ser preservada além da vida do próprio repositório digital (conforme 4.5).

11.2 O repositório digital garante a transformação de pacotes de informação para arquivamento (AIPs) em Pacotes de Disseminação de Informação (DIPs).

Os pacotes de disseminação de informação devem ser derivados a partir dos pacotes de informação para arquivamento, de acordo com um processo definido. Pacotes de disseminação de informação podem ser realizados no repositório digital e, em caso de condições alteradas, ser regenerados, ou criados, diretamente, a partir dos pacotes de informação para arquivamento (em tempo real), conforme necessário.

12 O sistema de gerenciamento de dados é capaz de fornecer as funções de repositório digital necessárias.

Gestão de dados é um processo de corte transversal que é compatível com os processos essenciais de um repositório digital - ingestão, armazenamento de arquivo e acesso - e também o planejamento e a execução das medidas de conservação, assegurando, ao mesmo tempo, a integridade e autenticidade em todas as fases de processamento.

O escopo do sistema de gestão de dados é ditado pelas metas do repositório digital. No Gerenciamento de dados, deve-se realizar as seguintes tarefas:

- A identificação dos objetos digitais e suas relações são essenciais para a administração dos objetos;
- pré-condição para encontrar e acessar objetos digitais é uma descrição formal do seu conteúdo e estrutura, garantindo interpretabilidade e integridade, e planejamento e implementação de medidas de preservação pressupõe descrição técnica dos objetos
- A documentação de todas as alterações dos objetos digitais é necessária para garantir a autenticidade dos dados
- A gravação de todas as restrições legais e sua base (leis, regulamentos, contratos, acordos) é necessária para assegurar que os requisitos legais são observados em todo o processamento.

Essas tarefas estão reunidas pela geração e armazenamento de metadados. Os metadados podem ser registrados de forma estruturada em um plano de metadados. Vários esquemas de metadados se estabeleceram para fins diferentes (por exemplo, metadados descritivos, estruturais, administrativos, técnicos, jurídicos) e para diferentes áreas (por exemplo, arquivos, bibliotecas, museus). A orientação para um padrão nacional ou internacional ou a posterior utilização de um esquema de metadados generalizados, muitas vezes, é possível e faz sentido no que diz respeito, em particular, para a sustentabilidade dos dados, e também para a cooperação e troca de dados entre produtores / fornecedores, o repositório digital e usuários. Um esquema de metadados contém campos definidos (elementos de dados), em que o respectivo conteúdo é registrado. O resultado é uma estrutura de dados que pode ser usada tanto por seres humanos quanto por máquinas.
O repositório digital deve estabelecer regras para o preenchimento dos campos com o conteúdo (por exemplo, uso de terminologia controlada). Diferentes ferramentas permitem a geração automática ou extração de metadados (por exemplo JHOVE para metadados técnicos).
Nesse catálogo de critérios, os metadados são tratados como parte das unidades de informação conceituais: pacote de transferência, pacote de arquivo e um pacote de acesso. Estes podem ser administrados, por exemplo, em bancos de dados e / ou estruturas XML.

12.1 O repositório digital única e persistentemente identifica seus objetos e seus relacionamentos.

O repositório digital deve usar identificadores internos para gerenciar os objetos e suas peças e relacionamentos (parte / totalidade, diferentes variantes, versões etc.), especialmente para a atribuição única de dados de conteúdo para os metadados (conforme 12.7).

A utilização de identificadores persistentes, visíveis externamente e padronizados, deve assegurar o referenciamento confiável e a citabilidade dos objetos.

A utilização de um serviço de resolução permite a incorporação de identificadores persistentes em endereço *URL*, garantindo assim acesso permanente. Isso requer gerenciamento dos dados do serviço de resolução.

O repositório digital compromete-se a apoiar o serviço de resolução na manutenção dos dados.

12.2 O repositório digital grava metadados adequados para o formato formal e descrição de conteúdo-base, descrição e identificação dos objetos digitais.

O escopo, estrutura e conteúdo dos metadados descritivos devem depender dos objetivos do repositório digital, sua comunidade / comunidades designadas e tipos de objetos. Descrição formal e baseada no conteúdo dos objetos na forma de metadados torna possível encontrar objetos; isto é essencial para as opções de busca que são oferecidas aos usuários.

12.3 O repositório digital registra metadados adequados para a descrição estrutural dos objetos digitais.

A estrutura de objetos complexos deve ser adequadamente descrita de modo que ela possa ser reconstituída e utilizada como entidades inteiras.

12.4 O repositório digital registra metadados adequados para documentar todas as alterações feitas pelo repositório digital aos objetos digitais.

O repositório digital deve documentar todas as alterações feitas nos objetos digitais. Isso também inclui o registro das pessoas e sistemas envolvidos e os correspondentes direitos (conforme. 3.2). Isso documenta a autenticidade (conforme. 7) e também garante preservação técnica dos objetos digitais.

Em particular, os objetos digitais nos repositório digitais que escolheram a migração como sua estratégia de preservação em longo prazo são

frequentemente alterados. A isso se somam as transformações que são realizadas, durante a submissão ao repositório digital e para entrega de objetos de acesso.

12.5 O repositório digital adquire metadados adequada para a descrição técnica dos objetos digitais.

Para garantir a interpretabilidade e integridade e controlar as medidas de preservação, os próprios objetos e, no caso de objetos complexos, todos seus arquivos devem ser descritos de forma abrangente em termos técnicos. Isso inclui, em particular, a descrição das informações de representação.

12.6 O repositório digital adquire metadados adequados para gravar os direitos e condições de uso correspondentes.

O uso dos objetos digitais pode ser restrito por motivos legais ou contratuais. Dependendo dessas condições e dos grupos de usuários correspondentes, esses direitos e condições devem ser registrados de forma a permitir que o uso seja controlado (por exemplo, acesso controlado, cópias anônimas dos usuários) e os usuários possam ser informados sobre eles (conforme. 3.3).

12.7 A estrutura de empacotamento é preservada em todos os momentos.

A conexão entre os metadados e os dados de conteúdo deve ser segura e sem ambigüidade.

Isso pode ser conseguido, por exemplo, por:

a) uso de identificadores persistentes internos, porém visíveis externamente, para o objeto digital e suas partes, especialmente dados de conteúdo e metadados (conforme. 12.1).

b) mantendo todo o conteúdo e metadados pertencentes a um objeto em um diretório ou em um arquivo.

C. Infraestrutura e Segurança

Em Infraestrutura e Segurança, analisam-se os aspectos técnicos do sistema como um todo e aspectos de segurança.

13 A infraestrutura de TI é apropriada.

A infraestrutura de TI deve colocar as especificações para lidar com os objetos em prática nos níveis de tecnologia e segurança. Ela é responsável pela totalidade de todos os objetos.

13.1 A infraestrutura de TI implementa os requisitos de gerenciamento de objetos.

Os requisitos especificados pelo repositório digital a respeito do manuseio de objetos devem ser implementados por todo o sistema em todas as fases de processamento. Isso inclui os principais processos (em OAIS: "entidades funcionais") de ingestão, armazenamento de arquivo, acesso e o processo de suporte de gerenciamento de dados (incluindo ações de preservação). A Extensão dessas funções pode ser necessária, como resultado dos objetivos do repositório digital.

13.2 A infraestrutura de TI implementa os requisitos de segurança do sistema de segurança de TI

Os requisitos de segurança do gerenciamento de objetos devem ser levados em consideração durante a realização:

- Assegurar a integridade dos objetos, ou seja, protegê-los contra modificações ilegais decorrentes de ações humanas deliberadas e involuntárias, e imperfeição técnica;
- Assegurando a autenticidade dos objetos;
- Assegurar a confidencialidade dos objetos, ou seja, excluir a possibilidade de aquisição não autorizada de informações;
- Assegurando a disponibilidade dos objetos, por meio de gerenciamento das funções do objeto (proteção contra sabotagem, falhas no sistema, etc.)

14 A infraestrutura protege o repositório digital e seus objetos digitais.

A infraestrutura deve proteger os objetos digitais de riscos baseados em sistema e riscos externos. Perigos baseados em sistema poderiam surgir, por exemplo, em decorrência de problemas de hardware ou o fracasso dos meios de armazenamento individual. Externamente, a primeira prioridade do repositório digital deve ser a proteção contra ameaças naturais (por exemplo, fogo, água, atividade sísmica), e também contra os riscos provocados pelos seres humanos. Os objetos podem ser

prejudicados, diretamente, por funcionários ou por meio de programas nocivos contrabandeados para o sistema (por exemplo, vírus). Proteger os dados também envolve impedindo o envio não intencional de informações por programas (*trojans*) ou pessoas (espionagem).

A proteção deve cobrir os objetos, as instalações utilizadas pelo repositório digital, o *hardware*, *software* e, não menos importante, o pessoal.
Os diferentes riscos devem ser contrabalançados por um pacote técnico (por exemplo, programas de proteção antivírus) e medidas organizacionais (por exemplo, restrições de acesso).

APÊNDICE B - PROCEDIMENTO AMPLIADO DE AUTOAVALIAÇÃO PARA OBTENÇÃO DO SELO NESTOR PARA ARQUIVOS DIGITAIS DE CONFIANÇA[128]

C1 Seleção de objetos de informação e suas representações
Foram definidos critérios para a seleção de objetos de informação e suas representações no arquivo digital. A estrutura é fornecida por obrigações legais, pela função básica da instituição ou empresa, seus próprios alvos.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Isso diz respeito ao papel ou missão do arquivo digital. O tipo de informação digital pela qual o arquivo digital é responsável deve ser claro tanto interna quanto externamente. A seleção deve ser documentada de forma transparente, com base em critérios, diretrizes e perfis. A C1 faz parte da definição dos objetivos e tarefas do arquivo digital e, portanto, é crucial para avaliar sua confiabilidade, especialmente ao avaliar a adequação de cada atividade.
Perguntas
- Que critérios foram estabelecidos para selecionar os objetos de informação e suas representações? - Qual é a justificativa para esses critérios? - Como os critérios podem ser acessados, interna e externamente?
Documentos
Critérios publicados para a seleção dos objetos de informação e suas representações: base legal, diretrizes de coleta, catálogos e regras para avaliação e seleção.

C2 Responsabilidade pela preservação
O arquivo digital assume a responsabilidade pela preservação, em longo prazo, dos objetos de informação sobre a base das exigências legais ou de seus próprios objetivos. A preservação, em longo prazo, significa garantir a usabilidade a longo prazo das informações contidas nas representações.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
O que é importante aqui é o compromisso do arquivo. Ele se compromete a coletar informações mas também garante que elas permaneçam permanentemente utilizáveis. O arquivo de preservação deve estar plenamente consciente das consequências de fazer este (auto) compromisso. O C2 faz parte da definição dos objetivos e tarefas do arquivo digital e, portanto, é crucial para avaliando sua confiabilidade, especialmente ao avaliar a adequação de cada atividade.
Perguntas
- Qual é a base da responsabilidade de preservação do arquivo? - Quais tarefas de arquivamento podem ser derivadas disso (documentação, armazenamento, preservação de acessibilidade, acesso, ...)? - Por qual período o arquivo assume esta responsabilidade?
Documentos
Lei, contrato, compromisso voluntário, política, declaração de missão, documento de estratégia.

C3 Comunidades Designadas
O arquivo digital definiu sua comunidade/comunidades designadas. Isso inclui o conhecimento de exigências específicas das comunidades designadas que influenciam a seleção dos serviços para serem fornecidos. Se as comunidades designadas ou suas necessidades mudarem com o tempo, o arquivo digital devem se adaptar de acordo.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
As comunidades designadas são essenciais para descrever as metas de preservação para as informações arquivadas. Ao determinar suas comunidades designadas, o arquivo digital deve ter em mente as perguntas que os usuários estarão fazendo ao acessar os recursos do arquivo, e o conhecimento que se pode esperar que eles tragam com consigo. As mudanças nas comunidades designadas e seus requisitos devem ser monitoradas e mecanismos instalados para lidar com eles. O C3 faz parte da definição dos objetivos e tarefas do arquivo digital e, portanto, é crucial para avaliar sua confiabilidade, especialmente ao avaliar a adequação de cada atividade.
Perguntas
- Quais comunidades designadas foram definidas para o arquivo digital? Como elas têm sido definidas? - Quais das necessidades específicas das comunidades designadas foram identificadas? - Como os serviços oferecidos foram alinhados com as exigências das comunidades designadas? - Quais métodos são usados para monitorar as mudanças nas comunidades designadas (Monitoramento da comunidade)? - Foram feitos planos para adaptar o arquivo digital às comunidades designadas e/ou novas tarefas?
Documentos
Descrição das comunidades designadas com suas exigências específicas, mais o método de monitoramento e base legal ou contratual.

C4 Acesso
O arquivo digital garante que os usuários autorizados nas comunidades designadas possam acessar as representações. Isso inclui possibilidades de busca apropriadas. O arquivo digital declara, abertamente, suas condições de uso e quaisquer custos que possam surgir, listando-as de forma transparente.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Esse critério tem três aspectos: acesso, busca e custos. É estipulado que os usuários devem ter acesso às informações arquivadas. A natureza deste acesso (por exemplo, acesso remoto ou local) pode ser decidida pelo arquivo digital. O acesso também inclui oferecer possibilidades de busca para encontrar a informação arquivada e também informações sobre os termos de uso e restrições.
Perguntas
- Como é garantido aos usuários autorizados o acesso ao arquivo digital? - Que possibilidades de busca existem? - Quais termos de uso existem?
Documentos
Instrumentos de documentação (por exemplo, catálogo, ajuda na busca), termos de uso (incluindo preços), documentação de cenários de acesso.

C5 Interpretabilidade
O arquivo digital definiu medidas para assegurar, em longo prazo, a interpretabilidade de pelo menos um das representações, satisfazendo assim uma pré-condição básica para o uso apropriado agora e no futuro. Este inclui a interpretabilidade tanto dos dados de conteúdo quanto dos metadados. Ao garantir isso, o arquivo digital deve levar em conta as necessidades de sua comunidade/comunidades designadas. As mudanças na ambiente técnico ou na comunidade ou comunidades designadas podem influenciar a interpretabilidade dos objetos. Usando procedimentos apropriados, o arquivo digital deve, portanto, verificar regularmente intervalos se os objetos ainda podem ser interpretados pela comunidade ou comunidades designadas.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Esse critério constitui parte da implementação da C2 "Responsabilidade por preservação", em particular a preservação da usabilidade da informação - a área mais importante do ponto de vista da preservação no longo prazo. A fim de garantir a usabilidade, em longo prazo, a (intelectual) das representações pela comunidade designada precisa ser levada em conta consideração além dos aspectos técnicos, tais como displays, reprodução, funcionamento, etc. Medidas de migração ou emulação devem ser planejadas para garantir que as representações permaneçam utilizáveis. A interpretabilidade intelectual deve ser apoiada por medidas adequadas para descrever o contexto de criação da informação, documentação adequada dos dados / estruturas / formatos (representação informação). As medidas planejadas devem ser proporcionais às necessidades e aos objetivos de uso das comunidades designadas. O guia "Planejamento de Preservação Digital" do NESTOR pode ajudar aqui. O digital arquivo deve ter documentado suas próprias considerações e medidas planejadas. O C5 fornece a base conceitual para o C11 "Medidas de preservação".
Perguntas
- Como é a interpretabilidade, em longo prazo, de, pelo menos, uma representação dos dados de conteúdo e metadados garantidos? - Como são levados em consideração os objetivos de uso e as necessidades da comunidade designada? - Que métodos existem para que as comunidades designadas verifiquem a interpretabilidade de bases regulares?
Documentos
Descrição das estratégias para a manutenção, em longo prazo, da interpretabilidade, sistema de planejamento de preservação.

C6 Base legal e contratual
Os procedimentos de ingestão, arquivamento e acesso do arquivo digital são baseados em procedimentos legais ou contratuais regulamentos concluídos com os produtores. A natureza e o escopo da entrega são regulamentados, assim como as obrigações do arquivo digital, as condições de uso e, quando aplicável, os custos.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Esse critério está ligado à C1 e C2. Aplicam-se regulamentos legais ou contratuais diferentes. Dependendo da estrutura dentro da qual um arquivo digital opera. Uma biblioteca de depósitos legais, provavelmente, está vinculada, pelas leis de depósito legal, a um arquivo estadual pela Lei de Arquivo do Estado, a uma biblioteca de coleções especiais por acordos de licença com editores, a um arquivo de dados de pesquisa por contratos com os fornecedores de dados. É importante para o arquivo digital saiba exatamente quais regulamentações se aplicam a ele e para garantir que Existem regulamentos legais ou contratos individuais para todas as áreas relevantes.
Perguntas
- Como são as entregas, as obrigações do arquivo digital, os termos de uso e os custos regulamentados com os produtores?
Documentos

Lista de normas legais e contratos

C7 Conformidade legal
O arquivo digital monitora e documenta a conformidade com os regulamentos pertinentes relativos à ingestão, arquivamento e uso de objetos digitais. Estes incluem: proteção de dados, proteção dos direitos dos afetados partes, regulamentos de confidencialidade, direitos autorais e de uso, conformidade interna e externa. Em que medida o critério deve ser atendido?
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
O arquivo digital deve antes de tudo ter identificado quais direitos se aplicam a ele. As medidas devem ser documentado e implementado para cada direito aplicável.
Perguntas
- Como são a proteção de dados, a proteção dos direitos das pessoas afetadas, os regulamentos de confidencialidade, direitos autorais e de uso e conformidade interna e externa monitorada?
Documentos
Lista de direitos relevantes e documentação de medidas para a observância desses direitos.

C8 Financiamento
Existe um planejamento orçamentário válido, assim como um plano de financiamento de longo prazo para o arquivo digital.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
O arquivo digital deveria primeiro ter identificado todas as suas unidades de custo atuais e futuras e as documentou em um modelo de custos. Isso poderia incluir a aquisição, operação e licenciamento orçamentos que cobrem despesas com hardware e software, custos de pessoal, taxas de consultoria, custos de serviços externos, etc. Todas as unidades de custo atuais devem ser suficientemente orçamentadas no planejamento financeiro atual. A revisão também deve incluir os processos estabelecidos na organização processual (ver C10), ao mesmo tempo em que se tomam os objetivos e tarefas do arquivo em conta. Além disso, o plano de financiamento também deve incluir previsões, em longo prazo, que contenham projeções futuras para os requisitos de financiamento do arquivo digital. Poucas instituições são, verdadeiramente, capazes de salvaguardar seus financiamentos além do orçamento anual atual; portanto, é suficiente para que o plano seja documentado aqui.
Perguntas
- Qual modelo de custo é utilizado? - Quais documentos de planejamento orçamentário existem? - Quais planos de financiamento no longo prazo existem para o arquivo digital?
Documentos
Modelo de custos, planejamento do orçamento atual, plano de financiamento.

C9 Pessoal
Há um número suficiente de pessoal adequadamente qualificado disponível. Existem descrições de cargos atualizadas que estabelecer as qualificações necessárias do pessoal do arquivo digital e conter um organograma e/ou um plano de desenvolvimento do pessoal com base nas tarefas e objetivos do arquivo digital.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Este critério contém dois fatores que o arquivo digital deve definir: O que ele compreende por qualificações, e que níveis de pessoal considera adequados? Com base nos objetivos e tarefas do arquivo, a revisão também deve incluir especificamente as responsabilidades do pessoal como estabelecido no organograma e no organograma de procedimentos (ver C10). Deve-se observar que medidas formais especializadas de treinamento no campo do arquivamento digital de longo prazo estão ainda em fase de desenvolvimento nos países de língua alemã (entre os quais se destacam os cursos de treinamento iniciais e adicionais oferecidos pelo NESTOR (Escola NESTOR, Oficinas).
Perguntas
- Quantos membros do pessoal estão disponíveis (divididos por qualificação e função), e o que o planejamento é feito? - Como esses fatores ajudam o arquivo digital a realizar suas tarefas?
Documentos
Descrição das funções, organograma, plano de desenvolvimento do pessoal.

C10 Organização e processos
A estrutura organizacional deve ser apropriada para os objetivos, tarefas e processos do arquivo digital. A organização estrutural e processual deve ser definida. As responsabilidades devem ser estabelecidas. O arquivo digital é incorporado ao ponto apropriado no cronograma de responsabilidades.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Aqui é importante documentar como a estrutura organizacional corresponde aos objetivos e tarefas do arquivo. Esse critério fornece a base para avaliar a adequação do financiamento (C8) e do pessoal (C9).
Perguntas
- Qual estrutura organizacional (organização estrutural e processual) o arquivo digital têm? - Que responsabilidades foram estabelecidas? - Como essa estrutura permite que o arquivo desempenhe suas tarefas?
Documentos
Modelo de processo, cronograma de responsabilidades, organograma

C11 Medidas de preservação
O arquivo digital deve conduzir o planejamento estratégico como um meio de preservar os objetos digitais que lhe foi confiada. Isso deve incluir tarefas iminentes ou esperadas e especificar os prazos em que devem ser concluídas. O planejamento, em longo prazo, deve se basear no monitoramento dos aspectos legais e sociais. Mudanças, exigências e expectativas das comunidades designadas e todas as mudanças técnicas relevantes para a preservação sustentada e o uso apropriado dos objetos de informação na forma de suas representações. Os possíveis efeitos no cumprimento das tarefas são avaliados. Estruturas adequadas e existem procedimentos para isso.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Para realizar o planejamento estratégico de medidas de preservação, o arquivo digital também deve considerar aspectos como tempo, pessoal e recursos financeiros, restrições legais, restrições técnicas instalações, etc., além de seus objetivos e tarefas. A ferramenta PLATO, por exemplo, pode fornecer suporte técnico adequado para tal planejamento; pode ser utilizado para ajudar a elaborar um plano de plano de preservação transparente. A C11 leva as estratégias e planos de preservação da interpretabilidade, documentados na C5, para a próxima etapa de planejamento concreto.
Perguntas
- De que forma o planejamento estratégico das medidas de preservação é feito? - Como o planejamento se correlaciona com os objetivos gerais e os outros aspectos do trabalho do arquivo?
Documentos
Plano de preservação

C12 Gestão de crises / sucessão
O arquivo digital possui um plano que garante a continuidade das tarefas de preservação mesmo além da própria existência do arquivo. O arquivo digital deveria ter feito planos de contingência. Em tal caso, o trabalho de preservação deve ser continuado em uma estrutura organizacional diferente, assim garantindo que as tarefas definidas possam ser realizadas na íntegra. Quando isto não for possível, quaisquer deficiências devem ser documentadas. O arquivo digital deve tomar precauções para garantir que a transição processo pode ser definida, planejada e implementada em tempo hábil.
Em que medida o critério deve ser cumprido?
Implementado - 10 pontos
Explicação
Isto está condicionado a todos os processos e tecnologias do arquivo digital, especialmente os formatos de exportação, sendo documentados - ou seja, devem ser documentados suficientemente bem para o digital arquivo como um todo, tarefas individuais e objetos de informação a serem transferidos para um terceiro no caso de emergência. Se qualquer deficiência resultante parecer provável, estas devem ser documentadas. Acordos devem ser elaborados com possíveis sucessores, sempre que possível (por exemplo, com arquivos estatais, arquivos comerciais, etc.).
Perguntas
- Até que ponto o arquivo digital garantiu que os objetos de informação fossem preservados, mesmo depois que o próprio arquivo tiver deixado de existir? - O que constitui uma crise que exigiria a transferência de tarefas para terceiros, e como isso é decidido? - Que planos existem no caso de uma crise?
Documentos
Plano de crise, declaração de transferência.

C13 Propriedades significativas
O arquivo digital identifica e documenta quais das propriedades das representações transferidas são significativas para a preservação dos objetos de informação. Ao determinar o escopo das propriedades a serem preservadas, deve ser encontrado um equilíbrio, tendo em mente os próprios objetivos do arquivo, entre as possibilidades técnicas e os custos de preservação no longo prazo, por um lado, e as necessidades do comunidade/comunidades designadas, por outro lado.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
O objetivo da preservação digital é preservar indefinidamente as propriedades de um objeto de informação que são considerados importantes (= "significativos"), independentemente de sua atual técnica representação. O objetivo do critério 13 "Propriedades significativas" é verificar se a definição e descrição das propriedades significativas dos objetos de informação foram suficientemente consideração na arquitetura do sistema, no modelo de dados e nos fluxos de trabalho. C13 é um pré-requisito para C17/18/19, pois a autenticidade (conforme definido na DIN 31644) a ser assegurada requer a identificação de propriedades significativas. O estado da arte: O cumprimento integral deste critério não pode ser esperado no momento, já que mais tempo é necessário para que a comunidade aceite e implemente o conceito de propriedades significativas. O "Guia de Planejamento de Preservação NESTOR" deve ser consultado.
Perguntas
- O que o arquivo digital entende por propriedades significativas e como ele lida eles? - Em que medida os objetivos do arquivo digital foram levados em consideração? - Como o arquivo consegue o equilíbrio entre o trabalho envolvido e o desempenho do o sistema, por um lado, e os interesses de uso dos clientes, por outro? - Como as propriedades significativas dos objetos de informação foram ancoradas no sistema? arquitetura, o modelo de dados e o fluxo de trabalho?
Documentos
Documentação das propriedades significativas

C14 Integridade: Interface de invenção
O arquivo digital tem sua própria interface para ingerir as representações de uma forma que retenha sua integridade. A interface contém todas as funções e processos destinados a transferir a pacotes informativos de apresentação dos produtores, transformando-os em informações de arquivo e incorporando-os ao arquivo digital. A interface permite que o produtor e a administração de arquivos digitais para verificar e manter a integridade das representações.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
O processo de transferência, no qual as representações de objetos de informação são transferidas desde a esfera de responsabilidade do fornecedor até a do arquivo, é especialmente crítico no que diz respeito à necessidade de proteger os dados relevantes contra a corrupção. A finalidade do critério 14 é avaliar se a interface de ingestão do arquivo digital é adequada para garantir que as representações sejam mantidas completas e intactas em um processo de transferência confiável e transparente. C14 e C21 - "Especificação dos pacotes de informações de apresentação" e C22 "Transformação dos pacotes de informações de apresentação em pacotes de informações de arquivo" são mutuamente dependentes. As funções da interface de ingestão que garantem a integridade representam um aspecto especial do C33 "Infraestrutura de TI".
Perguntas
- Quais funções estão incluídas na arquitetura do sistema para garantir a integridade e a segurança de dados durante o processo de ingestão (por exemplo, verificação de vírus, verificação da integridade dos dados com base em valores *hash* para os dados de conteúdo, metadados e pacotes de informações de apresentação como um todo)? - Estas verificações são realizadas durante a transferência e também durante a transformação do enviar pacotes de informações em pacotes de informações de arquivo? - Na forma de quais processos estas funções são incorporadas nas especificações do sistema? - Como o arquivo lida com quaisquer erros detectados durante a verificação de integridade?
Documentos
Documentação técnica da interface de ingestão, incluindo todos os processos, descrição da transferência, transformação para arquivo de pacotes e fluxos de trabalho de armazenamento.

C15 Integridade: Funções do armazenamento de arquivos
O armazenamento de arquivos oferece funções necessárias para verificar e manter a integridade da representações da administração do arquivo digital. As funções incluem o registro dos pacotes de informações de arquivo em mídia de armazenamento, armazenamento de longo prazo, restauração do arquivo pacotes informativos e todas as mudanças nos pacotes.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Garantir que as representações arquivadas dos objetos de informação permaneçam completas e intactas por períodos mais longos é um dos principais requisitos do armazenamento de arquivos em um sistema digital confiável arquivo. Para satisfazer este requisito, o sistema deve fornecer uma gama de funções dedicadas a recuperação de pacotes de informações de arquivo em caso de danos. O C15 está intimamente ligado ao C33 "IT Infraestrutura" (especialmente armazenamento de arquivos) e C34 "Segurança" (especificamente técnica-organizacional medidas do conceito de segurança).
Perguntas
- Que funções e processos são planejados no sistema para garantir que o arquivo pacotes de informações permanecem completos e intactos durante o processo de armazenamento (por exemplo, seleção de meios de armazenamento adequados, redundância, refrescante, migração de mídia)? - Quais mecanismos verificam a integridade dos pacotes de informações de arquivo salvas para intervalos adequados? - Quais mecanismos estão incorporados ao sistema, ou estão planejados, para a recuperação de danos pacotes de informações de arquivo? Como são documentadas as rotinas de verificação e recuperações?
Documentos
Documentação técnica do armazenamento do arquivo, sistema de armazenamento, gerenciamento de risco, conceito de preservação do fluxo de *bits.*

C16 Integridade: interface do usuário
O arquivo digital tem uma interface que permite aos usuários e à administração do arquivo digital verificar e manter a integridade das representações. Isto inclui a transformação a partir de pacotes de arquivos informativos em pacotes informativos de divulgação.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
As representações arquivadas dos objetos de informação devem permanecer completas e intactas. durante e após o uso, e ser transparente para todas as partes envolvidas. A fim de atender a este requisito, a arquivo digital deve estar ciente e revelar os limites de sua responsabilidade, assumir todos os aspectos de o processo de fornecimento (incluindo as ajudas de interpretação que proporciona) e oferecer aos usuários possibilidades de fazendo verificações completas da integridade dos dados que lhes são fornecidos. O C16 está ligado ao C33 "Infraestrutura de TI". e C4 "Acesso".
Perguntas
- Que medidas estão em vigor para garantir que as informações solicitadas estejam completas e intactas após a conversão dos pacotes de informações do arquivo em informações de divulgação embalagens? Que procedimento é adotado se a integridade for perdida? - Que possibilidades o usuário tem para verificar a integridade das informações arquivadas desde o momento da transferência para o arquivo digital até o seu uso?
Documentos
Documentação técnica da interface do usuário, incluindo todos os processos, sistema de acesso.

C17 Autenticidade: *Ingest*
O arquivo digital tem procedimentos que permitem avaliar a autenticidade das representações ao ser ingerido e a autenticidade dos pacotes de informações a serem avaliados e protegidos.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
A preservação no longo prazo dos objetos de informação pode ser considerada autêntica se, uma vez inseridos, as representações transferidas dos objetos de informação digital só podem ser alteradas por medidas deliberadas e documentadas que garantem a preservação de propriedades significativas. Durante o processo de ingestão, as representações são transferidas da esfera de responsabilidade do fornecedor para a do arquivo. A autenticidade deve ser avaliada com base no significativo especificado propriedades e preservadas nas etapas seguintes do processo. C17 é necessário pelo C13 "Significativo propriedades" e está ligado ao C33 "Infraestrutura de TI". O estado da arte: O cumprimento completo deste critério não é atualmente esperado devido à estreita ligação com C13.
Perguntas
- São etapas do processo identificáveis no processo de ingestão (transferência, transformação da apresentação em pacotes de informações de arquivo e armazenamento) que influenciam a autenticidade do objeto (separação do portador de dados, normalização)? - Quais processos têm o arquivo digital especifico para proteger a autenticidade dos objetos de informação correntes ou em perspectiva de transferência? Como podem ser verificadas as propriedades dos objetos de informação para preservação? - Que medidas são tomadas se a autenticidade estiver em perigo?
Documentos
Documentação técnica da interface de ingestão, incluindo todos os processos. Registro de todas as mudanças nas representações.

C18 Autenticidade: Medidas de preservação
O arquivo digital utiliza métodos que garantem a autenticidade dos objetos durante implementação das medidas de preservação no longo prazo e documentar o grau de autenticidade.
Em que medida o critério deve ser cumprido?
. Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
As medidas de preservação podem tornar necessário criar uma nova representação técnica de um objeto de informação digital ou incorporar as representações existentes em um ambiente de emulação modificado. Um arquivo digital confiável deve assegurar que os objetos relevantes mantenham sua autenticidade enquanto passam por esses processos e que todas as medidas devem ser documentadas de forma permanente e transparente. O C18 é exigido pelo C13 "Propriedades significativas" e é um requisito particular do C11 "Medidas de preservação". O estado da arte: O cumprimento completo deste critério não é esperado atualmente devido à estreita ligação com C13.
Perguntas
- Quais processos foram especificados para proteger a autenticidade dos objetos de informação digital durante a conservação? - Como é garantida a preservação de propriedades significativas no processo de migração ou na implementação de novos ambientes de emulação? Como isto é monitorado (automaticamente/manualmente, para todas as representações/uma amostra aleatória)? - Como o arquivo digital procede se as propriedades significativas individuais não são preservadas, seja total ou parcialmente?
Documentos
Registro de todas as mudanças nas representações, documentação do processo de monitoramento das propriedades significativas.

C 19 Autenticidade: Uso
O arquivo digital permite que os usuários e a administração do arquivo digital possam verificar e manter a autenticidade das representações. Isto inclui a transformação das informações de arquivo pacotes em pacotes de informações de divulgação.
Em que medida o critério deve ser cumprido?
. Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34. Explicação:
Explicação
Um arquivo digital confiável deve permitir que cada usuário verifique se a representação é autêntica no que diz respeito à área de responsabilidade do arquivo digital. O arquivo também deve ser capaz de gerar pacotes de informações de divulgação que cumpram a exigência de autenticidade. C19 é exigido pelo C13 "Propriedades significativas". O estado da arte: O cumprimento completo deste critério não é atualmente esperado devido à estreita ligação com C13.
Perguntas
- Durante a transformação dos pacotes de arquivo em pacotes de informação de divulgação, como a autenticidade é mantida, como são preservadas as propriedades significativas? - Que possibilidades o usuário tem para verificar a autenticidade das informações arquivadas desde o momento da transferência para o arquivo digital?
Documentos
Documentação técnica da interface do usuário, incluindo todos os processos, sistema de acesso.

C20 Autoridade técnica
O arquivo digital obtém autoridade técnica sobre as representações que estão sendo ingeridas, permitindo-lhe transformá-los em pacotes de informações de arquivo e, se necessário, realizar no longo prazo medidas de preservação. Após a transferência, todas as medidas necessárias podem ser realizadas sem qualquer restrições técnicas.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Quando uma representação de um objeto de informação digital é transferida para um arquivo digital, o arquivo deve obter todo o poder técnico de disposição sobre os dados que estão sendo arquivados, a fim de transportar de todas as medidas subsequentes sem restrições. Deve ser assegurado que qualquer medida técnica existente as restrições de uso (por exemplo, criptografia, proteção contra cópia e impressão, etc.) são identificadas e desativadas. O C20 é uma parte do C21 "Pacotes de informações de submissão" A autoridade técnica deve ser levada em consideração em C6 "Base legal e contratual".
Perguntas
- Quais processos são planejados antes da transferência de dados, a fim de garantir que o arquivo digital autoridade de dados em uma base permanente - jurídica, organizacional e técnica? - Como o arquivo digital garante, em termos práticos, que todas as restrições técnicas ao uso de as representações podem ser identificadas e desativadas? Como são, por exemplo, criptografia, impressão e cópia proteção e limites de tempo de legibilidade tratados? - Como o arquivo digital consegue autoridade técnica se as representações são transferidas com restrições?
Documentos
Acordo com os produtores, descrição da verificação das restrições técnicas.

C21 Pacotes de informações sobre a submissão
O arquivo digital emitiu especificações a respeito de seus pacotes de informações de apresentação. O arquivo digital concorda com os produtores que submeterão os pacotes de informação (dados de conteúdo e metadados). Os pacotes de informações de apresentação são verificados com base em especificações.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
O critério C21 "Pacotes de informações de submissão" serve para verificar até que ponto o arquivo digital especificou adequadamente a composição dos pacotes de dados para a transferência de dados. Ele devem ser determinados quais dados de conteúdo e metadados podem ser combinados de que forma em um pacotes informativos de apresentação, e que acordos devem ser feitos com os produtores a fim de para implementar estes regulamentos. Além disso, deve haver um procedimento para verificar a conformidade do pacotes informativos de apresentação com o regulamento. A especificação dos pacotes de informações de submissão sob C 21 é uma condição prévia para os critérios C14 e C17 "Integridade e autenticidade do processo de ingestão".
Perguntas
- Quais especificações o arquivo digital tem em relação às informações de apresentação embalagens? Quais dados de conteúdo são aceitos? Quais metadados são necessários? Existem exigências e processos especiais para a criação de pacotes de informações de apresentação? - Quais medidas existem para validar a conformidade dos pacotes informativos de submissão? - Os pacotes informativos de submissão defeituosos são rejeitados antes da transferência, ou são corretivos medidas empreendidas dentro de uma área de trabalho definida no arquivo digital?
Documentos
Especificação dos pacotes de informação de apresentação.

C 22 Transformação dos pacotes de informações de apresentação em pacotes de informações de arquivo
O arquivo digital converte pacotes de informação de submissão em pacotes de informação de arquivo.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Uma vez transferidos os pacotes de informação de submissão, o arquivo digital geralmente terão que convertê-los em pacotes de informações de arquivo. Dependendo do arquivamento os dados existentes são convertidos, estruturados e/ou complementados com os metadados necessários para preservação no longo prazo. O C22 está ligado ao C14 e C17.
Perguntas
- Como são especificados os processos de transformação do arquivo digital? Qual conversão e medidas estruturantes são especificadas? - Que medidas de garantia de qualidade existem?
Documentos
Especificação da transformação, descrição do processo.

C 23 Pacotes de informações de arquivo
O arquivo digital emitiu especificações para seus pacotes de informações de arquivo. O arquivo digital define quais pacotes de informações de arquivo (dados de conteúdo e metadados) devem ser armazenados e em que forma. Os pacotes de informações de arquivo são verificados com base nas especificações.
Em que medida o critério deve ser cumprido?
. Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Os pacotes de informações arquivísticas a serem preservados são criados na transformação processo após a transferência dos pacotes de informações de apresentação. Um arquivo digital de confiança deve estar de posse de especificações precisas para seus pacotes de informações de arquivo. Estes devem contêm informações adequadas sobre os dados de conteúdo, os metadados necessários para a preservação no longo prazo e sobre a estrutura das embalagens. Conformidade dos novos pacotes de informações de arquivo com As especificações devem ser verificáveis. A especificação dos pacotes de informações de arquivo no C23 fornece a base para especificar as transformações em C22 e C25. É uma pré-condição para a verificação da integridade e autenticidade do armazenamento de arquivos em C15 e C18 e para garantir a interpretabilidade em C24. Ver C27-32 com relação aos metadados como parte constituinte dos pacotes de informações de arquivo.
Perguntas
- São as partes constituintes e a estrutura dos pacotes de informações de arquivo suficientes especificado? - Como é verificada a qualidade dos pacotes de informações de arquivo?
Documentos
Especificação do modelo do objeto; ver C27-32 a respeito dos metadados.

C 24 Interpretabilidade dos pacotes de informações de arquivo
Medidas técnicas de preservação são tomadas para garantir a interpretabilidade dos pacotes de informação de arquivo.
Em que medida o critério deve ser cumprido?
. Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Para garantir a preservação no longo prazo das informações contidas nos pacotes de informação de arquivo em um arquivo digital confiável deve definir medidas destinadas a evitar possível corrupção do fluxo de bits dos arquivos salvos e tomar precauções para evitar a perda de interpretabilidade do conteúdo. C24 especifica o C5 "Interpretabilidade" e traduz os planos do C11 "Medidas de preservação" em ação. As medidas técnicas na C24 estão documentadas na C 30 e C 31. Pré-condições para a C 24, de são proteção a nível técnico, preservação do fluxo de bits (C15).
Perguntas
- Se houver uma estratégia de migração: Que abordagem é adotada para a migração de formatos de arquivos obsolescentes e como é feita? Que medidas de garantia de qualidade existem? - Se existe uma estratégia de emulação: Como são selecionados os emuladores adequados pelo arquivo digital, os usuárioss ou processos automáticos? - Que outras ajudas de interpretação existem?
Documentos
Documentação das migrações realizadas, especificações dos emuladores, de uma estrutura de emulação, especificação de outras ajudas de interpretação (informações de representação).

C 25 Transformação de pacotes de informações de arquivo em informações de divulgação pacotes
O arquivo digital transforma os pacotes de informações de arquivo em pacotes de informações de divulgação.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Se um usuário de um arquivo digital confiável envia um pedido para o arquivo, ele normalmente emitiu um pacote de informações de divulgação. Este pacote de informações de divulgação deve ser criado a partir de um pacote de informações de arquivo pelo sistema em um processo de transformação. O pacote de informações de divulgação pode conter conteúdo e metadados das informações de um pacote de informação de arquivo e possivelmente metadados adicionais criados para o propósito específico. O processo de transformação deve ser especificado com um nível adequado de precisão; a conformidade deve ser transparente e verificável. O C25 é uma condição prévia para verificar a integridade e autenticidade da interface/utilização do usuário (C16, C19).
Perguntas
- Como é o processo para transformar os pacotes de informações de arquivo em pacotes de informação para divulgação especificados? Quais mudanças são feitas nos dados de conteúdo e metadados? - Quais medidas de garantia de qualidade existem?
Documentos
Especificação da transformação, descrição do processo.

C26 Pacotes de informações de divulgação
O arquivo digital especifica os pacotes de informação de divulgação com base nos requisitos das comunidades designadas.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Um arquivo digital de confiança deve ter especificações precisas para seus pacotes de divulgação de informação. Estes devem conter informações adequadas sobre os dados de conteúdo, sobre os metadados necessários para seu uso e sobre a estrutura dos pacotes. Os pacotes de divulgação de informação só podem conter uma parte das informações de conteúdo contidas em um pacote de informações de arquivo ou pode precisar ser transformado em um formato de arquivo diferente. Conformidade do novo pacote de divulgação de informação com as especificações devem ser verificáveis. A finalidade do critério C26 "Pacotes de informação de divulgação" é verificar estes critérios de qualidade para definir os pacotes de disseminação de informação. C26 está relacionado ao C3 "Comunidades Designadas" cujos requisitos precisam ser atendidos, e ao C4 "Acesso" que regula as questões básicas relativas ao uso.
Perguntas
- Em que medida as exigências das comunidades designadas são levadas em consideração? - São as possíveis partes constituintes e as estruturas do pacote de informações de divulgação especificado em detalhes suficientes e de uma forma compreensível para o usuário?
Documentos
Especificação dos pacotes de informações de divulgação

C27 Identificação
Um arquivo digital deve usar identificadores internos para gerenciar os objetos de informação e suas representações e, quando aplicável, suas partes e relações (parte/totalidade, diferentes variantes, versões etc.), especialmente para garantir a atribuição exclusiva dos dados de conteúdo aos metadados. O uso de identificadores persistentes, visíveis externamente e padronizados, garante o rastreamento confiável dos objetos de informação e suas representações, e consequentemente também acesso.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Os objetos de informação, suas representações e suas partes estão permanentemente ligados a cada outros. Esses links só podem ser preservados através do uso de identificadores persistentes. Os identificadores não devem mudar ao longo do tempo (ou seja, ser permanente) e deve ser criado usando uniformes especificações. Elas devem ser reconhecíveis por usuários externos, produtores e outros. Ao entrar no identificador, os usuários externos devem ser capazes de encontrar e usar o objeto requerido. Possível específico Os requisitos para identificadores são descritos, por exemplo, na norma *DIN* 13646 "*Requirements for the long-term handling* de identificadores persistentes".
Perguntas
- Quais identificadores o arquivo digital utiliza? - Qual procedimento tem sido utilizado para dar identificadores únicos a todos os objetos de informação, e suas partes, e a todo o conteúdo e metadados? - Como é conduzida a atribuição baseada em identificadores? - Como é garantida a permanência dos identificadores? - Como os identificadores são colocados à disposição dos usuários externos?
Documentos
Especificação dos identificadores internos e externos

C28 Metainformação descritiva
O escopo, estrutura e conteúdo dos metadados descritivos são definidos. Eles dependem dos objetivos do arquivo digital, suas comunidades designadas e os tipos de objetos.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Os metadados descritivos classificam e identificam o conteúdo dos dados que estão sendo arquivados, tornam possível rastrear e simplificar seu uso. De acordo com a natureza específica do papel do arquivo, seus métodos de trabalho e tradições, e dependendo do conteúdo a ser arquivado para qual comunidade designada, os metadados descritivos podem ter um conteúdo completamente diferente e estrutura e aderir a diferentes diretrizes de descrição. Estas incluem ambas padronizadas (por exemplo, DC ou EAD) e esquemas de metadados personalizados. Os nomes dos elementos dos metadados, o significado do o conteúdo e quaisquer campos obrigatórios devem ser determinados. A relação entre os metadados e os dados que estão sendo descritos são definidos.
Perguntas
- Quais regras para especificar os metadados descritivos que o arquivo digital utiliza? Quais as normas são implantadas? Até que ponto os objetivos, as comunidades designadas e o objeto tipos levados em consideração durante a especificação dos metadados descritivos? - Que medidas o arquivo digital toma para garantir que as diretrizes descritivas são observadas?
Documentos
Especificação dos metadados descritivos, notificação das diretrizes de descrição utilizadas, normas e auxílios, documentação da prática atual.

C29 Metadados estruturais
A estrutura das representações deve ser adequadamente descrita para que os objetos de informação possam ser reconstruídos e utilizados.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Uma representação de um objeto de informação arquivado pode consistir em muitos componentes técnicos (geralmente arquivos individuais) que só se tornam totalmente compreensíveis quando montado em um contexto estruturado (por exemplo, a ordem das páginas de um livro ou dos documentos em um arquivo). Dependendo do tipo de objeto a ser arquivado, os metadados estruturais servem para renderizar o contexto completo do objeto de informação transparente e para torná-lo utilizável.
Perguntas
- Quais metadados estruturais o arquivo digital utiliza? Até que ponto ele reflete os diferentes tipos de objetos? Quais padrões são implantados? - Que medidas o arquivo digital utiliza para garantir que os metadados estruturais possam ser utilizados para reproduzir a estrutura autêntica de diferentes representações?
Documentos
Especificação dos metadados estruturais, notas sobre as normas utilizadas.

C30 Metainformação técnica
Os metadados técnicos são definidos para garantir a interpretabilidade, integridade e autenticidade e para gerenciar as medidas de preservação.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Os metadados técnicos descrevem os objetos arquivados de um ponto de vista técnico. Eles simplificar a documentação da completude e integridade do estoque de arquivo, facilitar a adequação formulários de acesso e são necessários para a gestão técnica das medidas de preservação. Que Os metadados necessários dependem, por exemplo, do tipo de objeto, da estratégia de preservação escolhida e de os objetivos e as comunidades designadas do arquivo particular. O conceito PREMIS contém um padrão comum para metadados técnicos.
Perguntas
- Quais metadados técnicos são coletados? Quais padrões são implantados? - Quais processos (por exemplo, migração, provisão) e status (por exemplo, integridade, autenticidade) são apoiados ou documentados por quais metadados?
Documentos
Especificação dos metadados técnicos, notificação das normas utilizadas.

C31 Registro das medidas de preservação
O arquivo digital registra as medidas de preservação e quaisquer mudanças nas representações.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Durante o processo de arquivamento, as representações transferidas devem ser repetidamente transformadas em novas representações ou serem expandidas para incluir emuladores (migração ou emulação estratégia). Essas mudanças têm um impacto direto sobre a integridade e autenticidade do arquivo representações e objetos de informação e devem ser sistemática e permanentemente registrados para garantir que todos os processos de mudança permaneçam transparentes. Deve ser possível visualizar os logs. O PREMIS contém um padrão comum para medidas de preservação de madeira.
Perguntas
- Que medidas e mudanças são registradas? - Como as medidas e mudanças são registradas (por exemplo, automaticamente, manualmente)? Os agentes são quem está envolvido nas mudanças documentadas? Que normas são implantadas? - Que medidas são tomadas para garantir que as entradas de registro permaneçam legíveis, compreensíveis e utilizáveis no futuro?
Documentos
Sistema para medidas de preservação de registro, especificação de metadados, notificação de normas utilizadas.

C32 Metainformação administrativa
. O arquivo digital definiu seus metadados administrativos a fim de tornar a administração e uso transparente dos objetos de informação e de suas representações. O uso das representações pode ser restrito por razões legais ou contratuais.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
A administração interna e o acesso aos objetos digitais arquivados devem ser conduzidos em uma base técnica organizada, por razões legais ou contratuais. Os metadados administrativos necessários devem ser coletados sistematicamente para que somente as medidas permitidas (por exemplo, armazenamento múltiplo, migração, etc. e acesso para usuários autorizados) podem ser realizadas. Quais dados são realmente necessários depende da base legal do arquivo digital, seus objetos e grupos de usuários.
Perguntas
- Quais metadados administrativos são coletados? Quais regulamentos e normas são baseados em? - Que relação os metadados administrativos têm com as informações em C6 e C7?
Documentos
Especificação dos metadados administrativos, notificação das normas utilizadas.

C33 Infraestrutura de TI
A infraestrutura de TI deve realizar as especificações para o manuseio dos objetos de informação e representações a nível tecnológico e de segurança.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
O objetivo da infraestrutura de TI é implementar a tecnologia e a segurança requisitos especificados no documento C13-26. Assim, a infraestrutura deve ser descrita em termos abstratos, embora seu funcionamento não precise ser testado de forma exaustiva. A própria infraestrutura de TI do arquivo ou que (parcialmente) operado por um prestador de serviços consiste em hardware, cabeamento, software e interfaces necessário para operar o arquivo de preservação. O objetivo do C33 é verificar e fazer transparente a adequação, confiabilidade, segurança e perspectivas futuras desta infraestrutura.
Perguntas
- Qual infraestrutura de TI existe? - Quais são as relações entre as decisões estruturais concretas e outras decisões funcionais e decisões técnicas (cf. C13-26)? - Quais normas e diretrizes foram implementadas como resultado? - Que medidas estão planejadas para manter a infraestrutura de TI atualizada?
Documentos
Documentação técnica, representação gráfica da infraestrutura de TI (onde apropriado)

C34 Segurança
A organização e a infraestrutura protegem o arquivo digital e seus objetos de informação arquivados e representações.
Em que medida o critério deve ser cumprido?
Uma média de 7 pontos deve ser alcançada na avaliação dos critérios aplicáveis C13 - C34.
Explicação
Cada arquivo digital de confiança deve implementar medidas adequadas para proteger seu próprio integridade e de seus bens de arquivo para garantir que os bens permaneçam intactos e para cumprir suas obrigações legais ou obrigações contratuais. Tais medidas devem ser baseadas na identificação de seções do arquivo que são dignas de proteção, uma análise de qualquer ameaça potencial para o arquivo específico e um risco avaliação dos cenários de danos e, em última análise, resultar em um sistema de segurança consistente (por exemplo, com a ajuda de DRAMBORA).
Perguntas
- Quais partes do arquivo digital são dignas de proteção e até que ponto? - Quais cenários de dano baseados em ações maliciosas, erro humano ou falha técnica você considera como representando uma ameaça particular para a preservação dos objetos de informação e representação? Qual é a probabilidade de tais cenários de danos? Qual é a gravidade dos danos? Que nível de risco residual é aceitável? - Que medidas estão sendo tomadas para combater as ameaças? - Como a análise de risco e as contra-medidas planejadas foram transformadas em sistema de segurança? Quais normas e diretrizes estão sendo implementadas? - Quais medidas estão sendo planejadas para testar o sistema de segurança e seu posterior desenvolvimento?
Documentos
Sistema de segurança de TI e outros sistemas de segurança de infraestrutura

APÊNDICE C - LISTA DE CRITÉRIOS PARA AUDITORIA E CERTIFICAÇÃO DE REPOSITÓRIOS DIGITAIS CONFIÁVEIS - TRAC[129]

A. Infraestrutura Organizacional

A1. Governança e viabilidade organizacional

Independentemente do tamanho, escopo ou natureza do programa de preservação digital, um repositório confiável deve demonstrar um compromisso explícito, tangível e de longo prazo com o cumprimento das normas vigentes, políticas e práticas.

A1.1 O repositório possui uma declaração de missão que reflete um compromisso com a retenção no longo prazo, gerenciamento e acesso a informações digitais.

A declaração de missão do repositório deve ser claramente identificada e acessível aos depositantes e outras partes interessadas e contêm um compromisso explícito de longo prazo.

A1.2 O repositório possui um plano de sucessão formal apropriado, planos de contingência e / ou acordos de custódia em vigor no caso do repositório deixar de operar ou o governo ou instituição financiadora altererem substancialmente seu escopo.

Parte da promessa de cuidado perpétuo do repositório é o compromisso de identificar sucessores ou arranjos, se necessário. É necessário considerar essa responsabilidade enquanto o repositório ou dados são viáveis - não quando ocorre uma crise - para evitar perdas irreparáveis. Organizacionalmente, os dados em um repositório podem estar em risco, independentemente de o repositório ser executado por uma organização comercial ou uma entidade governamental (biblioteca ou arquivo nacional). Nos repositórios e arquivos gerenciados pelo governo, uma mudança de governo que altera, significativamente, o financiamento, a missão, o escopo de coleta ou o pessoal

da instituição pode colocar os dados em risco. Esses riscos são semelhantes aos enfrentados pelos repositórios de setores comerciais e de pesquisa e devem ser minimamente abordados, por planos de sucessão para coleções significativas dentro do repositório maior.

Um plano formal de sucessão deve incluir a identificação de herdeiros confiáveis, se aplicável, e o retorno de objetos digitais aos depositantes com notificação prévia adequada etc. Se um plano formal de sucessão não existe, o repositório deve poder apontar para indicadores que formariam a base de um plano, por exemplo, parceiros, declarações de compromisso, prováveis herdeiros. Os planos de sucessão não precisam especificar a transferência de todo repositório para uma única organização, se isso não for viável. Vários herdeiros são possíveis, desde que os dados permaneçam acessíveis.

A2. Estrutura organizacional e pessoal

Um repositório deve ter pessoal designado com as competências e a formação necessárias e deve proporcionar o desenvolvimento de uma formação contínua. O repositório deve ser capaz de documentar os esforços para definir e manter as competências necessárias, papéis, descrições de funções e planos de desenvolvimento.

A2.1 O Repositório identificou e estabeleceu as funções que deve desempenhar e tem pessoal nomeado com competências e experiência adequadas ao desempenho destas funções.

O repositório deve identificar as competências e os conjuntos de aptidões necessários para o seu funcionamento, ao longo do tempo, e demonstrar que o pessoal e os consultores possuem o leque de competências necessárias, por exemplo, formação em arquivo, competências técnicas e jurídicas.

A2.2 O repositório tem o número adequado de funcionários para apoiar todas as funções e serviços.

O pessoal do repositório deve ser adequado ao âmbito e à missão do programa de arquivamento. O repositório deve ser capaz de demonstrar um esforço para determinar o número e o nível adequados de pessoal que corresponde aos requisitos e compromissos. (Esses requisitos estão relacionados com o núcleo de funcionalidades abrangidas, por um processo de certificação. De especial

interesse para a certificação de repositórios é se a organização dispõe de pessoal adequado para apoiar as atividades relacionadas com a preservação, em longo prazo, dos dados). Os compromissos acumulados do repositório podem ser identificados em contratos de depósito, contratos de serviço, licenças, declarações de missão, planos de trabalho, prioridades, metas e objetivos. Mão de obra ou incompatibilidade entre compromissos e pessoal indicam que o repositório não pode cumprir seus acordos e requisitos.

A2.3 O Repositório dispõe de um programa de desenvolvimento profissional ativo que proporciona ao pessoal oportunidades de desenvolvimento de competências e conhecimentos.

A tecnologia continuará a mudar, pelo que o repositório deve assegurar que os conjuntos de competências do seu pessoal evoluam, idealmente, por meio de uma abordagem de aprendizagem, ao longo da vida, para desenvolver e reter o pessoal. Como os requisitos e as expectativas relativas a cada área funcional evoluem, o repositório deve demonstrar que o pessoal é preparado para enfrentar novos desafios.

A3. Responsabilidade processual e enquadramento político

Um repositório deve fornecer uma documentação clara e explícita dos seus requisitos, decisões e desenvolvimento, e ações para garantir a preservação no longo prazo e o acesso aos conteúdos digitais aos seus cuidados. Essa documentação assegura aos consumidores, gestores, produtores e certificadores que o repositório cumpre os seus requisitos e desempenha plenamente o seu papel de repositório digital de confiança. Certificação, o indicador mais claro de uma prática sólida e baseada em padrões do repositório, é facilitada pela responsabilidade processual que resulta em políticas, procedimentos e práticas abrangentes e atuais.

A3.1 O Repositório definiu a(s) sua(s) comunidade(s) designada(s) e os conhecimentos associados e dispõe de definições e políticas acessíveis ao público para ditar a forma como seus serviços de preservação serão cumpridos.

A definição da(s) comunidade(s) designada(s) (comunidade de produtores e utilizadores) é alcançada por meio de processos de planejamento utilizados para criar o repositório e definir os seus serviços. A definição será extraída de várias

fontes, desde estudos de mercado a acordos de nível de serviço para os produtores até a missão ou âmbito da instituição em que o repositório se encontra integrado.

Satisfazer as necessidades da comunidade designada - a compreensibilidade esperada da informação, e não apenas o acesso à mesma afetará a gestão do objeto digital, bem como a infraestrutura técnica do repositório global. Para um planejamento adequado, em longo prazo, o repositório ou organização deve compreender e instituir políticas de apoio a essas necessidades.

Para uma determinada apresentação de informações, o repositório deve indicar, claramente, a definição operacional de compreensibilidade que está associada à(s) comunidade(s) designada(s) correspondente(s). A(s) comunidade(s) designada(s) pode(m) variar de uma apresentação para outra, tal como a definição de compreensibilidade que estabelece a responsabilidade do repositório nessa área. Isso pode ir, desde a ausência de responsabilidade, se os *bits* forem apenas para preservação, para a manutenção de um determinado nível de utilização, se os membros da(s) comunidade(s) designada(s) está(ão) determinado(s) fora do repositório, a uma responsabilidade de assegurar um dado nível de compreensão humana da(s) comunidade(s) designada(s), que exige(m) uma representação da informação adequada.

A documentação da compreensibilidade incluirá, normalmente, uma definição das aplicações que a(s) comunidade(s) designada(s) utilizará(ão) com a informação, eventualmente após transformação por serviços do repositório. Por exemplo, se uma comunidade designada for definida como sendo constituída por leitores de inglês com acesso a serviços de ferramentas de elaboração de documentos disponíveis, e se essa definição estiver claramente associada a um determinado conjunto de conteúdos de Informação de Conteúdo e Informação de Descrição para Preservação, então o requisito é cumprido.

A3.2 O Repositório tem procedimentos e políticas em vigor e mecanismos para a sua revisão, atualização, e desenvolvimento à medida que o repositório cresce e à medida que a tecnologia e a prática comunitária evoluem.

As políticas e procedimentos do repositório devem ser completos, escritos ou disponíveis de uma forma tangível, permanecerem atuais e devem evoluir de modo a refletir a evolução dos requisitos e das práticas. O repositório deve

demonstrar que existe uma auditoria e manutenção de políticas e procedimentos e que estes são regularmente aplicados. As políticas e os procedimentos devem incidir em áreas nucleares, incluindo, por exemplo, requisitos de transferência, apresentação, controle de qualidade, gestão de armazenamento, planejamento de catástrofes, gestão de metadados, acesso, gestão de direitos, estratégias de preservação, pessoal e segurança. Os documentos de alto nível devem fazer compromissos organizacionais e intenções claras. Os documentos de nível inferior devem tornar claras as práticas quotidianas e os procedimentos. As versões desses documentos devem ser bem geridas pelo repositório (por exemplo, versões desatualizadas são claramente identificadas ou mantidas off-line) e o pessoal qualificado e os seus pares devem estar envolvidos em revisão, atualização e extensão desses documentos. O repositório deve ser capaz de documentar os resultados do acompanhamento de desenvolvimentos relevantes; capacidade de resposta às normas e práticas vigentes, requisitos e normas emergentes que sejam específicos do domínio, se for caso disso; e normas semelhantes desenvolvimentos. O repositório deve ser capaz de demonstrar que definiu "uma documentação" para o repositório.

A3.3 O Repositório mantém políticas escritas que especificam a natureza de quaisquer autorizações legais necessárias para preservar os conteúdos digitais ao longo do tempo, e o repositório pode demonstrar que estas autorizações tem sido adquiridas quando necessário.

Uma vez que o direito de mudar ou alterar a informação digital é, frequentemente, limitado por lei ao criador, é importante que os repositórios digitais respondam à necessidade de poder trabalhar com o digital e, eventualmente, modificar objetos para mantê-los acessíveis ao longo do tempo. Os repositórios devem ter políticas e acordos escritos com depositantes que especifiquem e/ou transfiram determinados direitos para o repositório, permitindo a sua adequada e necessária ação de preservação a realizar nos objetos digitais dentro do repositório.

Pelo fato de que as negociações jurídicas possam levar tempo, atrasando ou impedindo, potencialmente, a ingestão de objetos digitais em risco, um repositório digital pode acolher ou aceitar objetos digitais mesmo com apenas direitos de preservação mínimos, utilizando um acordo aberto e abordar mais tarde direitos mais pormenorizados. Os direitos de um repositório devem, pelo

menos, limitar sua responsabilidade ou mitigar a exposição legal que ameace o próprio repositório. Um repositório sem controle suficiente da informação estará, juridicamente, em risco.

A3.4 O Repositório compromete-se a proceder a uma revisão e avaliação formal e periódica para assegurar capacidade de resposta aos desenvolvimentos tecnológicos e à evolução das necessidades.

A preservação, em longo prazo, é uma responsabilidade partilhada e complexa. Um repositório digital de confiança contribui para beneficiar-se da amplitude e profundidade das normas e práticas baseadas na comunidade. A revisão regular é necessária para o desenvolvimento contínuo e saudável do repositório. O contexto organizacional do repositório deve determinar a frequência, a extensão e o processo de autoavaliação. O repositório deve também ser capaz de fornecer um conjunto específico de requisitos que tenha definido, mantendo-se e se esforçando para se fazer conhecido. (Ver também A3.9.)

A3.5 O Repositório tem políticas e procedimentos para assegurar que as reações dos produtores e utilizadores sejam buscadas e abordadas ao longo do tempo.

O repositório deve ser capaz de demonstrar que cumpre requisitos explícitos, que sistematicamente e rotineiramente procura o *feedback* das partes interessadas para monitorar as expectativas e os resultados, e que este pode responder à evolução das necessidades.

A3.6 O Repositório tem um histórico documentado das alterações às suas operações e procedimentos, softwares e hardwares que, se for caso disso, estejam ligados à estratégias de preservação relevantes e descreve os efeitos potenciais na preservação dos conteúdos digitais.

O repositório deve documentar toda a gama das suas atividades e desenvolvimentos, ao longo do tempo, incluindo decisões sobre a infraestrutura organizacional e tecnológica. Se o repositório utiliza *software* para documentar este histórico, deve ser capaz de demonstrar esse rastreio.

A3.7 O Repositório compromete-se a garantir a transparência e a responsabilidade em todas as ações de apoio à operação e gestão do

repositório, especialmente às que afetam a preservação de conteúdos digitais ao longo do tempo.

A transparência é a melhor garantia de que o repositório funciona de acordo com as normas aceitas e práticas. A transparência é essencial para a responsabilização, e ambas são alcançadas, por meio de uma prática ativa e contínua de documentação. O repositório deverá ser capaz de documentar os seus esforços no sentido de produzir informações sobre seu desenvolvimento, implementação, evolução e desempenho disponíveis e acessíveis às partes interessadas. Os meios de comunicação habituais que uma organização utiliza para fornecer notícias significativas e as atualizações às partes interessadas devem ser suficientes para satisfazer esse requisito.

A3.8 O Repositório compromete-se a definir, recolher, acompanhar e fornecer, a pedido, suas medições de integridade da informação.

O repositório deve desenvolver ou adaptar medidas adequadas para garantir a integridade das suas explorações. Os mecanismos para medir a integridade evoluirão à medida que a tecnologia evolui, mas, atualmente, incluem exemplos como a utilização de verificadores de valor na entrada e ao longo do processo de conservação. A cadeia de custódia para a totalidade do seu conteúdo digital a partir do ponto de depósito deve ser explícito, completo, correto e atual. O repositório deve demonstrar que o conteúdo que possui corresponde ao conteúdo que recebeu, por exemplo, com uma função de registro implementada que documenta o conteúdo a partir do envio. Perdas associadas à migração e outras ações de preservação também devem ser documentadas e disponibilizadas às partes interessadas. (Veja C1.5 e C1.6.)

Se os protocolos, regras e mecanismos estiverem incorporados no software do repositório, deverá haver alguma forma de demonstrar a implementação de medições de integridade.

A3.9 O Repositório compromete-se a cumprir um calendário regular de autoavaliação e certificação e, se certificado, compromete-se a notificar os organismos de certificação de alterações operacionais que irão mudar ou anular o seu estatuto de certificação.

Um repositório não pode se autocertificar, porque uma medição objetiva, externa, utilizando uma medição consistente e um processo de certificação

repetível é necessário para assegurar e demonstrar que o repositório reúne e irá, provavelmente, continuar a satisfazer os requisitos de preservação. Por conseguinte, a certificação é o melhor indicador de que o repositório cumpre os seus requisitos, cumpre o seu papel e adere às normas adequadas. O repositório deve demonstrar que integra a preparação e a resposta à certificação nas suas operações e no seu planejamento. (Ver também A3.4.)

A4. Sustentabilidade financeira

Um repositório digital confiável deve poder provar a sua sustentabilidade financeira. No geral, um repositório digital confiável adere a todas as boas práticas de negócios e deve ter um plano de negócios sustentável - um conjunto de documentos que reflitam o passado, presente e futuro do repositório e suas atividades. Um plano de negócio incorpora planos de gestão e implicações financeiras relacionadas ao desenvolvimento e atividades-padrão de produção e pode observar as estratégias e / ou riscos que afetariam as operações.

A capacidade comercial e financeira normal deve ser revista pelo menos anualmente. Procedimentos-padrão de contabilidade devem ser utilizados. Tanto os ciclos de planejamento financeiro, a curto ou longo prazo, deverão demonstrar um equilíbrio permanente de risco, benefícios, investimentos e despesas. Os orçamentos de exploração e as reservas devem ser adequados.

A4.1 O Repositório dispõe de processos de planejamento empresarial de curto e longo prazo para sustentar o repositório ao longo do tempo.

O repositório deve demonstrar que possui processos formais, cíclicos e pró-ativos de planejamento empresarial em condições. Uma breve descrição do plano de negócios do repositório deve mostrar como o repositório irá gerar rendimentos e ativos, pelos serviços, parcerias com terceiros, subsídios, etc. Quanto ao ponto A1.2 (planejamento sucessório/de contingência/garantia), o repositório deve estabelecer esses processos quando for viável para evitar crises empresariais. Essas questões podem ser pertinentes para esse requisito:

- Ao abrigo desse plano, em que medida o repositório é apoiado, ou espera-se que seja apoiado, por receitas de organizações e agências que contribuam com conteúdos, tais como editoras?
- Em que medida o repositório é apoiado, ou espera-se que seja apoiado, por receitas provenientes de assinantes ou instituições assinantes?

- Que medidas estão em vigor, caso existam, para limitar o acesso das partes interessadas não assinantes?
- Que incentivos financeiros são oferecidos, caso existam, para desencorajar os assinantes de adiar a seu investimento no repositório? De descontinuar o investimento no repositório?
- Em que medida é o repositório apoiado ou espera-se que seja apoiado, por outras partes?
- Como os principais custos futuros, tais como migrações, melhorias de capital, aprimoramentos, proporcionando o acesso em caso de falha da editora, etc., serão distribuídos entre editores, assinantes, e outras partes apoiadoras?
- Que planos de contingência existem para cobrir a perda de receitas futuras e/ou financiamento externo?
- Em caso de falha catastrófica, os ativos de reserva são suficientes para assegurar o restabelecimento de acesso dos assinantes aos conteúdos de forma razoavelmente rápida?
- Se este é um repositório nacional ou patrocinado pelo governo, como ele é isolado de eventos políticos, conflitos internacionais ou crises diplomáticas, que podem afetar sua capacidade de servir círculos estrangeiros?

A4.2 O repositório possui processos para revisar e ajustar os planos de negócios pelo menos anualmente.

O repositório deve demonstrar o seu empenho no planejamento pró-ativo do negócio, executando processos cíclicos de planejamento, pelo menos anualmente. O repositório deve ser capaz de demonstrar a sua capacidade de resposta a resultados da auditoria, por exemplo.

A4.3 As práticas e procedimentos financeiros dos repositórios são transparentes, em conformidade com normas e práticas contabilísticas relevantes, e auditadas por terceiros de acordo com requisitos legais territoriais.

O repositório não pode apenas reivindicar transparência, tem de demonstrar que ajusta as suas práticas comerciais para manter transparentes, conformes e passíveis de auditoria. Os requisitos de confidencialidade podem proibir a produção de informação sobre as finanças públicas do repositório, mas o

repositório deve poder demonstrar que é tão transparente quanto necessário e pode estar de acordo com âmbito da sua comunidade.

A4.4 O Repositório tem um compromisso contínuo de analisar e relatar os riscos e benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).

O repositório deve comprometer-se, pelo menos, com essas categorias de análise e relato, e manter um equilíbrio adequado entre eles. O repositório deve ser capaz de demonstrar que identificou e documentou essas categorias e gere-as ativamente, incluindo a identificação e resposta aos riscos, descrevendo e alavancando os benefícios, especificando e equilibrando os investimentos, e antecipando e preparando-se para despesas.

A4.5 O Repositório compromete-se a acompanhar e a fazer pontes entre as lacunas de financiamento.

O repositório deve reconhecer a possibilidade de lacunas entre o financiamento e os custos de atender aos compromissos do repositório com seus interessados. Compromete-se a construir pontes entre essas lacunas, garantindo financiamento e compromissos de recursos, especificamente, para esse fim; esses compromissos podem advir do próprio repositório ou organizações-mãe, conforme aplicável. Mesmo com procedimentos eficazes de planejamento de negócios em vigor, qualquer repositório com compromissos, de longo prazo, provavelmente enfrentará algum tipo de lacuna de recursos no futuro. O repositório deve fornecer essencialmente um amortecedor de seguro como primeira - e espero que seja eficaz - defesa, evitando a necessidade de invocar um plano de sucessão, exceto em situações extremas, como a repositório interromper operações permanentemente.

A5. Contratos, licenças e responsabilidades

Os contratos, licenças e responsabilidades de um repositório devem ser explícitos. Devem definir claramente e em termos mensuráveis; delimitar funções, responsabilidades, prazos e condições; e ser facilmente acessíveis ou disponíveis às partes interessadas, a pedido. Os contratos incluem os celebrados entre o repositório e proprietários de conteúdos (depositantes, editores, etc.) e os que se encontram entre o repositório e o seu próprio serviço fornecedores (contratos de serviços/manutenção

do sistema), com os desenvolvedores do sistema, etc. Independentemente da relação, estes contratos e licenças devem estar disponíveis para auditorias, de modo a que as responsabilidades e riscos possam ser avaliados.

A5.1 Se o repositório gerir, preservar e/ou fornecer acesso a materiais digitais em nome de outra organização, tem e mantém contratos ou acordos de depósito adequados.

Os repositórios, especialmente os que têm acordos de depósito de terceiros, devem garantir contratos relevantes, licenças ou acordos de depósito que expressam os direitos, responsabilidades e expectativas de cada parte. Os contratos e os acordos formais de depósito devem ser rubricados e atuais.

Quando a relação entre depositante e depositário é menos formal (ou seja, um membro facultativo que deposita um trabalho no repositório de preservação de uma instituição acadêmica), a documentação que articula a capacidades e compromissos do repositório devem ser fornecidas a cada depositante.

Os repositórios envolvidos no arquivamento da Web podem ter dificuldade em cumprir este requisito devido à forma como a informação de base Web é colhida/capturada para preservação no longo prazo. Este tipo de dado raramente é adquirido com contratos ou acordos de depósito. Pela sua própria natureza, a informação digital na Web é entendida como pertencendo a "todos e a ninguém". Alguns repositórios capturam, gerem e preservam o acesso a este material sem autorização escrita dos criadores do conteúdo. Outros passam pelo muito demorado e dispendioso processo de contatar os proprietários de conteúdos antes de captar e ingerir informações. Independentemente dos processos, repositórios de recolhimento e ingestão de materiais baseados na Web devem articular as suas questões de direitos no âmbito das políticas de acesso público, e dispor de mecanismos para responder aos proprietários dos conteúdos se os direitos do repositório de recolher e preservar certas informações são contestados.

Idealmente, estes acordos serão acompanhados, ligados, geridos e tornados acessíveis numa base de dados de contratos.

A5.2 Os contratos de repositório ou acordos de depósito devem especificar e transferir todos os elementos necessários direitos de conservação, devendo esses direitos transferidos ser documentados.

Uma vez que o direito de mudança ou alteração da informação digital é frequentemente limitado por lei ao criador, é importante que os contratos e acordos relativos aos repositórios digitais respondam à necessidade de ser possível trabalhar e modificar potencialmente os objetos digitais para mantê-los acessíveis. Os acordos dos repositório com os depositantes devem especificar e/ou transferir determinados direitos para o repositório que permitam a sua conservação adequada e ações necessárias para os objetos digitais dentro do repositório. (Este requisito está ligado ao ponto A3.3).

Porque as negociações jurídicas podem demorar tempo, prevenindo ou retardando potencialmente a ingestão de objetos digitais em risco, é aceitável que um repositório digital acolha ou aceite objetos digitais mesmo com apenas um mínimo direitos de preservação com base num acordo aberto e, posteriormente, trate da expansão para direitos pormenorizados. Os direitos de um repositório devem, pelo menos, limitar a responsabilidade ou exposição legal do repositório que ameace a repositório propriamente dito.

A5.3 O Repositório especificou todos os aspectos adequados da aquisição, manutenção e acesso, e a retirada em acordos escritos com os depositantes e outras partes relevantes.

O contrato de depósito especifica todos os aspectos dessas questões que são necessários para que o repositório carregue sua função. Pode haver um único contrato cobrindo todos os depósitos, ou contratos específicos para cada depósito, ou um contrato padrão complementado por condições especiais para alguns depósitos. Estas condições especiais podem acrescentar ou anular alguns aspectos do contrato padrão. Os contratos podem ter que cobrir restrições de acesso e terão que cobrir todos os direitos de propriedade nos objetos digitais. Os acordos podem colocar responsabilidades sobre os depositantes, tais como assegurar que a submissão os Pacotes de Submissão de Informação (SIPs) estejam em conformidade com alguns padrões pré-acordados, e podem permitir que os repositórios recusem SIPs que não atendam a esses padrões. Outros repositórios podem se responsabilizar pela correção de erros nos SIPs. A divisão de responsabilidades deve ser sempre clara. Os acordos, escritos ou não, nem sempre podem ser necessário. O ônus da prova recai sobre o repositório para demonstrar que ele não precisa de tais acordos, por exemplo, porque tem um mandato legal para suas atividades.

Um acordo deve incluir, no mínimo, direitos de propriedade, direitos de acesso, condições para a retirada, nível de segurança, nível de busca, definições de SIP, tempo, volume e conteúdo das transferências. Um exemplo de um padrão a seguir para isso é a Metodologia CCSDS/ISO de Interface Produtor-Arquivo Padrão abstrato.

A5.4 Pistas de repositório e gestão dos direitos de propriedade intelectual e restrições à utilização de conteúdo do repositório, conforme exigido pelo acordo de depósito, contrato ou licença.

O repositório deve ter um mecanismo de rastreamento de licenças e contratos aos quais é obrigado.

Qualquer que seja o formato do sistema de rastreio, deve ser suficiente para a instituição rastrear, atuar e verificar os direitos e restrições relacionados com a utilização dos objetos digitais dentro do repositório.

A5.5 Se os repositórios de conteúdos digitais com propriedade/direitos pouco claros, as políticas estão alocadas para enfrentar a responsabilidade e os desafios a esses direitos.

As políticas e mecanismos do repositório devem ser examinados pelas autoridades institucionais adequadas e/ou peritos jurídicos para garantir que as respostas aos desafios cumpram a legislação e os requisitos pertinentes e que a responsabilidade potencial pelo repositório é minimizada.

B. Gestão de Objetos Digitais

As responsabilidades de gestão de objetos digitais de um repositório incluem tanto alguns aspectos "organizacionais" quanto técnicos relacionados com estas responsabilidades, tais como funções, processos e procedimentos de repositório necessários para ingerir, gerir e proporcionar o acesso a objetos digitais no longo prazo.

Requisitos para estas funções são categorizadas em seis grupos com base na funcionalidade de arquivo, permitindo o agrupamento no âmbito das entidades funcionais do OAIS:

- B1: A fase inicial da ingestão que trata da aquisição de conteúdos digitais.
- B2: A fase final de ingestão que coloca os conteúdos digitais adquiridos nos formulários, frequentemente referidos como Pacotes de Informação Arquivística (AIPs), utilizados pelo repositório para preservação no longo prazo.

- B3: Estratégias de preservação atuais, sólidas e documentadas, bem como mecanismos para mantê-las atualizadas face à evolução dos ambientes técnicos.
- B4: Condições mínimas para a conservação no longo prazo dos AIPs.
- B5: Metadados de nível mínimo para permitir a localização e gestão de objetos digitais dentro do sistema.
- B6: Capacidade do repositório para produzir e difundir versões exatas e autênticas dos objetos digitais AIPs.

Os requisitos aqui estabelecidos assumem a familiaridade com o OAIS e/ou com as práticas de repositório pormenorizadas.

B1. Ingestão: aquisição de conteúdos

A aquisição envolve uma interação crucial entre o repositório e o depositante. O sucesso nesta fase de ingestão indica a capacidade do repositório para obter controle suficiente sobre o conteúdo.

Os repositórios são provavelmente os que mais diferem nesta área de processos de ingestão, dependendo do tipo de material que recolhem e as suas relações com os seus produtores. Para qualquer repositório, pode ser indicado com alguma confiança que a ingestão termina quando um Pacote de Informação para arquivamento (AIP) e os seus metadados associados estão seguros no repositório, incluindo a criação de quaisquer cópias de segurança. É mais difícil fazer uma declaração geral sobre quando começa a ingestão. Alguns repositórios terão conteúdos submetidos pelos produtores, talvez inesperadamente. Outros irão procurar ativamente conteúdo e solicitá-lo dos produtores. Algumas relações produtor-repositório serão mais colaborativas, tornando-as menos claras que inicia uma determinada transação.

As relações entre produtores e repositórios que afetam a ingestão podem ser muito diferentes na sua formalidade e na medida em que as obrigações são impostas a diferentes partes. Arquivos nacionais, depósitos (direitos de autor) bibliotecas e repositórios institucionais podem ser capazes de obrigar os seus produtores (agências governamentais e editores) a fornecer conteúdos, mas pode ter pouco ou nenhum controle sobre a sua forma. Os outros repositórios não podem ser capazes de obrigar os produtores a oferecer conteúdos, mas podem ser capazes de selecionar a forma de conteúdo aceitável, se isso se aplica, por exemplo, aos formatos dos ficheiros ou às normas mínimas de metadados. Alguns repositórios podem ter pouca ou nenhuma relação com os produtores do conteúdo que preservam.

Dadas estas diferenças, algumas das exigências aqui são muito gerais e exigem julgamentos sobre o que é apropriado para um repositório, dada a sua missão declarada e as necessidades do repositório comunidade(s) designada(s). Mas o resultado que todos os repositórios estão a tentar alcançar é o mesmo: preservar o conteúdo isso é compreensível e utilizável no longo prazo. Para informações mais detalhadas e debates aprofundados de ingestão e aplicabilidade.

B1.1 O Repositório identifica propriedades que irá preservar para objetos digitais.

Este processo começa, em geral, com a declaração de missão do repositório e pode ser especificado com mais pormenor em acordos de pré-adesão com

produtores ou depositantes (por exemplo, acordos produtor-arquivo) e que muito específico nos acordos de depósito ou transferência para objetos digitais específicos e respectiva documentação.
Por exemplo, um repositório só pode comprometer-se a preservar o conteúdo textual de um documento e não seu aspecto exato numa tela. Outro pode querer preservar a aparência exata e a disposição do documento textual, enquanto outros podem optar por normalizar os dados durante o processo de ingestão.

B1.2 O Repositório especifica claramente as informações que devem ser associadas ao material no momento do seu depósito (isto é, SIP).
Para a maioria dos tipos de objetos digitais a serem ingeridos, o repositório deve ter critérios escritos, preparados pelo repositório, por si só ou em conjunto com outras partes, que especifique exatamente quais o(s) objeto(s) digital(ais) transferidos, que documentação está associada ao(s) objeto(s) e quaisquer restrições de acesso, quer seja técnica, regulamentar ou imposta pelo doador.
O nível de precisão destas especificações variará em função da natureza da política de recolhimento do repositório e a sua relação com os criadores. Por exemplo, os repositórios que se dedicam à colheita na Web, ou aqueles que resgatam materiais digitais muito depois dos seus criadores os terem abandonado, não pode impor condições aos criadores de material, uma vez que não são "depositantes" no sentido habitual da palavra. Mas os ceifeiros - debulhadores podem, por exemplo, decidir quais os elementos de metadados das transações *HTTP* que captaram num sítio são passíveis de serem preservados juntamente com os arquivos do site, e isto ainda constitui "informação associada ao material digital". Podem também optar por registrar as informações ou decisões - quer sejam tomadas por seres humanos, quer por algoritmos automáticos - o que levou a que site fosse capturado.

B1.3 O Repositório tem mecanismos para autenticar a origem de todos os materiais.
Os procedimentos operacionais normalizados escritos do repositório e as práticas reais devem garantir que os objetos digitais são obtidos da fonte esperada, que a proveniência adequada foi mantida e que os objetos são os objetos esperados. A confirmação pode utilizar vários meios, incluindo, entre outros, o tratamento digital, verificação e validação dos dados e através do

intercâmbio de instrumentos adequados de propriedade (por exemplo, acordos de apresentação/acordo de depósito/acordo de doação).

B1.4 O processo de ingestão do Repositório verifica a exaustividade de cada objeto apresentado (ou seja, o SIP) e exatidão, tal como especificado no ponto B1.2.

As informações recolhidas durante o processo de ingestão devem ser comparadas com as informações de outras fontes - as expectativas do produtor ou do próprio repositório - para verificar a correção da transferência de dados e ingerir o processo. À medida que um repositório pode determinar a correção dependerá do que sabe sobre o SIP e que ferramentas estão disponíveis para verificar a sua correção. Isto pode significar simplesmente verificar se os formatos de arquivo são o que eles dizem ser (arquivos TIFF são formatos TIFF válidos, por exemplo), ou podem implicar na verificação do conteúdo. Isto pode envolver a verificação humana em alguns casos, tais como a confirmação de que a descrição de uma imagem corresponde à imagem.

Os repositórios devem ter estabelecido procedimentos para o manuseio de SIPs incompletos. Estes podem variar de rejeitar a transferência, suspender o processamento até que a informação em falta seja recebida, seja simplesmente relatando os erros. Da mesma forma, a definição de "completude" deve ser apropriada a um repositório de atividades. Se um inventário de arquivos fosse fornecido por um produtor como parte de negociações prévias, seria esperado que fossem feitas verificações em relação a esse inventário. Mas para algumas atividades, como a colheita pela *Web*, "completude" pode significar simplesmente "o que pudermos capturar na sessão de colheita". Quaisquer que sejam os *checks* realizados devem ser consistentes com a própria definição e entendimento documentado do repositório de completude e exatidão.

B1.5 O Repositório obtém controle físico suficiente sobre os objetos digitais para preservá-los.

O repositório deve obter o controle completo dos bits dos objetos digitais transportados com cada SIP. Para exemplo, alguns SIPs podem apenas referenciar objetos digitais e, nesses casos, o repositório deve obter objetos digitais referenciados se eles fizerem parte do objeto com o qual o repositório se comprometeu conservar. Este nem sempre será o caso: trabalhos acadêmicos em um repositório podem conter referências a outros papéis que são mantidos

em um repositório diferente, ou não mantidos em nenhum lugar, e sites da Web colhidos podem conter referências a materiais no mesmo site ou em sites diferentes que o repositório tenha optado por não capturar ou não foi capaz de capturar.

B1.6 O Repositório fornece ao produtor/depositário respostas apropriadas em pontos durante os processos de ingestão.

Com base no plano inicial de processamento e acordo entre o repositório e o produtor/depositário, o repositório deve fornecer ao produtor/depositário relatórios de progresso em pontos específicos e pré-determinados ao longo de todo o processo de ingestão. As respostas podem incluir recibos iniciais de ingestão, ou recibos que confirmem que o AIP foi criado e armazenado. As respostas do repositório podem variar de nada a predeterminado, relatórios periódicos de completude e correção de ingestão, relatórios de erros e qualquer transferência final de documento de custódia. Os depositantes podem solicitar mais informações de forma *ad hoc* quando o acordo prévio sobre relatórios são insuficientes.

B1.7 O Repositório pode demonstrar quando a responsabilidade pela preservação é formalmente aceita para o conteúdo dos objetos de dados submetidos (ou seja, SIPs).

Um componente-chave da responsabilidade de um repositório para obter controle suficiente dos objetos digitais é o ponto quando o repositório gerencia o *bitstream*. Para alguns repositórios isso ocorrerá quando ele receber pela primeira vez o SIP de transformação, para outros pode não ocorrer até que o SIP ingerido seja transformado em um AIP. Neste caso, a o repositório aceita formalmente a responsabilidade de preservação dos objetos digitais do depositante.

Os repositórios que se reportam aos seus depositantes geralmente marcarão esta aceitação com alguma forma de notificação ao depositante. (Isso pode depender das responsabilidades do repositório, conforme designado no acordo do depositante). Um repositório pode marcar a transferência através do envio de um documento formal, muitas vezes um documento final cópia assinada do contrato de transferência, de volta ao depositante, significando a conclusão da transformação do processo SIP em AIP. Outras abordagens são igualmente

aceitáveis. Breves atualizações diárias podem ser geradas por um repositório que fornece apenas relatórios anuais de transferência formal.

B1.8 O Repositório possui registros contemporâneos de ações e processos administrativos que são relevantes para a preservação (Ingestão: aquisição de conteúdo).

Estes registros devem ser criados no ou sobre o tempo das ações a que se referem e estão relacionados a ações tomadas durante a Ingestão: processo de aquisição de conteúdo. Os registros podem ser automatizados ou podem ser escritos por indivíduos, dependendo da natureza das ações descritas. Onde são utilizados padrões comunitários ou internacionais como o PREMIS, o repositório deve demonstrar que todas as ações relevantes são realizadas.

B2. Ingestão: criação do pacote de arquivamento

Os repositórios digitais devem tomar medidas para preservar as informações ingeridas, e as coisas que eles divulgam aos usuários finais devem estar fortemente vinculadas aos objetos originais que foram depositados. Para parafrasear o OAIS, estes requisitos destinam-se a garantir que a informação (objetos digitais e todos metadados apropriados) recebidos e verificados de cada produtor sejam colocados no formulário de arquivo (AIP) e sejam armazenados em arquivo para preservação no longo prazo. Mais especificamente, o repositório deve, na verdade completar o processo de ingestão, criando alguma forma apropriada - identificável como armazenagem de arquivos - na qual armazene as informações. Isto inclui o endereçamento de metadados apropriados para atender os níveis de compreensão esperada, a associação de identificadores únicos para poder referenciar o conteúdo digital, o mapeamento a partir do conteúdo submetido aos formulários de armazenamento da AIP, e informações auditáveis de procedência garantindo a não-perda ou corrupção de conteúdo no desenvolvimento das AIPs.

B2.1 O Repositório tem uma definição escrita e identificável para cada AIP ou classe de informação preservado pelo repositório.

Um AIP contém estes componentes-chave: o objeto de dados primário a ser preservado, seu suporte Informações de Representação (formato e significado

dos elementos do formato), e as diversas categorias de Informações de Descrição de Preservação (PDI) que também precisam estar associadas ao objeto de dados primário: Fixidez, Proveniência, Contexto e Referência. Deve haver uma definição de como estas categorias de informações estão ligadas entre si e/ou relacionadas de tal forma que podem ser sempre encontradas e gerenciadas dentro do arquivo.

É apenas necessário que existam definições para cada AIP, ou classe de AIP, se houver muitas instâncias do mesmo tipo. Repositórios que armazenam uma grande variedade de tipos de objetos podem precisar de uma definição específica para cada tipo AIP que possuem, mas espera-se que a maioria dos repositórios estabeleça descrições de classe que se apliquem a muitos AIPs. Deve ser possível determinar qual definição se aplica a qual AIP.

Embora este requisito se refira principalmente a questões de identificação e vinculação de componentes-chave de AIP, B2.2 coloca condições mais rigorosas sobre o conteúdo dos componentes-chave para garantir que eles sejam adequados para o fim pretendido. A separação dos dois critérios é importante, particularmente se um repositório não satisfizer um deles. É importante saber se alguns ou todos os AIPs não estão definidos, ou que as definições de AIPs existem, mas não são adequadas.

B2.2 O Repositório tem uma definição de cada AIP (ou classe) que é adequada para caber no longo prazo necessidades de preservação.

Em muitos casos, se as definições exigidas pelo B2.1 existem, este requisito também é satisfeito, mas também pode ser necessário para que as definições digam algo sobre a semântica ou o uso pretendido dos AIPs, se isso pode afetar as decisões de preservação no longo prazo. Por exemplo, digamos que dois repositórios preservam apenas imagens estáticas digitais, ambas usando arquivos TIFF multi-imagem como formato de preservação. O Repositório 1 consiste em inteiramente de imagens fotográficas do mundo real destinadas à visualização pelas pessoas e tem uma única definição cobrindo todas os seus AIPs. (A definição pode se referir a uma definição local ou externa do formato TIFF).

O Repositório 2 contém algumas imagens, como raios-x médicos, que se destinam à análise por computador e que não podem ser vistas pelo olho humano, e outras imagens que são como as do Repositório 1. O Repositório 2

deve talvez definir duas classes de AIPs, mesmo que utilize apenas um formato de armazenamento para ambos. Uma futura ação de preservação pode depender do uso pretendido da imagem - uma ação que muda a profundidade de bits da imagem de uma forma que não é perceptível ao olho humano pode ser satisfatória para fotógrafos do mundo real, mas não para imagens médicas, por exemplo.

B2.3 Repositório tem uma descrição de como os AIPs são construídos a partir de SIPs.

O repositório deve ser capaz de mostrar como o objeto preservado é construído a partir do objeto inicialmente submetido para preservação. Em alguns casos, o AIP e o SIP serão quase idênticos à parte de embalagem e localização, e o repositório só precisa dizer isso. Mais comumente, transformações complexas (por exemplo, normalização de dados) podem ser aplicadas a objetos durante o processo de ingestão, e uma descrição precisa dessas ações (ou seja, metadados de preservação) pode ser necessária para assegurar que o objeto preservado representa a informação do objeto submetido. A descrição da construção do AIP deve incluir documentação que forneça a proveniência da ingestão para cada transformação SIP para AIP, consistindo tipicamente em uma visão geral do processo de processamento sendo aplicado a todas essas transformações, ampliada com descrição de diferentes classes de tal processamento e, quando aplicável, como as transformações especiais que se faziam necessárias.

Alguns repositórios podem precisar produzir essas complexas descrições caso a caso, sendo que, nesse caso serão necessários diários ou registros das ações tomadas para produzir cada AIP. Nesses casos, A documentação precisa ser mapeada entre os AIPs individuais, e o mapeamento precisa ser disponíveis para exame. Outros repositórios que podem executar uma abordagem mais em linha de produção podem têm uma descrição de como cada classe de objeto recebido é transformada para produzir o AIP. Deve estar claro qual definição se aplica a qual AIP. Se, para tomar um exemplo simples, dois AIP separados cada processo produzem um arquivo TIFF, deve ficar claro qual processo foi aplicado para produzir um arquivo TIFF em particular.

B2.4 O Repositório pode demonstrar que todos os objetos submetidos (ou seja, SIPs) são aceitos como um todo ou parte de um eventual objeto de arquivo (isto é, AIP), ou dispostos de outra forma em um modelo registrado.

A escala de tempo deste processo varia entre repositórios de segundos a muitos meses, mas os SIPs não devem permanecer em um estado de limbo para sempre. Os procedimentos de adesão e o processamento interno e os registros de auditoria devem manter registros de todas as transformações internas dos SIPs para demonstrar que eles tornam-se AIPs (ou parte de AIPs) ou são descartados. Informações descritivas adequadas também devem documentar a procedência de todos os objetos digitais.

B2.5 O Repositório tem e utiliza uma convenção de nomenclatura que gera identificadores para todos os objetos arquivados (i.e., AIPs).

Um repositório precisa garantir que uma convenção de nomenclatura aceita e padrão esteja em vigor, e que identifique seus materiais de forma única e persistente para uso tanto dentro como fora do repositório. O requisito de "visibilidade" aqui significa "visível" para gerentes de repositório e auditores. Não implica que esses identificadores únicos precisam estar visíveis para os usuários finais ou que eles sirvam como o principal meio de acesso aos objetos digitais.

Igualmente importante é um sistema de serviços confiáveis de vinculação / resolução, a fim de encontrar os objetos nomeados, não importa sua localização física. Isso é para que as ações relacionadas aos AIPs possam ser rastreados ao longo do tempo, alterações no sistema e alterações no armazenamento. Idealmente, o ID exclusivo vive como enquanto o AIP; caso contrário, deve haver rastreabilidade. O sistema de identificação deve ser visto como adequado aos requisitos atuais e previsivelmente futuros do repositório para coisas como números de objetos. Isto deve possibilitar demonstrar que os identificadores são únicos. Observe que B2.1 exige que o componentes de um AIP sejam adequadamente vinculados e identificados para o gerenciamento no longo prazo, mas não há restrições sobre como os AIPs são identificados com arquivos. Assim, no caso geral, um AIP pode ser distribuído por muitos arquivos ou um único arquivo pode conter mais de um AIP. Portanto, identificadores e nomes de arquivos podem não corresponder necessariamente um ao outro.

A documentação deve mostrar como os identificadores persistentes do AIP e seus componentes são atribuídos e mantidos de forma a serem únicos dentro do contexto do repositório. A documentação também deve descrever quaisquer processos utilizados para alterações de tais identificadores. Deve ser possível obter uma lista completa de todos esses identificadores e fazer verificações pontuais para duplicações.

B2.6 Se identificadores únicos forem associados a SIPs antes de ingeridos, o repositório preserva os identificadores de forma que mantenha uma associação persistente com o resultante arquivado objeto (por exemplo, AIP).

Os SIPs nem sempre conterão identificadores únicos quando o repositório os receber. Mas onde receberem e, particularmente, onde esses identificadores forem amplamente conhecidos antes dos objetos serem ingeridos, é importante que sejam retidos como estão, ou que algum mecanismo permita ao identificador original a ser transformado em um utilizado pelo repositório.

Por exemplo, considere um repositório de arquivos cujos SIPs consistem em coleções de arquivos de sistemas de gerenciamento eletrônico de documentos (EDMS). Cada SIP de entrada conterá um único identificador para cada arquivo dentro do EDMS, que pode ser apenas o caminho para o arquivo. O repositório não pode utilizá-los como estão, já que duas coleções diferentes podem conter arquivos com o mesmo patamar. O repositório pode gerar identificadores únicos qualificando o identificador original de alguma forma (por exemplo, prefixando o nome do caminho com um ID único atribuído ao SIP de que era uma parte). Ou pode simplesmente gerar novos identificadores numéricos únicos para cada arquivo em cada SIP. Se ele qualificar o identificador original, deve explicar o esquema que utiliza. Se ele gera identificadores totalmente novos, provavelmente precisará manter um mapeamento entre as identificações originais e IDs gerados, talvez usando metadados de nível de objeto.

A documentação deve mostrar a política de tratamento da identificação única dos componentes SIP como os objetos a serem preservados são ingeridos, preservados e disseminados. Onde há um manuseio especial necessário, isto deve ser documentado para cada SIP como parte da captura de informações de proveniência (ver B2.3).

B2.7 O Repositório demonstra que tem acesso às ferramentas e recursos necessários para estabelecer um contexto semântico ou técnico autoritário dos objetos digitais que contém (ou seja, acesso às Informações de Representação Internacionais apropriadas e registros de formato).

O *Global Digital Format Registry* (GDFR), o registro de formato de arquivo PRONOM dos Arquivos Nacionais do Reino Unido, e o *Digital Curation Centre's Representation Information Registry* do Reino Unido são três exemplos emergentes de potenciais padrões internacionais que um repositório possa adotar. Sempre que possível, o repositório deve utilizar estes tipos de fontes de informação padronizadas e confiáveis para identificar e/ou verificar o Informações de Representação de componentes de Informações de Conteúdo e PDI. Isto reduzirá os custos de manutenção no longo prazo para o repositório e vai melhorar do controle de qualidade.

A maioria dos repositórios manterá as informações de formato localmente para manter sua capacidade independente de verificar formatos ou outros detalhes técnicos ou semânticos associados a cada objeto de arquivo. Nesses casos, o uso de registros de formato internacional não se destina a substituir os registros de formato local, mas sim a servir como recurso para verificar ou obter informações independentes e confiáveis sobre todo e qualquer formato de arquivo.

B2.8 O Repositório de Arquivos/Registros registra Informações de Representação (incluindo formatos) ingeridas.

Quando os padrões internacionais para as Informações de Representação associadas não estão disponíveis, as O repositório precisa capturar tais informações e registrá-las para que possam ser facilmente encontradas e reutilizáveis.

Algumas delas podem ser incorporadas ao software. A Informação de Representação é fundamental para a capacidade de transformar bits em informações utilizáveis e devem estar permanentemente associados às Informações de Conteúdo.

B2.9 O Repositório adquire metadados de preservação (ou seja, PDI) para suas Informações de Conteúdo associadas.

Os metadados de preservação (PDI) são necessários não apenas pelo repositório para ajudar a garantir que as Informações de Conteúdo. não estejam corrompidas (Fixidez) e seja localizáveis (Informação de Referência), mas para ajudar a garantir que a Informação de Conteúdo seja adequadamente compreensível, fornecendo uma perspectiva histórica (Informação de Proveniência) e fornecendo relações com outras informações (Informações de Contexto). A extensão de tais necessidades de informação são melhor atendidas pelos membros da(s) comunidade(s) designada(s). As PDIs devem ser permanente associadas às Informações de Conteúdo.

B2.10 O Repositório tem um processo documentado para testar a compreensibilidade do conteúdo informativo e elevando o conteúdo informativo até o nível acordado de compreensibilidade.

Se as Informações de Conteúdo ou Informações de Descrição de Preservação (PDI) não forem diretamente utilizáveis pelas ferramentas de aplicação da(s) comunidade(s) designada(s), o repositório precisará ter um processo definido para dar-lhe forma utilizável ou para disponibilizar informações adicionais de Representação (ver B3.2).

Repositórios que compartilham o fardo de assegurar que metadados ou documentação adequada seja capturada ou gerada para atender a um grau de compreensão exigido pode implementar qualquer número de procedimentos para atender a este requisito. Tais repositórios tipicamente têm uma comunidade designada estritamente definida, como uma disciplina científica específica.

B2.11 O Repositório verifica cada AIP quanto à completude e exatidão no ponto em que ele é gerado.

Se o repositório tem um processo padrão para verificar se os SIPs estão completos e corretos ou ambos e um processo comprovadamente correto para transformar SIPs em AIPs, então ele precisa simplesmente demonstrar que as verificações iniciais foram realizadas com sucesso e que o processo de transformação foi realizado sem indicação de erros. Repositórios que devem criar processos únicos para muitos de seus AIPs também precisarão gerar métodos únicos para validar a completude e exatidão das AIPs. Isto pode incluir a realização de testes de algum tipo no conteúdo do AIP que pode ser comparado com os testes do SIP. Tais testes podem ser simples (contando o

número de registros em um arquivo, ou realizando alguma medida estatística simples, como calculando o histograma de brilho de uma imagem original e preservada), mas eles podem ser complexos ou conter alguns elementos subjetivos.

A documentação deve descrever como a completude e correção dos SIPs e AIPs são assegurados, começando por garantir o recebimento do produtor e continuando com a criação do AIP e apoiando a preservação no longo prazo. Exemplos de abordagens incluem o uso de *checksums*, testes que os *checksums* ainda estão corretos em vários pontos durante a ingestão e preservação, *logs* que tais foram feitas verificações, e quaisquer testes especiais que possam ser necessários para uma determinada instância ou classe SIP/AIP.

B2.12 O Repositório fornece um mecanismo independente para auditoria da integridade do coleta/conteúdo do repositório.

Em geral, é provável que um repositório que atenda a todos os critérios anteriores satisfaça este sem necessidade de demonstrar mais nada. Como um requisito à parte, demonstra a importância de se poder auditar a integridade da coleção como um todo.

Um mecanismo familiar do mundo dos materiais tradicionais em bibliotecas e arquivos é um registro de adesões ou aquisições que seja independente de outros metadados do catálogo. Um repositório deve ser capaz de mostrar, para cada item de seu registro de adesões, qual(is) AIP(s) contém(m) conteúdo desse item. Alternativamente, pode ser necessário mostrar que não há AIP para um item, seja porque ingestores ainda estão em andamento, ou porque o item foi rejeitado por algum motivo. Por outro lado, qualquer AIP deve poder ser relacionado a uma entrada no registro de aquisições.

B2.13 O Repositório possui registros contemporâneos de ações e processos de administração que são relevantes para a preservação (criação da AIP).

Estes registros devem ser criados no ou sobre o tempo das ações a que se referem e estão relacionados a ações associada à criação da AIP. Os registros podem ser automatizados ou podem ser escritos por indivíduos, dependendo da natureza das ações descritas. Onde são utilizados padrões comunitários ou

internacionais, tais como PREMIS, o repositório deve demonstrar que todas as ações relevantes são realizadas.

B3. Planejamento de Preservação

Um repositório ou sistema de arquivamento deve ter estratégias de preservação atuais, sólidas e documentadas em local e comprovadamente implementado. Não basta simplesmente preservar a informação. Um repositório deve fazê-lo de acordo com políticas e procedimentos pré-definidos, documentados, políticas de preservação e procedimentos, e deve ter mecanismos identificados para atualizar essas políticas e procedimentos em resposta às mudanças tecnológicas. Sem essa documentação, um repositório não pode passar por uma auditoria, mesmo que seu trabalho seja exemplar.

A documentação não precisa ser particularmente complexa. Também não é necessário prescrever em detalhes como o repositório irá lidar com o desconhecido. Por exemplo, um repositório não pode ser obrigado a documentar como ele irá preservar um formato de arquivo que ainda não foi inventado. Mas é de se esperar que descreva o que ele irá fazer quando apresentado pela primeira vez com um objeto em um formato que ele não tenha encontrado antes. Ele pode não ter estratégias para cada tipo de arquivo dentro do repositório (especialmente importante para instituições adquirentes e ingerindo o produto das atividades de colheita/arquivamento da Web), mas precisa ser capaz de articular consciência organizacional da diversidade de informações dentro do repositório, bem como de planos ou afirmações sobre as estratégias de preservação que serão ou não empregadas contra determinados arquivos. A política organizacional pode ser a de rejeitar o objeto ou de investigar a viabilidade de lidar com ele, ou a decisão pode depender de outros fatores, tais como quem ofereceu o objeto ou que informação ele contém.

Um repositório digital confiável não pode simplesmente dizer o que vai fazer; ele deve demonstrar suas políticas, práticas, e procedimentos. Esta documentação deve ser explícita, abrangente, atual e disponível.

B3.1 O Repositório tem estratégias de preservação documentadas.

Um repositório ou sistema de arquivamento deve ter estratégias de preservação atuais, sólidas e documentadas. Estas estratégias normalmente abordarão a degradação dos meios de armazenamento, a obsolescência dos *drives* de mídia e a obsolescência da Informação de Representação (incluindo formatos),

salvaguardas contra corrupção digital acidental ou intencional. Por exemplo, se a migração for a abordagem escolhida para algumas dessas questões, também é preciso haver uma política sobre o que desencadeia um migração e que tipos de migração são esperados para a solução de cada questão de preservação identificados.

B3.2 O Repositório dispõe de mecanismos de monitoramento e notificação quando Informações de Representação (incluindo formatos) aproximam-se da obsolescência ou não são mais viáveís.

Para a maioria dos repositórios, a preocupação será com as Informações de Representação (incluindo formatos) utilizadas para preservar informações, que podem incluir informações sobre como lidar com um formato de arquivo ou software que pode ser usado para renderizá-lo ou processá-lo. Algumas vezes o formato precisa ser alterado porque o repositório não pode para lidar com ele mais tempo. Algumas vezes o formato é mantido e as informações sobre qual software é necessário para processá-lo precisam mudar.

Em todos os casos, o repositório deve mostrar que possui algum mecanismo ativo para alertar sobre a iminência de mudanças obsolescência. A obsolescência é determinada em grande parte em termos da base de conhecimento da comunidade(s). Este requisito garante que as informações preservadas permaneçam compreensíveis e utilizáveis pela(s) comunidade(s) designada(s). Se o mecanismo depende de um registro externo, o deve demonstrar como utiliza as informações desse registro.

B3.3 O Repositório possui mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.

O repositório deve demonstrar ou descrever como ele reage às informações de monitoramento, que Às vezes é necessário um repositório para mudar a forma como ele lida com o material que possui de forma inesperada.

Planos tão simples quanto migrar do formato X para o formato Y quando os registros mostram que o formato X não é Os eventos mais longos suportados não são suficientemente flexíveis - outros eventos podem ter feito do formato Y uma má escolha. O repositório deve estar preparado para mudanças no ambiente externo que possam fazer seu plano atual (para migrar de X para Y em 10 anos) uma má escolha à medida que o tempo para implementar se aproxima.

O repositório deve ser capaz de mostrar que pode revisar planos de longo prazo à luz das mudanças das circunstâncias.

Outra possível resposta às informações coletadas pelo monitoramento é que o repositório crie mais Informações de Representação e/ou PDI.

B3.4 O Repositório pode fornecer provas da eficácia de seu planejamento de preservação.

O repositório deve ser capaz de demonstrar a preservação contínua, incluindo a compreensibilidade de suas participações ao longo de vários anos, dada a idade do repositório e de suas participações.

Isto pode ser avaliado em vários graus e depende da especificidade da(s) comunidade(s). Se uma comunidade designada for bastante ampla, um auditor poderá representar o sujeito do teste em uma avaliação. Comunidades designadas mais específicas podem exigir esforços significativos. Se o julgamento deve ser exercido quanto à realização de esforços adequados, deve ser justificada em detalhes.

B4. Armazenamento e preservação/manutenção de AIPs

Existe um conjunto mínimo de condições para se realizar a preservação no longo prazo das AIPs. O sistema (discutido em C1) deve fornecer serviços adequados para permitir um repositório de nível superior (objeto gerenciais) que operam em AIPs para desempenhar suas tarefas de forma confiável. Mas se as funções de nível superior não utilizam estes serviços, ou não os utilizam adequadamente, então a preservação não está assegurada. A preservação das AIPs devem seguir as estratégias de preservação documentadas, tipicamente incluindo tópicos como o uso de migração, transformações, checksums, cópias múltiplas, armazenamento distribuído e rastreamento do processamento histórico que pode afetar a confiança na preservação.

B4.1 O Repositório emprega estratégias de preservação documentadas.

As estratégias de preservação documentadas incluem evidências de planejamento de estratégias ainda não empregadas contra os objetos digitais do repositório. É provável que um repositório utilize múltiplas estratégias. Estratégias diferentes podem ser empregados por classe (tipo) de objeto digital, e/ou múltiplas estratégias podem ser empregadas em um único objeto classe de objeto. Isso dependerá das políticas e práticas locais de repositório, embora

qualquer estratégia desse tipo As decisões devem ser documentadas e devem ser baseadas em práticas comunitárias sólidas.

No mínimo, a documentação das estratégias de preservação deve ser incluída nas políticas e práticas de repositório. As boas práticas de repositório também exigem que as estratégias de preservação empregadas contra objetos digitais sejam gravados nos metadados de preservação do objeto. (Veja também B3.3.)

B4.2 Repositório implementa/responde a estratégias de armazenamento de objetos de arquivo (i.e., AIP) e migração.

Pelo menos dois aspectos da estratégia devem ser levados em conta: o que se refere à forma como os AIPs são atualmente armazenados (incluindo requisitos físicos, requisitos de mídia, localização das cópias, formatos e metadados) e aquilo que possa exigir migração de AIP de qualquer forma. Por exemplo, as migrações de AIP que resultam em transformações de conteúdo precisam ser rastreadas para permitir usuários posteriores para entender as implicações do processamento do repositório.

Se um repositório ainda não precisou executar qualquer tipo de estratégia de preservação no(s) AIP(s), ele deve demonstrar que sua política ainda não o exigiu.

B4.3 Repositório preserva as Informações de Conteúdo dos objetos de arquivo (ou seja, AIPs).

O repositório deve ser capaz de demonstrar que as AIPs refletem fielmente o que foi capturado durante o processo de ingestão e que quaisquer transformações posteriores ou futuras planejadas continuarão a preservar esse aspecto do acervo do repositório.

Este requisito assume que o repositório tem uma política especificando que os AIPs não podem ser excluídos em nenhum tempo. Esta implementação particularmente simples e robusta preserva as ligações entre o que era originalmente ingerido, bem como novas versões que tenham sido transformadas ou alteradas de alguma forma. Dependendo dessa implementação, estes novos objetos podem ser AIPs completamente novos ou apenas AIPs atualizados. De qualquer forma, ligações persistentes entre o objeto ingerido e o AIP devem ser mantidas.

B4.4 O Repositório monitora ativamente a integridade dos objetos de arquivo (ou seja, AIPs).

Na terminologia do OAIS, isto significa que o repositório deve ter Informações de Fixidez para AIPs e deve fazer algum uso dele. Atualmente, a maioria dos repositórios lida com isso ao nível das informações individuais usando um *checksum* de alguma forma, como o MD5. Neste caso, o repositório deve ser capaz de demonstrar que as Informações de Fixidez (*checksums*, e as informações que as ligam aos AIPs) são armazenadas separadamente ou protegidas separadamente dos próprios AIPs, para que alguém que possa maliciosamente alterar uma AIP provavelmente não seria capaz de alterar as Informações de Fixidez também. Um repositório deve ter logs que mostrem esta verificação sendo aplicada e uma explicação de como as duas classes de informação são mantidas separadas.

A integridade das AIPs também precisa ser monitorada em um nível superior, assegurando que todas as AIPs que deveriam existir de fato existem, e que o repositório não possui AIPs para as quais não está destinado. Informações do checksum por si só não serão capazes de demonstrar isso.

B4.5 O Repositório possui registros contemporâneos de ações e processos administrativos que são relevantes para a preservação (Armazenamento de Arquivos).

Estes registros devem ser criados no ou sobre o tempo das ações a que se referem e estão relacionados a ações associadas ao armazenamento de arquivos. Os registros podem ser automatizados ou podem ser escritos por indivíduos, dependendo da natureza das ações descritas. Onde são utilizados padrões comunitários ou internacionais, como o PREMIS, o repositório deve demonstrar que todas as ações relevantes são realizadas.

B5. Gestão da informação

Um componente crítico de qualquer repositório é sua funcionalidade de gerenciamento de informações. Independentemente de composição técnica e independentemente de ser considerado um repositório "claro" ou "escuro" - guardando material de retenção para acesso das futuras gerações - o sistema precisa ser capaz de armazenar, rastrear e utilizar metadados que suportem a funcionalidade central do repositório digital. O OAIS descreve isso mas, na prática, essas informações são críticas e são

geradas dentro de outras funções de repositório digital, tais como ingestão, armazenamento de arquivos, planejamento de preservação e acesso. Por esse motivo, esta seção, Gestão da Informação, aborda as demais necessidades associadas com metadados descritivos.

Independentemente do sistema, as informações descritivas (metadados) serão adquiridas e mantidas para acesso e recuperação. Se as pessoas não conseguem encontrar o que querem, o repositório não está atendendo às necessidades de seus usuários. Os requisitos mínimos de metadados para o gerenciamento de dados podem ser muito básicos. Na maioria dos casos, os requisitos mínimos de exigências de pesquisa não podem ser mais do que um identificador que uma comunidade designada usa para solicitar um objeto depositado, como um número de catálogo ou uma referência de arquivo. As pessoas também precisam saber se é permitida a obtenção de uma cópia utilizável e como.

Os requisitos mínimos de metadados descritivos de um repositório devem corresponder às necessidades mínimas da(s) comunidade(s) designada(s) pelo repositório. Isto não significa que o repositório precisa ser capaz de responder a cada um de seus usuários para obter informações adicionais do catálogo. Ao contrário, ele deve avaliar o que pode fornecer a um membro representante da(s) sua(s) comunidade(s) designada(s), com base em utilidade e custo. Se o repositório atende a várias comunidades, cada uma interessada em diferentes segmentos de suas participações, então os requisitos mínimos podem variar de AIP para AIP. Se um repositório tiver filmes digitais e músicas digitais, os elementos descritivos mínimos para filme e música serão diferentes.

As informações descritivas podem incluir muito mais do que a descrição narrativa que pode ser familiar ao usuário de uma biblioteca tradicional ou catálogo de arquivos. Também pode incluir qualquer informação que o potencial o usuário possa achar útil na avaliação da adequação e facilidade de uso de um objeto, incluindo indicações de tipos de ferramentas necessárias para o uso. Se o acervo de um repositório varia muito em tamanho e os objetos maiores não são adequados para download através de uma conexão de rede, por exemplo, a informação sobre o tamanho permite um usuário para escolher um método de entrega ideal, como uma fita para ser entregue pelo correio. Ou um repositório pode exigir a disponibilização de software especial ao usuário para permitir que um objeto seja interpretado.

O usuário deve ser capaz de determinar isso antecipadamente, em vez de possivelmente pagar para adquirir material apenas para descobrir que eles não têm as ferramentas para utilizá-lo.

Um repositório pode atender essa necessidade nas informações mais gerais que disponibiliza aos seus usuários, ao invés de que colocar informações específicas nas informações descritivas de cada AIP. Por exemplo, um repositório que contém apenas arquivos PDF pode:

- Declarar nas informações de cada AIP que se trata de um arquivo PDF.
- Ter informações gerais sobre como utilizar o repositório que declara que você precisará de um leitor de PDF para utilizar as suas participações.
- Define sua(s) comunidade(s) designada(s) como pessoas com acesso a um leitor de PDF.

Cabe ao repositório assegurar que todo e qualquer objeto armazenado tenha informações descritivas associadas com ele. Esta lista de verificação de auditoria não especifica como o repositório faz isso, apenas que deve estar claro como ele é feito. O repositório pode transferir o ônus inteiramente para os produtores de informações, exigindo que digam que o material oferecido para o repositório deve conter uma quantidade mínima de metadados para permitir o armazenamento de informações descritivas. O repositório pode assumir a tarefa de produzir as informações propriamente ditas. Ou ele pode preencher as lacunas no que os produtores fornecem - utilizando seus metadados quando é suficiente, e adicionando metadados quando não é. Qualquer que seja o repositório, ele deve estabelecer com antecedência os metadados mínimos requeridos que permitam que o material seja descoberto e identificado novamente.

B5.1 O Repositório articula os requisitos mínimos de metadados para permitir que a(s) comunidade(s) descubram e identifiquem material de interesse.

A recuperação de metadados é diferente dos metadados que descrevem o que foi encontrado. Por exemplo, em uma biblioteca podemos dizer que o título de um livro é obrigatório, mas sua editora não é, porque as pessoas geralmente pesquisam o título.

Um repositório não tem necessariamente que satisfazer todas as solicitações possíveis, mas deve ser capaz de lidar com os tipos de solicitação que virão de um usuário típico da(s) comunidade(s) designada(s). Os requisitos mínimos

devem ser articulados. O mínimo pode ser nada mais que um identificador que a(s) comunidade(s) designada(s) saberia(m) e usaria(m) para solicitar um objeto depositado.

B5.2 O repositório captura ou cria metadados descritivos mínimos e garante que eles sejam associados ao objeto arquivado (i.e., AIP).

O repositório tem que mostrar como ele obtém os metadados necessários. É necessário que os produtores forneçam os metadados (recusando um depósito que não o tenha) ou ele próprio fornece alguns metadados durante a ingestão?

A associação dos metadados ao objeto é importante, embora não exija um número um para uma correspondência e metadados não precisam necessariamente ser armazenados com o AIP. Esquemas hierárquicos de descrição permitem que alguns elementos descritivos sejam associados a muitos itens. A associação deve ser inquebrável - nunca deve ser perdida, mesmo que outras associações sejam criadas.

B5.3 O Repositório pode demonstrar que a integridade referencial é criada entre todos os objetos arquivados (ou seja, AIPs) e informações descritivas associadas.

Todo AIP deve ter alguma informação descritiva e toda informação descritiva deve apontar pelo menos para um AIP, de modo que a integridade possa ser validada. Esta deve ser uma exigência fácil de satisfazer e é uma pré-requisito para o próximo.

B5.4 O Repositório pode demonstrar que a integridade referencial é mantida entre todos objetos arquivados (ou seja, AIPs) e informações descritivas associadas.

Deve ser dada especial atenção às operações que afetam os AIPs e seus identificadores e como a integridade é mantida durante estas operações. Pode haver momentos, dependendo do projeto do sistema, em que não se pode demonstrar integridade referencial porque algum componente do sistema está fora de ação.

Entretanto, os repositórios, devem implementar procedimentos que lhes permitam saber quando a integridade referencial é temporariamente quebrada e garantir que ele possa ser restaurada.

B6. Gerenciamento de acesso

Deve-se entender que a capacidade e a sofisticação do sistema de acesso variará de acordo com a(s) comunidade(s) designada(s) pelo repositório e os mandatos de acesso do repositório. Por causa da variedade de repositórios, arquivos e mandatos de acesso, estes critérios podem estar sujeitos a perguntas sobre aplicabilidade e interpretação a nível local.

Os Repositórios com mandato para prover acesso atual devem ser capazes de produzir Pacotes de Disseminação de Informações (DIPs) que atendam às necessidades de seus usuários ou que sejam adequados aos níveis de acesso que eles oferecem. Arquivos "Escuros" ou arquivos nacionais que podem ter mandatos que restrinjam o acesso para um determinado número de anos produzirão mais DIPs para requisições internas, como a realização de migrações, em vez de acesso. Em qualquer caso, qualquer repositório deva ser capaz de produzir um DIP, por mais primitivo que seja e qualquer que seja o seu propósito.

Esses requisitos garantem que o acesso seja implementado de acordo com as políticas declaradas pelo repositório:

- B6.1 a B6.4 se preocupam principalmente com as condições de acesso e ações relacionadas com o comunidade(s);
- B6.5 e B6.6 se preocupam principalmente com a segurança de acesso, com foco na segurança interna (pessoal) acesso;
- B6.7 a B6.9 garantem que a função de acesso seja implementada corretamente. O acesso deve sempre entregar o que é necessário, ou deixar claro que não é possível por qualquer razão. Oportunamente, pode ser medido em segundos ou semanas, já que o acesso pode ser uma função online ou uma função postal ou pode ser mediada através de algum outro mecanismo ou uma combinação deles.
- B6.10 acrescenta um requisito específico além da necessidade de simplesmente fornecer acesso a um bens do repositório. Para que o repositório seja confiável, ele deve ser capaz de fornecer uma cópia de material que pode ser rastreado até os originais.

B6.1 O Repositório documenta e comunica à(s) sua(s) comunidade(s) designada(s) que opções de acesso e entrega estão disponíveis.

As políticas de repositório devem documentar os vários aspectos de acesso e entrega das informações preservadas. Geralmente, a(s) comunidade(s) designada(s) deve(m) conhecer as políticas ou, pelo menos, a consequências das mesmas. Os usuários devem saber o que podem pedir, quando e como, e o quanto custa, entre outras coisas.

Os repositórios podem ter que lidar com uma comunidade única e homogênea ou com comunidades múltiplas ou díspares. Diferentes políticas podem ser necessárias para diferentes comunidades, bem como para diferentes tipos de coleta.

B6.2 O Repositório implementou uma política de registro de todas as ações de acesso (inclui pedidos, ordens, etc.) que atendam aos requisitos do repositório e informações produtores/depositários.

Um repositório só precisa registrar as ações que atendam aos requisitos do repositório e suas informações produtores/depositores. Isto pode significar que pouca ou nenhuma informação é registrada sobre o acesso. Ou seja aceitável se o repositório puder demonstrar que não precisa fazer mais. Alguns repositórios podem querer informações sobre o que está sendo acessado, mas não sobre os usuários. Outros podem precisar de muito mais detalhes informações sobre acesso. Deve ser estabelecida e implementada uma política que se relacione a informações demonstráveis necessidades. Estes números estão sendo monitorados? As estatísticas são produzidas e disponibilizadas?

Evidências: Políticas de acesso; declarações de uso.

B6.3 O Repositório assegura que os acordos aplicáveis às condições de acesso são cumpridos.

O repositório deve ser capaz de mostrar quais acordos produtores/depositários se aplicam a quais AIPs e deve validar as identidades dos usuários a fim de garantir que os acordos sejam cumpridos. Embora seja fácil focar em negar o acesso ao considerar condições deste tipo (ou seja, impedindo que pessoas não autorizadas vejam o material), é igualmente importante mostrar que o acesso é concedido quando as condições dizem que deve ser.

As condições de acesso são muitas vezes apenas sobre quem pode ver as coisas, mas podem ser mais complexas. Elas podem envolver limites de quantidades - todos os membros de uma determinada comunidade têm

permissão para acessar 10 itens a ano sem custo, por exemplo. Ou podem envolver limites de uso ou tipo de acesso - alguns itens podem ser vistos mas não guardados para reutilização posterior, ou os itens só podem ser usados para pesquisa privada, mas não ganho comercial, por exemplo.

Vários cenários podem ajudar a ilustrar o que é necessário:

Se o material de um repositório é todo de acesso aberto, o repositório pode simplesmente demonstrar que o acesso é realmente disponível para todos.

Se todo o material do repositório estiver disponível para uma comunidade única e fechada, o repositório deve demonstrar que valida que os usuários são membros desta comunidade, talvez solicitando alguma prova de identidade antes de registrá-los, ou apenas restringindo o acesso por endereços de rede, se a comunidade pode ser identificadas dessa forma. Deve também demonstrar que todos os membros da comunidade podem de fato ter acesso, se assim o desejarem.

Se diferentes condições de acesso se aplicam a diferentes AIPs, o repositório deve demonstrar como estas são realizadas.

Se as condições de acesso exigirem que os usuários façam alguma declaração antes de receberem as DIPs, o repositório deve mostram que as declarações foram feitas. Estas podem ser formulários assinados, ou provas de que uma declaração tem foi visualizada online e um botão clicado para indicar o acordo. As declarações podem envolver não-divulgação ou acordo para nenhum uso comercial, por exemplo.

B6.4 O Repositório tem políticas de acesso documentadas e implementadas (regras de autorização, requisitos de autenticação) consistentes com os contratos de depósito para objetos armazenados.

As credenciais dos usuários só são relevantes para repositórios que atendam comunidades específicas ou que tenham restrições de acesso em algumas de suas propriedades. Uma credencial de usuário pode ser tão simples quanto o endereço IP de que um pedido se origina, ou pode ser um nome de usuário e senha, ou pode ser mais complexo e através de um mecanismo seguro. Assim, embora esta exigência possa não se aplicar a alguns repositórios, ela pode exigir muito validação formal para outros. O fundamental é que as políticas de acesso e entrega sejam refletidas na prática e que o nível de validação seja apropriado

para os riscos de se obter uma validação errada. Alguns das requisitos podem surgir de acordos com produtores/depositários e alguns de requisitos legais.
O pessoal do Repositório também precisará acessar objetos armazenados ocasionalmente, seja para completar ou não a ingestão de executar funções de manutenção, tais como verificação e migração, ou produzir DIPs. O repositório deve ter políticas e mecanismos para proteger os objetos armazenados contra danos por pessoal (ver C3.3).

B6.5 Sistema de gerenciamento de acesso ao repositório implementa integralmente a política de acesso.
O repositório deve demonstrar que todas as políticas de acesso estão implementadas. O acesso pode ser gerenciado parcialmente. por computadores e, em parte, por seres humanos verificando passaportes, por exemplo, antes de emitir um ID de usuário e A senha pode ser uma parte apropriada da gestão de acesso para algumas instituições.

B6.6 O Repositório registra todas as falhas de gerenciamento de acesso, e a equipe revisa as falhas inadequadas de incidentes de "negação de acesso".
Um repositório deve ter algum mecanismo automatizado para notar negações anômalas ou incomuns e usá-las para identificar ameaças à segurança ou falhas no sistema de gerenciamento de acesso, tais como usuários válidos tendo acesso negado. Isto não significa olhar para cada acesso negado. Este requisito não se aplica a repositórios com acesso irrestrito.

B6.7 O Repositório pode demonstrar que o processo que gera a solicitação de objeto(s) digitais (ou seja, DIP) é completado em relação à solicitação.
Se um usuário espera um conjunto, o usuário deve obter o conjunto completo. Se o usuário espera um arquivo, o usuário deve obter o arquivo completo. Se a solicitação do usuário não puder ser satisfeita, o usuário deve ser informado disto; por exemplo, a escassez de recursos pode significar que um pedido válido não possa ser atendido. Cenários aceitáveis incluem:
O usuário recebe o DIP completo solicitado e fica claro para o usuário que isto aconteceu.
O usuário é informado de que a solicitação não pode ser satisfeita.

Parte da solicitação não pode ser satisfeita, o usuário recebe um DIP contendo os elementos que podem ser disponibilizados, e o sistema deixe claro que o pedido é apenas parcialmente satisfeito.
Cenários inaceitáveis incluem:
A solicitação só pode ser parcialmente satisfeita e um DIP parcial é gerado, mas não está claro para o usuário que é parcial.
O pedido é adiado indefinidamente porque algo que ele requer, como o acesso a um determinado AIP, não é disponível, mas o usuário não é notificado nem há qualquer indicação de quando o conflito será resolvido.
O usuário é informado que o pedido não pode ser satisfeito, implicando que nada pode ser entregue, mas na verdade recebe um DIP, e fica inseguro quanto à sua validade ou integralidade.

B6.8 O Repositório pode demonstrar que o processo que gera os objetos digitais solicitados (ou seja, DIP) está correto em relação ao pedido.
O material correto deve ser entregue e transformações apropriadas devem ser aplicadas, se necessário, para gerar o DIP. Um exemplo simples é que se o repositório armazena imagens TIFF mas entrega JPEGS, a conversão deve ser mostrada como correta para qualquer padrão que pareça apropriado. Se o repositório oferece entrega como JPEG ou PNG, o usuário deve receber o formato solicitado. Muitos repositórios podem se aplicar
transformações mais complexas para gerar DIPs a partir de AIPs.

B6.9 Repositório demonstra que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição.
Eventualmente uma solicitação deve ter sucesso ou falhar, e deve haver limites de quanto tempo o usuário leva para saber disso. Os logs de acesso são a forma mais simples de demonstrar o tempo de resposta, mesmo que o repositório não retenha essas informações por muito tempo. Entretanto, um repositório pode demonstrar conformidade se puder demonstrar que todas pedidos falhados resultam em um log de erros de algum tipo, e que os pedidos são delimitados em duração de alguma forma.

B6.10 Repositório permite a divulgação de cópias autênticas do original ou objetos rastreáveis até os originais.

Parte da gestão de arquivos confiáveis trata da autenticidade dos objetos que são divulgados. Os usuários do repositório devem estar confiantes de que possuem uma cópia autêntica do objeto original, ou que ele é rastreável de alguma forma auditável até o objeto original. Esta distinção é feita porque os objetos não são sempre disseminados da mesma forma, ou nos mesmos agrupamentos, como são depositados. Um banco de dados pode ter subconjuntos de suas linhas, colunas e tabelas divulgadas para as quais a frase "cópia autêntica" tenha pouco significado. As ações de ingestão e preservação podem alterar os formatos dos arquivos, ou podem agrupar e dividir os objetos originais depositados.

A distinção entre cópias autênticas e objetos rastreáveis também pode ser importante quando processos de transformação são aplicados. Por exemplo, um repositório que armazena áudio digital de emissões de rádio pode disseminar texto derivado que é construído por reconhecimento automático de voz a partir do fluxo de áudio digital.

O texto derivado pode ser imperfeito, mas útil para muitos usuários, embora estes textos não sejam cópias autênticas do áudio original. Produzir uma cópia autêntica significa ou entregar o áudio original ou obter um humano para verificar e corrigir a transcrição contra o áudio armazenado.

Este requisito garante que as ações de ingestão, preservação e transformação não percam informações que suportariam uma trilha auditável entre o objeto original depositado e o eventual objeto disseminado objeto. Para a conformidade, a cadeia de autenticidade só precisa alcançar até o limite da ingestão, embora algumas comunidades, como as que lidam com registros legais, podem exigir cadeias de autenticidade que mais adiante.

Um repositório deve ser capaz de demonstrar os processos de construção do DIP a partir do(s) AIP(s) relevante(s).

Esta é uma parte fundamental para estabelecer que os DIPs refletem o conteúdo dos AIPs, e portanto do material original, em um modelo confiável e consistente. Os DIPs podem ser simplesmente uma cópia dos AIPs, ou podem resultar de uma simples transformação de formato de um AIP. Mas, em outros casos, eles podem ser derivados de formas complexas de um grande conjunto de AIPs. Um usuário pode solicitar um DIP composto pelas páginas de título de todos os e-books publicados em um determinado período, por exemplo, que exigirá que estes sejam extraídos de muitos AIPs diferentes. Um repositório que permite

pedidos de DIPs tão complexos precisarão se esforçar mais para demonstrar como ele atende a isso que um repositório que só permite solicitações de DIPs que correspondam a um AIP inteiro.

Um repositório não é necessita mostrar que cada DIP que ele fornece pode ser verificado como autêntico em uma data posterior; ele deve mostrar que pode fazer isso quando for requerido no momento da produção do DIP. O nível de autenticação deve ser determinado pela(s) comunidade(s) designada(s). Este requisito destina-se a habilitar altos níveis de autenticação, para não impor em todas as cópias, já que pode ser um processo caro.

C. Tecnologias, Infraestruturas Técnicas, e Segurança

Estes requisitos não prescrevem hardware e software específicos para garantir que os AIP´s possam ser preservados parno longo prazo, mas descrevem as melhores práticas de gestão e segurança dos dados. No total, estes critérios medem a adequação da infraestrutura técnica do repositório e a sua capacidade para satisfazer as exigências de gestão e segurança do repositório e dos seus objetos digitais.

Os critérios aqui enunciados são semelhantes aos das boas práticas informáticas exigidas pelas normas internacionais de gestão como a ISO 17799. É muito provável que os Repositórios ou organizações que tenham obtido a certificação ISO 17799 satisfaçam muitos destes critérios. Fornecer prova de certificação à gestão ou segurança relevante de informática podem servir como prova necessária para alguns dos critérios da seção C.

Estes requisitos estão agrupados em três níveis:

- C1: Requisitos gerais de infraestrutura do sistema.
- C2: Tecnologias adequadas, com base nos requisitos de infraestrutura do sistema, com requisitos adicionais de critérios que especificam as tecnologias e estratégias de utilização adequadas ao repositório designado comunidade(s).
- C3: Segurança de sistemas informatizados, tais como servidores, *firewalls* ou *routers* para sistemas de proteção contra incêndios e detecção de inundações a sistemas que envolvem ações por pessoas.

C1. Infraestrutura do sistema

Sem uma infraestrutura segura e de confiança, não se pode confiar nas funções desempenhadas nos AIP´s - eles são construídos sobre um castelo de cartas. As ações aqui especificadas são suficientemente gerais para se aplicarem a outros sistemas que não repositórios e arquivos.

C1.1 Funções de repositório em sistemas operativos bem suportados e outros núcleos *software* infraestrutural.

O requisito especifica "bem apoiado", em oposição a apoiado pelo fabricante ou outra frase similar. O nível de apoio a estes elementos da infraestrutura deve ser adequado às suas utilizações; o repositório deve demonstrar que compreende onde se situam os riscos. O grau de apoio necessário está relacionado com a criticidade do subsistema em causa. Um repositório pode ter, deliberadamente, um sistema antigo, utilizando um software de apoio desatualizado a alguns aspectos da sua função de ingestão. Se esse sistema falhar, pode demorar algum tempo para substituí-lo, se é que pode ser substituído de todo. Desde que o seu insucesso não afete as funções de missão crítica, isto é aceitável. Os sistemas utilizados para o desenvolvimento interno não podem ser protegidos ou apoiados ao mesmo nível que as de serviço ao utilizador final.

C1.2 Repositório garante que possui suporte adequado de *hardware* e *software* para backup funcionalmente suficiente para os serviços do repositório e para os dados detidos, por exemplo, metadados associados aos controles de acesso, repositório de conteúdos principais.

O repositório tem de ser capaz de demonstrar a adequação dos processos, *hardware* e *software* para os seus sistemas de apoio. Alguns necessitarão de planos de backup muito mais elaborados do que outros.

C1.3 O Repositório gere o número e a localização das cópias de todos os objetos digitais.

O sistema de repositório deve ser capaz de identificar o número de cópias de todos os objetos digitais armazenados, bem como a localização de cada objeto e das respectivas cópias. Isto aplica-se ao que se pretende que sejam cópias idênticas, e não versões de objetos ou cópias.

A localização deve ser descrita de forma a que o objeto possa ser localizado com precisão, sem ambiguidade. Pode ser uma localização física absoluta ou uma localização lógica dentro de um suporte de armazenamento ou de um subsistema de armazenamento. A forma de o testar, seria olhar para um determinado objeto e perguntar quantos exemplares existem, quais são armazenadas e onde se encontram.

Um repositório pode ter diferentes políticas para diferentes classes de objetos, dependendo de fatores tais como o produtor, o tipo de informação, ou o seu valor. Alguns repositórios podem ter apenas uma cópia (excluindo backups) de tudo, guardado num único local, embora isto não seja definitivamente recomendado. Pode haver requisitos de identificação adicionais se os mecanismos de integridade dos dados utilizarem cópias alternativas para substituir cópias falhadas.

C1.4 O Repositório dispõe de mecanismos para assegurar qualquer/várias cópias de objetos digitais são sincronizados.

Se existirem múltiplas cópias, tem de haver alguma forma de assegurar que as alterações intencionais a um objeto sejam propagadas a todas as cópias do objeto. Tem de haver um elemento de oportunidade para tal. Deve ser possível saber quando a sincronização tiver sido concluída e, idealmente, ter alguma estimativa prévia quanto tempo vai demorar. Dependendo de ser automatizado ou exigir uma ação manual (por exemplo, a recuperação de cópias do armazenamento externo), o tempo envolvido pode ser de segundos ou semanas. A duração em si é de imaterial - o que é importante é que haja uma compreensão de quanto tempo vai demorar.

Tem de haver também algo que aborde o que acontece enquanto a sincronização está em curso. Isso tem um impacto na recuperação de catástrofes: o que acontece se uma catástrofe e uma atualização coincidirem? Se uma cópia de uma objeto é alterado e ocorre uma catástrofe enquanto outras cópias estão a ser atualizadas, é essencial ser capaz de assegurar que a atualização seja posteriormente propagada com êxito.

C1.5 O Repositório possui mecanismos eficazes para detectar a corrupção ou perda de bits.

O repositório deve detectar com precisão a perda de dados para garantir que quaisquer perdas sejam abrangidas pelas tolerâncias estabelecidas por política (ver A3.6). As perdas de dados devem ser detectadas e detectáveis independentemente da fonte da perda. Isso aplica-se a todas as formas e âmbito da corrupção de dados, incluindo objetos em falta e corruptos ou objetos incorretos ou impostores, corrupção dentro de um objeto e erros de cópia, durante a migração de dados ou sincronização de cópias. Idealmente, o

repositório demonstrará que possui todas as AIP´s que é suposto ter e não têm outras, e que elas e os seus metadados não estão corrompidos.

A abordagem deve ser documentada e justificada e incluir mecanismos para mitigar perigos como falha de *hardware*, erro humano e ação maliciosa. Repositórios que utilizam mecanismos como as assinaturas MD5 só precisam de reconhecer a sua eficácia e o seu papel no âmbito do abordagem. Mas, na medida em que o repositório se baseia em esquemas de cultivo caseiro, tem de proporcionar uma abordagem justificativa convincente de que a perda de dados e a corrupção são detectadas dentro das tolerâncias estabelecidas pela política.

As perdas de dados devem ser detectadas com a rapidez suficiente para que as fontes sistêmicas de falha de rotina, tais como falhas de hardware, não sejam susceptíveis de se acumularem e causar perda de dados para além das tolerâncias estabelecidas pela política do repositório ou especificada em qualquer acordo de depósito relevante. Por exemplo, considere um repositório que mantenha uma coleção de cópias primárias e de segurança idênticas, sem qualquer outro mecanismo de redundância de dados.

Se os suportes das duas cópias tiverem uma taxa de falha media de 1% por ano e as falhas forem independentes, há uma probabilidade de 0,01% de que ambas as cópias falhem no mesmo ano. Se a política de um repositório limitar a perda a não mais de 0,001% da coleção por ano, com o objetivo, claro, de perder 0%, depois o repositório teria de confirmar a integridade dos meios de comunicação social pelo menos de 72 em 72 dias para atingir um tempo médio de recuperação de 36 dias, ou seja, cerca de um décimo de um ano. Esse exemplo simplificado ilustra o tipo de questões que um repositório deve considerar, mas o objetivo é um tratamento abrangente das fontes de perda de dados e do seu mundo real e complexidade. Quaisquer dados que sejam (temporariamente) perdidos devem ser recuperáveis a partir de cópias de segurança.

C1.6 Repositório reporta à sua administração todos os incidentes de corrupção ou perda de dados, e medidas tomadas para reparar/substituir dados corrompidos ou perdidos.

A existência de mecanismos eficazes para detectar a corrupção e a perda de bits num sistema de repositório é fundamental, mas é apenas uma parte importante de um processo mais vasto. No seu conjunto, o repositório deve registrar, relatar e reparar como possíveis todas as violações da integridade dos dados. Isso

significa que o sistema deve poder notificar os administradores do sistema de quaisquer problemas registrados. Esses incidentes, as ações de recuperação e os seus resultados devem ser reportados aos administradores e devem estar disponíveis.

Por exemplo, o repositório deve documentar os procedimentos a seguir, quando é detectada uma perda ou corrupção, incluindo normas para medir o sucesso das recuperações. Quaisquer ações empreendidas para reparar objetos, como parte desses procedimentos, devem ser registrados. A natureza desse registro deve ser documentada pelo repositório, e a informação deve poder ser recuperada quando necessário. Essa documentação desempenha um papel fundamental na medição da autenticidade e integridade dos dados na posse do repositório.

C1.7 O Repositório tem processos definidos para a mudança de suportes de armazenamento e/ou hardware (por exemplo refrescante, migração).

O repositório deve ter acionadores para iniciar a ação e compreender quanto tempo demorará a migração de suportes de armazenamento, ou "refrescamento" - copiar entre suportes sem reformatar o fluxo de bits.

Irá terminar antes da mídia estar morta, por exemplo? A cópia de grandes quantidades de dados pode demorar muito tempo. e pode afetar o desempenho de outros sistemas. É importante que o processo inclua uma verificação de que a cópia aconteceu corretamente. (Ver B4.2.)

Os repositórios devem também considerar a obsolescência de qualquer/todos os componentes de hardware, dentro do repositório, como potenciais eventos de desencadeamento da migração. Cada vez mais, é difícil obter suporte adequado, em longo prazo para sistemas componentes de hardware, expondo os repositórios a riscos e responsabilidades, caso eles escolham continuar a operar o hardware além do fabricante ou do suporte de terceiros.

C1.8 O Repositório tem um processo documentado de gestão de alterações que identifica as alterações a processos críticos que afetam potencialmente a capacidade do repositório para cumprir os seus responsabilidades obrigatórias.

Entre os exemplos, contam-se as alterações nos processos de gestão de dados, acesso e armazenamento de arquivos, ingerir, e segurança. O que é realmente

importante é saber que mudanças foram feitas e quando foram feitas. A rastreabilidade permite compreender o que foi afetado por alterações específicas nos sistemas.

C1.9 O Repositório tem um processo para testar o efeito de alterações críticas no sistema.

As alterações aos sistemas críticos devem, sempre que possível, ser pré-testadas separadamente, os comportamentos esperados. documentados, e procedimentos de desmantelamento preparados. Após as alterações, os sistemas devem ser monitorizados para comportamento inesperado e inaceitável. Se tal comportamento for descoberto, as mudanças e as suas consequências devem ser invertidas.

Os ensaios em todo o sistema ou o ensaio de unidades podem satisfazer este requisito; os ensaios complexos do tipo segurança não são necessários. Os testes podem ser muito dispendiosos, mas deve haver algum reconhecimento do fato de que um regime completamente aberto, em que nenhuma alteração seja avaliada ou testada, terá problemas.

C1.10 O Repositório tem um processo para reagir à disponibilidade de novas atualizações de segurança de software com base numa avaliação de risco-benefício.

As decisões de aplicar atualizações de segurança são, provavelmente, o resultado de uma avaliação de risco-benefício; Os *patches* de segurança são frequentemente responsáveis por perturbar aspectos alternativos da funcionalidade do sistema ou desempenho. Pode não ser necessário que um repositório implemente todos os *patches* de software, e a aplicação de qualquer uma delas deve ser cuidadosamente ponderada. Cada atualização de segurança implementada pelo repositório deve ser documentada com detalhes sobre a forma como é concluída; tanto automáticas como manuais são aceitáveis atualizações. As atualizações de segurança significativas podem pertencer a outro *software* que não o núcleo sistemas operativos, tais como aplicações de bases de dados e servidores Web, e estas devem também ser documentadas.

C2. Tecnologias adequadas

Um repositório deve utilizar estratégias e normas relevantes para a(s) sua(s) comunidade(s) designada(s) e para a(s) sua(s) comunidade(s) digital(ais) tecnologias.

C2.1 O Repositório dispõe de tecnologias de hardware adequadas aos serviços que presta às suas comunidade(s) designada(s) e dispõe de procedimentos para receber e acompanhar notificações e avaliar quando são necessárias alterações de tecnologia de hardware.

O repositório tem de estar ciente dos tipos de serviços de acesso esperados pelas suas comunidade(s), incluindo, se for caso disso, os tipos de meios de comunicação a fornecer, e deve assegurar que as suas capacidades de hardware podem suportar esses serviços. Por exemplo, pode ter de melhorar a largura de banda de sua ligação em rede, ao longo do tempo, para satisfazer o volume crescente de dados de acesso e as expectativas.

C2.2 O Repositório dispõe de tecnologias de software adequadas aos serviços que presta à sua(s) comunidade(s) designada(s) e dispõe de procedimentos para receber e acompanhar notificações, e avaliar quando são necessárias alterações tecnológicas de software.

O repositório tem de estar ciente dos tipos de serviços de acesso esperados pelas suas comunidade(s), e para garantir que as suas capacidades de *software* possam apoiar esses serviços. Por exemplo, pode ter de acrescentar traduções de formato para satisfazer as necessidades das ferramentas de aplicação, atualmente, muito utilizadas, ou pode ter de acrescentar um serviço de subconfiguração de dados para objetos de dados muito grandes.

C3. Segurança

O termo "sistema" refere-se aqui a mais do que sistemas informáticos, tais como *servidores, firewalls ou routers*. A proteção contra incêndios e os sistemas de detecção de inundações também são significativos, tal como os sistemas que envolvem ações por parte das pessoas. Os dois primeiros requisitos aqui são gerais e o terceiro aborda a segurança interna, enquanto o restante aborda a recuperação em caso de catástrofe.

C3.1 O Repositório mantém uma análise sistemática de fatores tais como dados, sistemas, pessoal, instalações físicas, e necessidades de segurança.

A avaliação regular dos riscos deve abordar as ameaças externas e os ataques de negação de serviço. Essas análises são susceptíveis de serem documentadas em vários locais diferentes e não precisam de ser contidas de forma exaustiva num único documento

C3.2 O Repositório implementou controles para abordar adequadamente cada uma das necessidades de segurança.

O repositório deve mostrar como tem lidado com as suas necessidades de segurança. Se alguns tipos de materiais forem mais susceptíveis de serem atacados, o repositório terá de proporcionar mais proteção, por exemplo.

C3.3 O pessoal do Repositório tem funções, responsabilidades e autorizações delineadas em relação a implementar alterações no sistema.

As autorizações sobre quem pode fazer o quê - quem pode adicionar utilizadores, quem tem acesso a metadados de alteração, quem pode obter os registros de auditoria. É importante que as autorizações sejam justificadas, que o pessoal compreenda o que são autorizados a fazer, e que existe uma visão consistente disto em toda a organização.

C3.4 O Repositório possui plano(s) escrito(s) adequado(s) de preparação para catástrofes e recuperação, incluindo pelo menos uma cópia de segurança externa de toda a informação preservada, juntamente com uma cópia externa do plano(s) de recuperação.

O repositório deve ter um plano escrito com algum processo de aprovação para o que acontece em tipos específicos de catástrofe (incêndio, inundação, comprometimento do sistema, etc.) e por quem tem responsabilidade pelas ações. O nível de detalhamento de um plano de emergência e os riscos específicos abordados devem ser adequados à localização do repositório e expectativas do serviço. O incêndio é uma preocupação quase universal, mas os terremotos podem não exigir planejamento em todos os locais. O plano de emergência deve, no entanto, lidar com situações não especificadas que têm consequências específicas, como a falta de acesso a um edifício.

APÊNDICE D - AUDITORIA E CERTIFICAÇÃO DE REPOSITÓRIOS CONFIÁVEIS: CRITÉRIOS E LISTA DE VERIFICAÇÃO (ACTDR)

Seção	3 Infraestrutura Organizacional
Categoria	3.1. Governança e Viabilidade Organizacional
Critério	3.1.1 O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, retenção no longo prazo, gerenciamento e acesso a informações digitais.
Texto de suporte	Isso é necessário para garantir o compromisso com a preservação, retenção, gerenciamento e acesso no mais alto nível administrativo do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Declaração de missão ou documento constitutivo do repositório ou de sua organização matriz que lide especificamente ou implique implicitamente a preservação de informações e / ou outros recursos sob seu alcance; um mandato regulamentar legal, estatutário ou governamental aplicável ao repositório que lide especificamente ou exija implicitamente a preservação, retenção, gerenciamento e acesso a informações e / ou outros recursos sob sua alçada.
Discussão	A declaração de missão do repositório ou da organização-mãe deve abordar explicitamente a preservação. Se a preservação não estiver entre os principais objetivos de uma organização que abriga um repositório digital, a preservação poderá não ser essencial para a missão da organização. Em alguns casos, um repositório segue sua missão de preservação como consequência dos objetivos maiores de uma organização em que está alojado, como uma universidade ou uma agência governamental, e sua missão mais restrita pode ser formalizada por meio de políticas explicitamente adotadas e aprovadas pelos maiores organização. Órgãos governamentais e outras organizações podem ter mandatos legais que exigem a preservação de materiais; nesse caso, esses mandatos podem ser substituídos por declarações de missão, pois definem o objetivo da organização.

Seção	3 Infraestrutura Organizacional
Categoria	3.1. Governança e Viabilidade Organizacional
Critério	3.1.2 O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório adotará no suporte no longo prazo de sua missão.
Texto de suporte	Isso é necessário para ajudar o repositório a tomar decisões administrativas, moldar políticas e alocar recursos para preservar com êxito suas propriedades.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Plano Estratégico de Preservação; ata de reunião; documentação das decisões administrativas que foram tomadas.
Discussão	O plano estratégico deve ser baseado na missão estabelecida da organização e em seus valores, visão e objetivos definidos. Os planos estratégicos geralmente cobrem um período de tempo finito específico, normalmente no intervalo de 3 a 5 anos.

Seção	3 Infraestrutura Organizacional
Categoria	3.1. Governança e Viabilidade Organizacional
Critério	3.1.2 O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório adotará no suporte no longo prazo de sua missão.
Subcritério	3.1.2.1 O repositório deve ter um plano de sucessão, planos de contingência e / ou custódia adequados, caso o repositório deixe de operar ou a instituição governadora ou financiadora mude substancialmente seu escopo.
Texto de suporte	Isso é necessário para preservar o conteúdo da informação confiada ao repositório, entregando-o a outro custodiante, caso o repositório deixe de operar.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Plano (s) de Contingência e de Sucessão escritos e críveis; declaração explícita e específica que documenta a intenção de garantir a continuidade do repositório e as medidas tomadas e a serem tomadas para garantir a continuidade; garantia de código, software e metadados críticos suficientes para permitir a reconstituição do repositório e seu conteúdo em caso de falha do repositório; custódia e/ou fundos de reserva reservados para contingências; acordos explícitos com organizações sucessoras documentando as medidas a serem tomadas para garantir a transferência completa e formal de responsabilidade pelo conteúdo digital do repositório e ativos relacionados, e concedendo os direitos necessários para garantir a continuidade do conteúdo e dos serviços do repositório.
Discussão	A falha de um repositório ameaça a sustentabilidade no longo prazo do conteúdo de informações de um repositório. Não é suficiente para o repositório ter um plano ou política informal a respeito de onde seus dados vão, caso ocorra uma falha. Um plano formal com procedimentos identificados precisam estar em vigor.

Seção	3 Infraestrutura Organizacional
Categoria	3.1. Governança e Viabilidade Organizacional
Critério	3.1.2 O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório adotará no suporte no longo prazo de sua missão.
SubCritério	3.1.2.2 O repositório deve monitorar seu ambiente organizacional para determinar quando executar seu plano de sucessão, planos de contingência e / ou acordos de custódia.
Texto de suporte	Isso é necessário para garantir que o repositório possa reconhecer quando é necessário executar esses planos.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Políticas administrativas, procedimentos, protocolos, requisitos; documentos de orçamentos e análises financeiras; calendários fiscais; Plano(s) de negócios; qualquer evidência de monitoramento e preparação ativos.
Discussão	O gerenciamento de um repositório deve ter procedimentos formais para verificar periodicamente a viabilidade do repositório. Essa verificação periódica deve ser usada para determinar se, ou quando, executar o plano formal de sucessão do repositório, planos de contingência e / ou acordos de custódia.

Seção	3 Infraestrutura Organizacional
Categoria	3.1. Governança e Viabilidade Organizacional
Critério	3.1.3 O repositório deve ter uma Política de Coleta ou outro documento que especifique o tipo de informação à qual preservará, reterá, gerenciará e fornecerá acesso.
Texto de suporte	Isso é necessário para que o repositório tenha orientações sobre a aquisição de conteúdo digital ao qual preservará, reterá, gerenciará e fornecerá acesso.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Política de cobrança e documentos comprovativos; Política de Preservação, missão, objetivos e visão do repositório.
Discussão	A política de coleta pode ser usada para entender o que o repositório contém, o que não contém e por quê. A política de coleta suporta a missão mais ampla do repositório. Sem essa política, é provável que o repositório colete de maneira aleatória ou armazene grandes quantidades de conteúdo digital de baixo valor. A política de coleta ajuda a organização a identificar qual conteúdo digital será ou não aceito para ingestão. Em uma organização com uma missão mais ampla do que a preservação do conteúdo digital, a política de coleta ajuda a definir o papel do repositório dentro do contexto organizacional maior.

Seção	3 Infraestrutura Organizacional
Categoria	3.2. Estrutura Organizacional e Pessoal
Critério	3.2.1 O repositório deve ter identificado e estabelecido o deveres que ele precisa executar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir esses deveres.
Discussão	A equipe do repositório deve ser composta por pessoal com o treinamento e as habilidades necessárias para realizar as atividades do repositório. O repositório deve ser capaz de documentar, por meio de planos de desenvolvimento, organogramas, descrições de cargos e políticas e procedimentos relacionados que o repositório está definindo e mantendo as habilidades e funções necessárias para a operação sustentada do repositório.

Seção	3 Infraestrutura Organizacional
Categoria	3.2. Estrutura Organizacional e Pessoal
Critério	3.2.1 O repositório deve ter identificado e estabelecido o deveres que ele precisa executar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir esses deveres.
Subcritério	3.2.1.1 O repositório deve ter identificado e estabelecido as tarefas que ele precisa executar.
Texto de suporte	Isso é necessário para garantir que o repositório possa concluir todas as tarefas associadas à preservação e gerenciamento de longo prazo dos objetos de dados.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Um plano de pessoal; definições de competência; descrições de emprego; planos de desenvolvimento profissional da equipe; certificados de treinamento e credenciamento; além de evidências de que o repositório analisa e mantém esses documentos à medida que os requisitos evoluem.
Discussão	A preservação depende de uma série de atividades, desde a manutenção de hardware e software até a migração de conteúdo e mídia de armazenamento, até a negociação de acordos de direitos de propriedade intelectual. Para garantir a sustentabilidade, em longo prazo, um repositório deve estar ciente de todas as atividades necessárias e demonstrar que pode concluí-las com êxito. O repositório pode atingir esses objetivos, por exemplo, identificando as competências e os conjuntos de habilidades necessários para realizar suas atividades ao longo do tempo - por exemplo, treinamento em arquivamento, habilidades técnicas e conhecimento jurídico.

Seção	3 Infraestrutura Organizacional
Categoria	3.2. Estrutura Organizacional e Pessoal
Critério	3.2.1 O repositório deve ter identificado e estabelecido os deveres que ele precisa executar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir esses deveres.
Subcritério	3.2.1.2 O repositório deve ter o número apropriado de funcionários para apoiar todas as funções e serviços.
Texto de suporte	Isso é necessário para garantir que os níveis de pessoal do repositório sejam adequados para preservar o conteúdo digital e fornecer um repositório seguro e de qualidade.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Organogramas; definições de papéis e responsabilidades; comparação dos níveis de pessoal com os padrões e padrões da indústria.
Discussão	O repositório deve determinar o número e o nível adequados de equipe que correspondem aos requisitos e compromissos. O repositório também deve demonstrar como avalia a eficácia e adequação da equipe para apoiar suas funções e serviços.

Seção	3 Infraestrutura Organizacional
Categoria	3.2. Estrutura Organizacional e Pessoal
Critério	3.2.1 O repositório deve ter identificado e estabelecido o deveres que ele precisa executar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir esses deveres.
Subcritério	3.2.1.3 O repositório deve ter um programa ativo de desenvolvimento profissional que forneça aos funcionários habilidades e oportunidades de desenvolvimento de conhecimentos.
Texto de suporte	Isso é necessário para garantir que os conjuntos de habilidades da equipe evoluam à medida que a tecnologia do repositório e os procedimentos de preservação mudam.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Planos e relatórios de desenvolvimento profissional; requisitos de treinamento e orçamentos de treinamento, documentação das despesas de treinamento (valor por equipe); metas de desempenho e documentação das atribuições e realizações do pessoal, cópias de certificados concedidos.
Discussão	A tecnologia e as práticas gerais de preservação digital continuarão mudando, assim como os requisitos de sua Comunidade Designada; portanto, o repositório deve garantir que os conjuntos de habilidades de sua equipe evoluam. Idealmente, o repositório atenderá a esse requisito por meio de uma abordagem de aprendizado ao longo da vida para desenvolver e reter funcionários.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.1 O repositório deve ter definido sua Comunidade Designada e a(s) base(s) de conhecimento associada(s) e deve ter essas definições adequadamente acessíveis.
Texto de suporte	Isso é necessário para que seja possível testar se o repositório atende às necessidades de sua Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Uma definição escrita da Comunidade Designada.
Discussão	A Comunidade Designada é definida como “um grupo identificado de Consumidores em potencial que deve ser capaz de entender um conjunto específico de informações. A comunidade designada pode ser composta por várias comunidades de usuários. Uma comunidade designada é definida pelo arquivo e essa definição pode mudar / evoluir ao longo do tempo”. - O repositório definiu as partes externas e seus ativos, proprietários e usos. Dois grupos: os editores de periódicos acadêmicos e seus leitores, cada um com direitos diferentes para acessar o material e os diferentes serviços oferecidos a eles. Alguns repositórios podem se chamar, por exemplo, de “arquivo escuro”, um arquivo que possui uma política para não permitir que os consumidores tenham acesso ao seu conteúdo por um determinado período de tempo, mas, no entanto, precisariam de uma Comunidade Designada.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.2 O repositório deve ter Políticas de Preservação em vigor para garantir que seu Plano Estratégico de Preservação seja cumprido.
Texto de suporte	Isso é necessário para garantir que o repositório possa cumprir a parte de sua missão relacionada à preservação.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Políticas de Preservação; Declaração de Missão do Repositório.
Discussão	As políticas do repositório mostram como o repositório atende aos requisitos do plano estratégico de preservação do repositório. Por exemplo, um plano estratégico de preservação pode conter um requisito de que o repositório “cumpra os atuais padrões de preservação preferenciais”. A política de preservação pode então exigir que o repositório “monitore os padrões atuais de preservação e garanta a conformidade do repositório com os padrões preferidos de preservação”. Em outro exemplo, o plano estratégico pode exigir que o repositório mantenha seus dados compreensíveis. A política de preservação pode incluir informações sobre o nível esperado de compreensibilidade da Comunidade Designada do repositório para cada Pacote de Informações de Arquivamento.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.2 O repositório deve ter Políticas de Preservação em vigor para garantir que seu Plano Estratégico de Preservação seja cumprido.
Subcritério	3.3.2.1 O repositório deve ter mecanismos para revisão, atualização e desenvolvimento contínuo de suas Políticas de Preservação à medida que o repositório cresce e à medida que a tecnologia e a prática da comunidade evoluem.
Texto de suporte	Isso é necessário para que o repositório tenha políticas e procedimentos completos e atualizados, que reflitam os requisitos e práticas atuais de suas comunidades para preservação.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação escrita atual e passada na forma de políticas de preservação, planos estratégicos de preservação e planos de implementação de preservação, procedimentos, protocolos e fluxos de trabalho; especificações de ciclos de revisão para documentação; documentação detalhando revisões, pesquisas e *feedback*. Se a documentação estiver incorporada na lógica do sistema, a funcionalidade deve demonstrar a implementação de políticas e procedimentos.
Discussão	As políticas de preservação capturam compromissos e intenções organizacionais em termos de pessoal, segurança e outras preocupações relacionadas à preservação. Os Planos de Implementação de Preservação abordam atividades e práticas de preservação, como transferência, envio, controle de qualidade, gerenciamento de armazenamento, gerenciamento de metadados e gerenciamento de acesso e direitos. O repositório pode achar benéfico manter todas as versões das políticas de preservação (por exemplo, versões desatualizadas são claramente identificadas e mantidas de alguma forma organizada) para documentar os resultados do monitoramento de novos desenvolvimentos, mostrando a capacidade de resposta do repositório aos padrões e práticas vigentes, requisitos emergentes e padrões específicos para o domínio, se apropriado, e desenvolvimentos semelhantes. Funcionários e colegas qualificados são uma parte importante do processo de revisão, pois eles ajudam a atualizar e expandir esses documentos. As políticas devem ser compreensíveis pela equipe do repositório para que eles possam realizar seu trabalho. Políticas e procedimentos de preservação devem ser demonstrados como compreensíveis e implementáveis.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.3. O repositório deve ter um histórico documentado das alterações em suas operações, procedimentos, software e hardware.
Texto de suporte	Isso é necessário para fornecer uma 'trilha de auditoria' através da qual as partes interessadas possam identificar e rastrear as decisões tomadas pelo repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Inventários de equipamentos de capital; documentação da aquisição, implementação, atualização e desativação de software e hardware críticos para repositórios; cronogramas e políticas de retenção e descarte de arquivos, cópias de versões anteriores de políticas e procedimentos; minutos de encontros.
Discussão	Esta documentação pode incluir decisões sobre a infraestrutura organizacional e técnica. Documentação ou entrevistas com a equipe apropriada que possa explicar as práticas e o fluxo de trabalho do repositório devem estar disponíveis.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.4 O repositório deve se comprometer com a transparência e a responsabilidade em todas as ações que suportam a operação e o gerenciamento do repositório que afetam a preservação do conteúdo digital ao longo do tempo.
Texto de suporte	Isso é necessário porque a transparência, no sentido de estar disponível para quem deseja conhecer, é a melhor garantia de que o repositório opera de acordo com os padrões e práticas aceitos.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Relatórios de auditorias e certificações financeiras e técnicas; divulgação de documentos de governança, análises independentes de programas e contratos e acordos com fornecedores de financiamento e serviços críticos.
Discussão	Se o repositório usar software para capturar informações sobre seu histórico, ele poderá demonstrar essas ferramentas de rastreamento. Quando apropriado, o histórico está vinculado a estratégias de preservação relevantes e descreve os possíveis efeitos na preservação de conteúdo digital. Esse requisito não significa que a organização deve disponibilizar informações que a tornariam vulnerável aos concorrentes, mas sim que a organização se comprometa a divulgar seus métodos para preservar o conteúdo digital, pelo menos para a Comunidade Designada ou outro interessado apropriado, a fim de demonstrar que está atendendo a todos os requisitos atuais de preservação.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.5 O repositório deve definir, coletar, rastrear e fornecer adequadamente suas medidas de integridade da informação.
Texto de suporte	Isso é necessário para fornecer documentação que tenha desenvolvido ou adaptado as medidas apropriadas para garantir a integridade de sua participação.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Definição ou especificação por escrito das medidas de integridade do repositório (por exemplo, soma de verificação computada ou valor de *hash*); documentação dos procedimentos e mecanismos para monitorar medições de integridade e responder a resultados de medições de integridade que indicam que o conteúdo digital está em risco; um processo de auditoria para coletar, rastrear e apresentar medições de integridade; Política de preservação e documentação do fluxo de trabalho.
Discussão	Os mecanismos para medir a integridade evoluirão, à medida que a tecnologia evoluir. O repositório pode fornecer documentação que tenha desenvolvido ou adaptado as medidas apropriadas para garantir a integridade de seus acervos. Se protocolos, regras e mecanismos estiverem incorporados no software do repositório, deve haver alguma maneira de demonstrar a implementação de medidas de integridade.

Seção	3 Infraestrutura Organizacional
Categoria	3.3. Responsabilização Processual e Política de Preservação Estrutural
Critério	3.3.6. O repositório deve se comprometer com um cronograma regular de autoavaliação e certificação externa.
Texto de suporte	Isso é necessário para garantir que o repositório continue confiável e que não haja ameaça ao seu conteúdo.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Listas de verificação concluídas e datadas de autoavaliações e / ou auditorias de terceiros; certificados concedidos para conformidade com as normas ISO relevantes; cronogramas e evidências de alocações orçamentárias adequadas para certificação futura.
Discussão	Uma verificação única da confiabilidade não é adequada porque muitas coisas mudam ao longo do tempo. Um compromisso de longo prazo deve ser demonstrado.

Seção	3 Infraestrutura Organizacional
Categoria	3.4. Sustentabilidade Financeira
Critério	3.4.1 O repositório deve ter processos de planejamento de negócios de curto e longo prazo para manter o repositório ao longo do tempo.
Texto de suporte	Isso é necessário para garantir a viabilidade do repositório durante o período prometido para fornecer acesso ao seu conteúdo para sua Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Planos estratégicos, operacionais e / ou de negócios atualizados e plurianuais; demonstrações financeiras anuais auditadas; previsões financeiras com vários cenários orçamentários; planos de contingência; análise de mercado.
Discussão	Um processo anual de planejamento de negócios é geralmente aceito como padrão para a maioria das organizações.

Seção	3 Infraestrutura Organizacional
Categoria	3.4. Sustentabilidade Financeira
Critério	3.4.2 O repositório deve ter práticas e procedimentos financeiros transparentes, compatíveis com as normas e práticas contábeis relevantes e auditados por terceiros de acordo com os requisitos legais territoriais.
Texto de suporte	Isso é necessário para se proteger contra improbidade ou outra atividade indesejável que possa ameaçar a viabilidade econômica do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Requisitos de disseminação demonstrados para práticas e planejamento de negócios; citações e / ou exemplos de requisitos, normas e práticas de contabilidade e auditoria; demonstrações financeiras anuais auditadas.
Discussão	O repositório não pode simplesmente reivindicar transparência, mas deve mostrar que ajusta suas práticas de negócios para mantê-las transparentes, compatíveis e auditáveis. Os requisitos de confidencialidade podem proibir a divulgação de informações sobre as finanças do repositório, mas o repositório deve ser capaz de demonstrar que está satisfazendo as necessidades de sua Comunidade Designada.

Seção	3 Infraestrutura Organizacional
Categoria	3.4. Sustentabilidade Financeira
Critério	3.4.3 O repositório deve ter um compromisso contínuo de analisar e relatar riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).
Texto de suporte	Isso é necessário para demonstrar que o repositório identificou e documentou essas categorias e as gerencia ativamente, inclusive identificando e respondendo a riscos, descrevendo e aproveitando benefícios, especificando e equilibrando investimentos e antecipando e preparando as despesas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentos de gerenciamento de riscos que identificam ameaças percebidas e potenciais e respostas planejadas ou implementadas (um registro de riscos); documentos de planejamento de investimentos em infraestrutura de tecnologia; análises de custo / benefício; documentos financeiros e portfólios de investimento; requisitos e exemplos de licenças, contratos e gerenciamento de ativos; evidência de revisão com base no risco.
Discussão	O repositório deve ter o objetivo de manter um equilíbrio apropriado entre risco e benefícios, investimento e retorno.

Seção	3 Infraestrutura Organizacional
Categoria	3.5 Contratos, Licenças e Passivos
Critério	3.5.1 O repositório deve ter e manter contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e / ou aos quais fornece acesso.
Texto de suporte	Isso é necessário para garantir que o repositório tenha os direitos e autorizações necessários para permitir a coleta e preservação de conteúdo digital ao longo do tempo, disponibilizar essas informações para a Comunidade Designada e defendê-los quando contestado.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Contratos e licenças de depósito devidamente assinados e executados, de acordo com as leis e regulamentos locais, nacionais e internacionais; políticas sobre acordos de depósito de terceiros; definições de níveis de serviço e usos permitidos; políticas de repositório para o tratamento de 'obras órfãs' e resolução de disputas de direitos autorais; relatórios de avaliações de risco independentes dessas políticas; procedimentos para revisar e manter regularmente acordos, contratos e licenças.
Discussão	Os repositórios podem precisar mostrar evidências de que seus contratos estão sendo seguidos. Isso é especialmente importante para aqueles com acordos de depósito de terceiros. Esses acordos podem exigir que o repositório garanta que contratos, licenças ou acordos de depósito relevantes expressem direitos, responsabilidades e expectativas de cada parte. Contratos e acordos formais de depósito devem ser legítimos; isto é, eles precisam ser assinados e atualizados. Quando o relacionamento entre depositante e repositório é menos formal (por exemplo, um membro do corpo docente que deposita trabalho no repositório de preservação de uma instituição acadêmica), deve ser fornecida documentação a cada articulador que articule as capacidades e compromissos do repositório. Os repositórios envolvidos na coleta na Web podem achar esse requisito difícil devido à maneira como as informações baseadas na Web são coletadas / capturadas para preservação no longo prazo, e, portanto, raramente são necessários contratos ou acordos de depósito. Alguns repositórios capturam, gerenciam e preservam o acesso a esse material sem a permissão por escrito dos criadores do conteúdo. Outros passam pelo processo muito dispendioso e dispendioso de entrar em contato com os proprietários do conteúdo antes de capturar e ingerir informações. Idealmente, os acordos são rastreados, vinculados, gerenciados e disponibilizados em um banco de dados de contratos.

Seção	3 Infraestrutura Organizacional
Categoria	3.5 Contratos, Licenças e Passivos
Critério	3.5.1 O repositório deve ter e manter contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e / ou aos quais fornece acesso.
Subcritério	3.5.1.1 O repositório deve ter contratos ou acordos de depósito que especifiquem e transfiram todos os direitos de preservação necessários, e esses direitos transferidos devem ser documentados.
Texto de suporte	Isso é necessário para ter controle suficiente das informações para preservação e limitar a exposição do repositório a responsabilidades ou danos legais e financeiros.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Contratos, acordos de depósito; especificações dos direitos transferidos para diferentes tipos de conteúdo digital (se aplicável); declarações de política sobre os direitos de preservação necessários.
Discussão	Como o direito de alterar ou alterar informações digitais geralmente é restrito por lei ao criador, é importante que os contratos e contratos do repositório digital atendam à necessidade de poder trabalhar e modificar objetos digitais para mantê-los acessíveis. Os acordos de repositório com depositantes devem especificar e / ou transferir para o repositório certos direitos, permitindo ações de preservação apropriadas e necessárias para os objetos digitais dentro do repositório. Como as negociações legais podem levar tempo, potencialmente impedindo ou diminuindo a ingestão de objetos digitais em risco, é aceitável que um repositório digital aceite objetos digitais, mesmo com apenas direitos mínimos de preservação usando um contrato aberto e, em seguida, lide com a expansão de direitos detalhados posteriormente.

Seção	3 Infraestrutura Organizacional
Categoria	3.5 Contratos, Licenças e Passivos
Critério	3.5.1.2 O repositório deve ter especificado todos os aspectos apropriados de aquisição, manutenção, acesso e retirada em acordos escritos com depositantes e outras partes relevantes.
Texto de suporte	Isso é necessário para garantir que os respectivos papéis de repositório, produtores e colaboradores no depósito de conteúdo digital e na transferência de responsabilidade pela preservação sejam compreendidos e aceitos por todas as partes.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Contratos de submissão, contratos de depósito e ações de presente devidamente executados; procedimentos operacionais padrão escritos.
Discussão	O contrato de depósito especifica todos os aspectos desses problemas que são necessários para o repositório executar sua função. Pode haver um único contrato cobrindo todos os depósitos, ou contratos específicos para cada depósito, ou um contrato padrão complementado por condições especiais para alguns depósitos. Essas condições especiais podem adicionar ao contrato padrão ou substituir alguns aspectos do contrato padrão. Os acordos podem precisar cobrir restrições de acesso e precisarão cobrir todos os direitos de propriedade dos objetos digitais. Os acordos podem atribuir responsabilidades aos depositantes, como garantir que os SIPs (Submission Information Packages) estejam em conformidade com alguns padrões pré-acordados e permitir que os repositórios recusem SIPs que não atendam a esses padrões. Outros repositórios podem assumir a responsabilidade de corrigir erros nos SIPs. A divisão de responsabilidades deve sempre ser clara. Acordos, escritos ou não, podem nem sempre ser necessários. O ônus da prova está no repositório para demonstrar que ele não precisa de tais acordos porque, por exemplo, possui um mandato legal para suas atividades. Um acordo deve incluir, no mínimo, direitos de propriedade, direitos de acesso, condições para retirada, nível de segurança, nível de auxílio para busca, definições de SIP, tempo, volume e conteúdo das transferências. Um exemplo de um padrão a seguir para isso é o Padrão Abstrato da Metodologia da Interface entre Produtores e Arquivos CCSDS / ISO.

Seção	3 Infraestrutura Organizacional
Categoria	3.5 Contratos, Licenças e Passivos
Critério	3.5.1.3 O repositório deve ter políticas escritas que indiquem quando ele aceita a responsabilidade de preservação pelo conteúdo de cada conjunto de objetos de dados enviados.
Texto de suporte	Isso é necessário para evitar mal-entendidos entre o repositório e o produtor / depositante sobre quando e como ocorre a transferência de responsabilidade pelo conteúdo digital.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Contratos de submissão, contratos de depósito e ações de presente devidamente executados; recibo de confirmação enviado de volta ao produtor / depositante.
Discussão	Se esse requisito não for atendido, existe o risco de, por exemplo, apagar o original antes que o repositório assuma a responsabilidade pelos objetos de dados enviados. Sem o entendimento de que o repositório já assumiu a responsabilidade de preservação pelo SIP, existe o risco de que o produtor / depositante faça alterações nos dados e estes não sejam adequadamente preservados, pois já foram ingeridos pelo repositório. Por exemplo, por conveniência, o repositório poderia receber uma cópia dos dados brutos da ciência do instrumento ao mesmo tempo que a equipe científica os obtém, mas a equipe científica seria responsável por eles até que passasse a responsabilidade para o repositório final. Repositórios que relatam aos seus depositantes geralmente marcarão essa aceitação com alguma forma de notificação (por exemplo, recibos de confirmação) ao depositante. (Isso pode depender das responsabilidades do repositório, conforme designado no contrato de depositante.) Um repositório pode marcar a transferência enviando um documento formal, geralmente uma cópia final assinada do contrato de transferência, de volta ao depositante, significando a conclusão da transformação de SIP para SIP. Processo AIP. Outras abordagens são igualmente aceitáveis. Atualizações diárias breves podem ser geradas por um repositório que fornece apenas relatórios formais anuais de transferência.

Seção	3 Infraestrutura Organizacional
Categoria	3.5 Contratos, Licenças e Passivos
Critério	3.5.1.4 O repositório deve ter políticas em vigor para lidar com responsabilidades e desafios à propriedade / direitos.
Texto de suporte	Isso é necessário para minimizar possíveis responsabilidades e desafios aos direitos do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Uma definição de direitos, licenças e permissões a serem obtidas de produtores e contribuidores de conteúdo digital; citações de leis e regulamentos relevantes; política de resposta aos desafios; histórico documentado de resposta a desafios de maneiras que não inibem a preservação; registros de assessoria jurídica relevante solicitados e recebidos.
Discussão	As políticas de preservação do repositório e os planos e mecanismos de implementação da preservação devem ser examinados pelas autoridades institucionais apropriadas e / ou especialistas jurídicos para garantir que as respostas aos desafios sigam as leis e requisitos relevantes e que a responsabilidade potencial pelo repositório seja minimizada.

Seção	3 Infraestrutura Organizacional
Categoria	3.5 Contratos, Licenças e Passivos
Critério	3.5.2 O repositório deve rastrear e gerenciar os direitos de propriedade intelectual e as restrições ao uso do conteúdo do repositório, conforme exigido pelo contrato de depósito, contrato ou licença.
Texto de suporte	Isso é necessário para permitir que o repositório rastreie, atue e verifique direitos e restrições relacionados ao uso dos objetos digitais dentro do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Uma declaração de Política de Preservação que define e especifica os requisitos e o processo do repositório para gerenciar os direitos de propriedade intelectual; acordos de depositantes; amostras de acordos e outros documentos que especificam e tratam dos direitos de propriedade intelectual; documentação de monitoramento por repositório ao longo do tempo de alterações no status e propriedade da propriedade intelectual em conteúdo digital mantido pelo repositório; resulta do monitoramento, metadados que capturam informações sobre direitos.
Discussão	O repositório deve ter um mecanismo para rastrear licenças e contratos aos quais é obrigado. Qualquer que seja o formato do sistema de rastreamento, deve ser suficiente para a instituição rastrear, agir e verificar os direitos e restrições relacionados ao uso dos objetos digitais no repositório.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.1 O repositório deve identificar as informações do conteúdo e as propriedades das informações que o repositório preservará.
Texto de suporte	Isso é necessário para deixar claro aos financiadores, depositantes e usuários quais responsabilidades o repositório está assumindo e quais aspectos são excluídos. É também uma etapa necessária para definir as informações necessárias dos produtores ou depositantes de informações.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Declaração de missão; acordos de submissão / acordos de depósito / ações de doações; documentos de fluxo de trabalho e política de preservação, incluindo definição por escrito das propriedades, conforme acordado no contrato de depósito / escritura de doação; procedimentos de processamento escrito; documentação das propriedades a serem preservadas.
Discussão	Esse processo começa em geral com a declaração de missão do repositório e pode ser especificado em acordos de pré-adesão com produtores ou depositantes (por exemplo, contratos de arquivo-produtor) e tornado muito específico em acordos de depósito ou transferência para objetos digitais específicos e sua documentação relacionada. Por exemplo, um repositório pode comprometer-se apenas a preservar o conteúdo textual de um documento e não a sua aparência exata na tela. Outro pode querer preservar a aparência e o layout exatos dos documentos textuais, enquanto outros podem optar por manter as unidades de medida dos campos de dados e normalizar os dados durante o processo de ingestão. Se identificadores exclusivos estiverem associados a objetos digitais antes da ingestão, eles também poderão ser propriedades que precisam ser preservadas.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.1 O repositório deve identificar as Informações de Conteúdo e as propriedades das informações que o repositório preservará.
Subcritério	4.1.1.1 O repositório deve ter um (s) procedimento (s) para identificar essas propriedades de informação que ele preservará.
Texto de suporte	Isso é necessário para estabelecer um entendimento claro com os depositantes, financiadores e comunidades designadas do repositório, como o repositório determina e verifica quais serão as características e propriedades dos itens preservados no longo prazo. Esses procedimentos serão necessários para confirmar a autenticidade ou identificar reivindicações errôneas de autenticidade do registro digital preservado.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Definições das propriedades da informação que devem ser preservadas; contratos de submissão / contratos de depósito, políticas de preservação, procedimentos de processamento por escrito, documentação do fluxo de trabalho.
Discussão	Esses procedimentos documentam os métodos e fatores que um repositório usa para determinar os aspectos de diferentes tipos de Informações de Conteúdo pelos quais ele aceita responsabilidade de preservação para suas comunidades designadas. Por exemplo, o procedimento de um repositório pode ser usar formatos de arquivo para determinar as propriedades que ele preservará, a menos que especificado de outra forma em um contrato de depósito. Nesse caso, o repositório poderá demonstrar a proveniência de objetos que podem ter o mesmo formato de arquivo quando recebidos, mas são preservados de maneira diferente no longo prazo.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.1 O repositório deve identificar as Informações de Conteúdo e as propriedades das informações que o repositório preservará.
Subcritério	4.1.1.2 O repositório deve ter um registro das Informações do Conteúdo e das Propriedades das Informações que ele preservará.
Texto de suporte	Isso é necessário para identificar por escrito as informações de conteúdo dos registros pelos quais ele assumiu a responsabilidade de preservação e as propriedades das informações que se comprometeu a preservar para esses registros com base nas informações de conteúdo.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Políticas de preservação, manuais de processamento, inventários ou pesquisas de coleta, registros dos tipos de informações de conteúdo, estratégias de preservação adquiridas e planos de ação.
Discussão	O repositório deve demonstrar que estabelece e mantém um entendimento de suas coleções digitais suficientes para realizar a preservação necessária para manter as propriedades com as quais se comprometeu. O repositório pode usar essas informações para determinar a eficácia de suas atividades de preservação ao longo do tempo.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.2 O repositório deve especificar claramente as informações que precisam ser associadas a informações específicas de conteúdo no momento de seu depósito.
Texto de suporte	Isso é necessário para que haja um entendimento claro do que precisa ser adquirido do Produtor.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Requisitos de transferência; acordos de produtor-arquivo; planos de fluxo de trabalho para produzir o AIP.
Discussão	Para a maioria dos tipos de objetos digitais a serem ingeridos, o repositório deve ter critérios escritos, preparado pelo repositório por conta própria ou em conjunto com outras partes, que especificam exatamente que objeto(s) digital(is) são transferidos, que documentação está associada com o(s) objeto(s), e quaisquer restrições de acesso, sejam elas técnicas, regulamentares ou impostas pelo doador. Estes critérios documentam quais informações o repositório e suas comunidades designadas podem esperar pelo(s) objeto(s) digital(is) no momento do depósito. O depositante pode ser um processo de colheita criado pelo repositório. O nível de precisão nestas especificações irá variar de acordo com a natureza do a política de coleta do repositório e sua relação com os criadores. Por exemplo, os repositórios engajados na colheita pela Web, ou aqueles que resgatam materiais digitais muito tempo depois de seus criadores abandonaram-nas, não podem impor condições aos criadores do material, pois são não 'depositantes', no sentido usual da palavra. Mas os colhetores Web podem, por exemplo, decidir quais elementos de metadados das transações HTTP que capturaram um *site* devem ser preservados junto com os arquivos do site, e isso ainda constitui 'informação associada ao digital material". Eles também podem optar por registrar as informações ou decisões - sejam elas tomadas por humanos ou por algoritmos automatizados - o que levou à captura do site. O repositório pode verifique o que ele recebe do produtor com base nas especificações.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.3 O repositório deve ter especificações adequadas que permitam o reconhecimento e a análise dos SIPs.
Texto de suporte	Isso é necessário para garantir que o repositório possa extrair informações dos SIPs.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Informações de embalagem para os SIPs; Informações de representação para os dados de conteúdo SIP, incluindo especificações de formato de arquivo documentadas; padrões de dados publicados; documentação da construção válida do objeto.
Discussão	O repositório deve ser capaz de determinar qual é o conteúdo de um SIP com relação à construção técnica de seus componentes. Por exemplo, o repositório precisa reconhecer um arquivo TIFF e confirmar que não é simplesmente um arquivo com um nome de arquivo que termina em 'TIFF'. Outro exemplo seria um site para o qual o repositório precisaria reconhecer e testar a validade da variedade de tipos de arquivo (por exemplo, HTML, imagens, áudio, vídeo, CSS, etc.) que fazem parte do site. . Isso é necessário para confirmar: 1) o SIP é o que o repositório esperava; 2) as informações do conteúdo estão corretamente identificadas; e 3) as propriedades das informações de conteúdo a serem preservadas foram selecionadas adequadamente.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais.
Texto de suporte	Isso é necessário para evitar o fornecimento incorreto de informações às informações preservadas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Acordos de submissão juridicamente vinculativos / acordos de depósito / ações de doação, evidência de medidas tecnológicas apropriadas; logs de procedimentos e autenticações.
Discussão	Os procedimentos operacionais padrão escritos do repositório e as práticas reais devem garantir que os objetos digitais sejam obtidos do depositante esperado. Exemplos de um produtor incluem pessoas, organizações, entidades corporativas ou processos de colheita. Repositórios diferentes adotarão diferentes níveis de prova necessários; a comunidade designada deve ter a oportunidade de revisar as evidências.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.5 O repositório deve ter um processo de ingestão que verifica cada SIP quanto à integridade e correção.
Texto de suporte	Isso é necessário para detectar e corrigir erros no SIP quando criados e possíveis erros de transmissão entre o depositante e o repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Diretiva de preservação adequada e plano de implementação de preservação de documentos e arquivos de log do sistema de sistema (s) que executam procedimento (s) de ingestão; logs ou registros de arquivos recebidos durante o processo de transferência e ingestão; documentação de procedimentos operacionais padrão, procedimentos detalhados e / ou fluxos de trabalho; formato de registros; definições de completude e correção.
Discussão	As informações coletadas durante o processo de ingestão devem ser comparadas com as de alguma outra fonte para verificar a correção do processo de transferência e ingestão de dados. Outras fontes incluem metadados técnicos e descritivos obtidos antes da ingestão e também podem incluir expectativas estabelecidas pelo depositante, pelo produtor do objeto, por um registro de formato ou pelas próprias expectativas do repositório. A extensão em que um repositório pode determinar a correção dependerá do que ele sabe sobre o SIP e de quais ferramentas estão disponíveis para verificar a correção. Pode significar simplesmente verificar se os formatos de arquivo são o que eles alegam ser (os arquivos TIFF têm o formato TIFF válido, por exemplo) ou podem implicar na verificação do conteúdo. Isso pode envolver a verificação humana em alguns casos, como confirmar que a descrição de uma imagem corresponde à imagem. Isso permite que o repositório demonstre que seus objetos preservados copiaram completa e corretamente o que pretendia copiar dos SIPs. Ele também permite que o repositório documente os motivos de outras ações relacionadas ao SIP, como rejeitar a transferência, suspender o processamento até que as informações ausentes sejam recebidas ou simplesmente reportar os erros. Similarmente, a definição de 'completude' deve ser apropriada às atividades de um repositório. Se um inventário de arquivos fosse fornecido por um produtor como parte das negociações de pré-ingestão, seria de se esperar que fossem realizadas verificações nesse inventário. Quaisquer que sejam as verificações realizadas, devem ser consistentes com a própria definição documentada do repositório e com a compreensão da integridade e correção. Uma coisa que um repositório pode querer fazer é verificar a interrupção da rede ou outra corrupção durante o processo de transmissão. é verificar a interrupção da rede ou outra corrupção durante o processo de transmissão.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.
Texto de suporte	Isso é necessário para garantir que a preservação possa ser realizada, com controle físico e seja autorizada, com controle legal.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentos mostrando o nível de controle físico que o repositório realmente possui. Um catálogo separado de banco de dados / metadados, listando todos os objetos digitais no repositório e metadados suficientes para validar a integridade desses objetos (tamanho do arquivo, soma de verificação, hash, local, número de cópias etc.).
Discussão	O repositório deve obter controle completo dos bits dos objetos digitais transmitidos com cada SIP. É necessário controle físico e legal suficiente para que os arquivos façam as alterações exigidas pelo Plano de Implementação de Preservação desses dados e os distribuam aos seus consumidores. Por exemplo, nos casos em que os SIPs fazem referência apenas a objetos digitais, o repositório também deve fazer referência aos objetos digitais ou preservá-los se o repositório atual não estiver comprometido com essa preservação

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.7 O repositório deve fornecer ao produtor / depositante respostas adequadas nos pontos acordados durante os processos de ingestão.
Texto de suporte	Isso é necessário para garantir que o produtor possa verificar se não há falhas inadvertidas na comunicação que, de outra forma, poderiam permitir a perda de SIPs.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Contratos de submissão / contratos de depósito / escrituras de doações; documentação de fluxo de trabalho; procedimentos operacionais padrão; evidência de 'reporte', como relatórios, correspondência, memorandos ou e-mails.
Discussão	Com base no plano de processamento inicial e no acordo entre o repositório e o produtor / depositante, o repositório deve fornecer ao produtor / depositante relatórios de progresso nos pontos acordados durante o processo de ingestão. As respostas do repositório podem variar de nada a relatórios periódicos predeterminados da integridade e correção da ingestão, relatórios de erros e qualquer transferência final do documento de custódia. Os produtores / depositantes podem solicitar informações adicionais *ad hoc* quando os relatórios previamente acordados forem insuficientes.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.1 Ingest: Aquisição de Conteúdo
Critério	4.1.8 O repositório deve ter registros contemporâneos de ações e processos de administração relevantes para a aquisição de conteúdo.
Texto de suporte	Isso é necessário para garantir que essa documentação, que pode ser necessária em uma auditoria, seja capturada e seja precisa e autêntica.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação escrita das decisões e / ou medidas tomadas; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes, recibos de confirmação enviados aos fornecedores.
Discussão	Esses registros devem ser criados no momento ou no horário das ações a que se referem e estão relacionados às ações realizadas durante o processo Ingest: Aquisição de conteúdo (4.1). Os registros podem ser automatizados ou podem ser gravados por indivíduos, dependendo da natureza das ações descritas. Onde padrões comunitários ou internacionais são usados, o repositório deve demonstrar que todas as ações relevantes são realizadas.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.1 O repositório deve ter para cada AIP ou classe de AIPs preservados pelo repositório uma definição associada que seja adequada para analisar o AIP e adequada para as necessidades de preservação de longo prazo.
Texto de suporte	Isso é necessário para garantir que o AIP e sua definição associada, incluindo Informações de Embalagem apropriadas, sempre possam ser encontrados, processados e gerenciados dentro do arquivo.
Subcritério	4.2.1.1 O repositório deve ser capaz de identificar qual definição se aplica a qual AIP.
Texto de suporte	Isso é necessário para garantir que a definição apropriada seja usada ao analisar / interpretar um AIP.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação que vincula claramente cada AIP, ou classe de AIPs, à sua definição.
Discussão	O repositório pode usar qualquer método para associar as definições e os AIPs que forneçam a ligação contínua e contínua das duas entidades.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.1 O repositório deve ter para cada AIP ou classe de AIPs preservados pelo repositório uma definição associada que seja adequada para analisar o AIP e adequada para as necessidades de preservação de longo prazo.
Subcritério	4.2.1.2 O repositório deve ter uma definição de cada AIP que seja adequada para preservação no longo prazo, permitindo a identificação e análise de todos os componentes necessários nesse AIP.
Texto de suporte	Isso é necessário para mostrar explicitamente que os AIPs são adequados ao objetivo a que se destinam, que cada componente de um AIP foi concebido e executado adequadamente e que os planos para a manutenção de cada AIP estão em vigor. (Consulte 4.3, Planejamento de preservação, abaixo.)
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Demonstração do uso das definições para extrair informações de conteúdo e PDI (proveniência, direitos de acesso, contexto, referência e informações de fixação) dos AIPs. Deve-se notar que a proveniência de um objeto digital, por exemplo, pode ser estendida ao longo do tempo para refletir ações adicionais de preservação.
Discussão	A documentação deve identificar cada classe de AIP e descrever como cada uma delas é implementada dentro do repositório. As implementações podem, por exemplo, envolver alguma combinação de arquivos, bancos de dados, e/ou documentos. A documentação deve relacionar o conteúdo do componente AIP com as necessidades de preservação relacionadas do repositório, com detalhes suficientes para os fornecedores do repositório e consumidores a confiarem que as propriedades significativas das AIPs serão preservadas. A documentação deve mostrar claramente que as componentes da AIP, como Informações de Representação e Proveniência, podem ser gerenciadas e mantidas atualizadas. O repositório deve identificar claramente quando novas versões de AIPs precisam ser criadas, a fim de mantê-las aptas para propósito. As dependências externas da AIP também devem ser registradas. As definições devem existir para cada AIP, ou classe de AIP, se houver muitas instâncias da mesma tipo. Os repositórios que armazenam uma grande variedade de tipos de objetos podem precisar de uma definição específica para cada AIP que possuem, mas espera-se que a maioria dos repositórios estabeleça descrições de classe que se aplicam a muitas AIPs. Deve ser possível determinar qual definição se aplica a quais AIPs. Também pode ser necessário que as definições digam algo sobre a semântica ou uso pretendido das AIPs, caso isso possa afetar as decisões de preservação no longo prazo. Por exemplo, a utilização das AIPs, dois repositórios podem ambos preservar apenas imagens estáticas digitais, ambos usando TIFF multi-imagem arquivos como seu formato de preservação. O Repositório 1 consiste inteiramente de arquivos fotográficos de imagens do mundo real destinadas à visualização por pessoas e tem uma única definição que abrange todas as suas AIPs. (A definição pode se referir a uma definição local ou externa do formato TIFF). O Repositório 2 contém algumas imagens, tais como raios-x médicos, que se destinam à análise por computador, ao invés da visualização pelo olho humano, e outras imagens que são como as do Repositório 1. O Repositório 2 talvez deva definir duas classes de AIPs, mesmo que utilize apenas um armazenamento formato para ambos. Uma futura ação de preservação pode depender do uso pretendido da imagem - uma ação que muda a profundidade da imagem de uma forma que não é perceptível para olhos humanos pode ser satisfatória para fotografias do mundo real, mas não para imagens médicas, por exemplo. Um AIP contém estes componentes-chave: o objeto de dados primário a ser preservado, sua Informações de Representação de Apoio (formato e significado dos elementos do formato), e o várias categorias de Informações de Descrição de Preservação (PDI) que também precisam ser associadas ao objeto de dados primário: Fixidade, Proveniência, Contexto e

	Referência. Lá deve ser uma definição de como essas categorias de informação estão ligadas.
Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.2 O repositório deve ter uma descrição de como os AIPs são construídos a partir dos SIPs.
Texto de suporte	Isso é necessário para garantir que o(s) AIP (s) represente(m) adequadamente as informações no(s) SIP(s).
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentos de descrição do processo; documentação do relacionamento SIP-AIP; documentação clara de como os AIPs são derivados dos SIPs.
Discussão	Em alguns casos, os AIPs e os SIPs serão quase idênticos, além da embalagem e da localização, e o repositório só precisa dizer isso. Em outros casos, transformações complexas (por exemplo, normalização de dados) pode ser aplicada a objetos durante o processo de ingestão, e uma descrição precisa dessas ações podem ser necessárias para refletir como o(s) AIP(s) foi(foram) adequadamente transformado(s), a partir das informações no(s) SIP(s). A descrição da construção do AIP deve incluir documentação que dá uma descrição detalhada do processo de ingestão para cada transformação de SIP para AIP, consistindo tipicamente em uma visão geral do processamento sendo aplicado a todos como transformações, ampliadas com a descrição de diferentes classes de tal processamento e, quando aplicável, com as transformações especiais que se faziam necessárias. Alguns repositórios podem precisar produzir essas complexas descrições caso a caso. Sob tais circunstâncias devem ser criados diários de casos ou registros de ações tomadas para produzir cada AIP e mantidos. Nesses casos, a documentação deve ser mapeada para AIPs individuais, e o mapeamento deve estar disponível para exame. Outros repositórios que possam executar uma abordagem mais de linha de produção podem ter uma descrição de como cada classe de objetos recebidos é transformado para produzir a AIP. Deve ficar claro qual definição se aplica a qual AIP. Se, para tomar um simples exemplo, dois processos separados produzem cada um uma unidade de arquivo TIFF, deve estar claro que processo foi aplicado para produzir cada tipo determinado de arquivo TIFF.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.3 O repositório deve documentar a disposição final de todos os SIPs.
Texto de suporte	Em particular, o seguinte aspecto deve ser verificado.
Subcritério	4.2.3.1 O repositório deve seguir procedimentos documentados se um SIP não for incorporado a um AIP ou descartado e deve indicar por que o SIP não foi incorporado ou descartado.
Texto de suporte	Isso é necessário para garantir que os SIPs recebidos tenham sido tratados adequadamente e, em particular, não tenham sido perdidos acidentalmente.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Arquivos de processamento do sistema; registros de disposição; acordos de doadores ou depositantes / ações de doações; sistema de rastreamento de procedência; arquivos de log do sistema; documentos de descrição do processo; documentação do relacionamento do SIP com o AIP; documentação clara de como os AIPs são derivados dos SIPs; documentação do padrão / processo contra o qual a normalização ocorre; documentação do resultado da normalização e como o AIP resultante é diferente do (s) SIP.
Discussão	A escala de tempo desse processo varia entre repositórios de segundos há muitos meses, mas os SIPs não devem permanecer em um estado de limbo não processado para sempre. Os procedimentos de adesão e os logs internos de processamento e auditoria devem manter registros de todas as transformações internas dos SIPs para demonstrar que eles se tornam AIPs (ou parte dos AIPs) ou são descartados. Informações descritivas apropriadas também devem documentar a proveniência de todos os objetos digitais.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs.
Texto de suporte	Em particular, os seguintes aspectos devem ser verificados.
Subcritério	4.2.4.1 O repositório deve identificar exclusivamente cada AIP dentro do repositório.
Microcritério	4.2.4.1.1 O repositório deve ter identificadores únicos.
Microcritério	4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do AIP e seus componentes, de modo a serem únicos no contexto do repositório.
Microcritério	4.2.4.1.3 A documentação deve descrever qualquer processo usado para alterações em tais identificadores.
Microcritério	4.2.4.1.4 O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais de duplicação.
Microcritério	4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e previsíveis do repositório, como número de objetos.
Texto de suporte	Isso é necessário para garantir que cada AIP possa ser encontrado sem ambiguidade no futuro. Isso também é necessário para garantir que cada AIP possa ser diferenciado de todos os outros AIPs no repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação que descreve a convenção de nomenclatura e evidência física de sua aplicação (por exemplo, logs).
Discussão	Em branco

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Subcritério	4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs.
Microcritério	4.2.4.2 O repositório deve ter um sistema de serviços confiáveis de vinculação / resolução para encontrar o objeto identificado exclusivamente, independentemente de sua localização física.
Texto de suporte	Isso é necessário para que as ações relacionadas aos AIPs possam ser rastreadas ao longo do tempo, nas alterações do sistema e nas alterações de armazenamento.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação que descreve a convenção de nomenclatura e evidência física de sua aplicação (por exemplo, logs).
Discussão	Um repositório precisa garantir que exista uma convenção de nomenclatura padrão aceita que identifique seus materiais de forma exclusiva e persistente para uso dentro e fora do repositório. O requisito de 'visibilidade' aqui significa 'visível' para gerentes e auditores de repositório. Isso não implica que esses identificadores exclusivos precisem estar visíveis para os usuários finais ou que sirvam como o principal meio de acesso a objetos digitais. Idealmente, o ID exclusivo permanece enquanto o AIP; caso contrário, deve haver rastreabilidade. A subseção 4.2.1 exige que os componentes de um AIP sejam adequadamente vinculados e identificados para o gerenciamento no longo prazo, mas não impõe restrições sobre como os AIPs são identificados com os arquivos. Assim, no caso geral, um AIP pode ser distribuído por muitos arquivos ou um único arquivo pode conter mais de um AIP. Portanto, identificadores e nomes de arquivos podem não corresponder necessariamente um ao outro. A documentação deve representar esses relacionamentos.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.5 O repositório deve ter acesso às ferramentas e recursos necessários para fornecer informações de representação autorizadas para todos os objetos digitais que ele contém.
Texto de suporte	Em particular, os seguintes aspectos devem ser verificados.
Subcritério	4.2.5.1 O repositório deve ter ferramentas ou métodos para identificar o tipo de arquivo de todos os Objetos de Dados enviados.
Microcritério	4.2.5.2 O repositório deve ter ferramentas ou métodos para determinar quais informações de representação são necessárias para tornar cada objeto de dados compreensível para a comunidade designada.
Microcritério	4.2.5.3 O repositório deve ter acesso às informações de representação necessárias.
Microcritério	4.2.5.4 O repositório deve ter ferramentas ou métodos para garantir que as Informações de Representação necessárias sejam persistentemente associadas aos Objetos de Dados relevantes.
Texto de suporte	Isso é necessário para garantir que os objetos digitais do repositório sejam compreensíveis para a Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Assinatura ou acesso a registros de informações de representação (incluindo registros em formato); registros visíveis em registros locais (com links persistentes para objetos digitais); registros de banco de dados que incluem informações de representação e um link persistente para objetos digitais relevantes.
Discussão	Essas ferramentas e recursos podem ser mantidos internamente ou compartilhados por, por exemplo, um conjunto confiável de registros. No entanto, esse requisito não exige que cada repositório tenha essas ferramentas e recursos, apenas que ele tenha acesso a eles. Por exemplo, um repositório pode acessar registros externos. Qualquer registro desse tipo é um tipo especializado de repositório, que deve ser certificado / confiável. O repositório pode usar esses tipos de fontes de informações padronizadas e autorizadas para identificar e / ou verificar os componentes de Informações de Representação das Informações de Conteúdo e PDI. Isso reduzirá os custos de manutenção de longo prazo para o repositório e melhorará o controle de qualidade. Às vezes, existem informações gerais de representação (por exemplo, informações de formato) e informações específicas de representação (por exemplo, significados de campos individuais em um conjunto de dados). Geralmente, as informações gerais estarão disponíveis em um repositório externo, mas o repositório local pode precisar manter as informações específicas da instância. É provável que muitos repositórios desejem manter cópias locais das Informações de Representação relevantes; Contudo, isso pode não ser prático em todos os casos. Mesmo onde um repositório se esforça para manter todas essas informações localmente, pode haver, por exemplo, um agendamento de atualizações, o que significa que, até que uma atualização seja realizada, as Informações de Representação locais estão incompletas. Isso pode ser considerado como um tipo de armazenamento em *cache* local de, por exemplo, as informações de representação mantidas em registros. Como alternativa, pode-se dizer que, nesses casos, o uso de registros internacionais não visa substituir registros locais, mas serve como um recurso para verificar ou obter informações independentes e autorizadas sobre toda e qualquer informação de representação. A boa prática sugere que qualquer informação de representação realizada localmente também deve ser disponibilizada para outros repositórios por meio de um registro confiável.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.6 O repositório deve ter processos documentados para adquirir informações de descrição de preservação (PDI) para suas informações de conteúdo associadas e adquiri-las de acordo com os processos documentados.
Texto de suporte	Em particular, os seguintes aspectos devem ser verificados.
Subcritério	4.2.6.1 O repositório deve ter processos documentados para a aquisição da PDI.
Subcritério	4.2.6.2 O repositório deve executar seus processos documentados para adquirir a PDI.
Subcritério	4.2.6.3 O repositório deve garantir que o PDI esteja persistentemente associado às informações relevantes do conteúdo.
Texto de suporte	Isso é necessário para garantir que uma trilha auditável para apoiar reivindicações de autenticidade esteja disponível, que alterações não autorizadas nas explorações digitais possam ser detectadas e que os objetos digitais possam ser identificados e colocados em seu contexto apropriado.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Procedimentos operacionais padrão; manuais descrevendo procedimentos de ingestão; documentação visível sobre como o repositório adquire e gerencia Informações de Descrição de Preservação (PDI); criação de somas de verificação ou resumos, consultando a Comunidade Designada sobre o Contexto.
Discussão	O PDI é necessário não apenas pelo repositório para ajudar a garantir que as Informações do Conteúdo não sejam corrompidas (*Fixity*) e localizáveis (Informações de Referência), mas para ajudar a garantir que as Informações do Conteúdo sejam adequadamente compreensíveis, fornecendo uma perspectiva histórica (Informações de Proveniência) e fornecendo relacionamentos com outras informações (Informações de Contexto). A extensão dessas necessidades de informação é melhor atendida pelos membros da(s) Comunidade(s) Designada(s). O PDI deve estar permanentemente associado às informações de conteúdo.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.7 O repositório deve garantir que as Informações de Conteúdo dos AIPs sejam compreensíveis para sua Comunidade Designada no momento da criação do AIP.
Texto de suporte	Em particular, os seguintes aspectos devem ser verificados.
Subcritério	4.2.7.1 O repositório deve ter um processo documentado para testar a compreensibilidade de suas Comunidades Designadas das Informações de Conteúdo dos AIPs em sua criação.
Subcritério	4.2.7.2 O repositório deve executar o processo de teste para cada classe de informações de conteúdo dos AIPs.
Subcritério	4.2.7.3 O repositório deve levar as Informações de Conteúdo do AIP até o nível de compreensão exigido, se falhar no teste de compreensão.
Texto de suporte	Isso é necessário para garantir que um dos principais testes de preservação, a saber, que as explorações digitais sejam compreensíveis por sua Comunidade Designada, possa ser atendido. (Veja 4.3 para requisitos adicionais de compreensão além da ingestão.)
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Procedimentos de teste a serem executados em relação às *holdings* digitais para garantir sua compreensão para a Comunidade Designada definida; registros de tais testes sendo realizados e avaliados; evidência de coleta ou identificação de informações de representação para preencher quaisquer lacunas de inteligibilidade encontradas; retenção de indivíduos com os conhecimentos da disciplina.
Discussão	Este requisito está relacionado à compreensibilidade do AIP. Se o material ingerido não for compreensível, o repositório precisará ingerir ou disponibilizar informações adicionais garantir que os AIPs sejam compreensíveis para a(s) Comunidade(s) Designada(s). Por exemplo, se os documentos forem escritos em um idioma que está morrendo e a Comunidade Designada não puder mais entender o idioma em que os documentos foram escritos, o repositório precisará fornecer documentação adicional que permita à Comunidade Designada entender os documentos (por exemplo, traduções dos documentos em um idioma que a Comunidade Designada possa entender ou dicionários que permitam às Comunidades Designadas traduzir os documentos para um idioma que seus membros entendam).

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.8 O repositório deve verificar cada AIP quanto à integridade e correção no ponto em que é criado.
Texto de suporte	Isso é necessário para garantir que o que é mantido no longo prazo seja o que deveria ser e possa ser rastreado com as informações fornecidas pelos Produtores.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Descrição do procedimento que verifica a integridade e a correção dos AIPs; registros do procedimento.
Discussão	O repositório deve ter certeza de que os AIPs criados são os esperados, comparando-os com a definição associada para cada AIP ou classe de AIP e a descrição de como os AIPs são construídos a partir de SIPs . Se o repositório tiver um processo padrão para verificar se os SIPs estão completos e corretos e um processo comprovadamente correto para transformar SIPs em AIPs, basta demonstrar que as verificações iniciais foram realizadas com êxito e que o processo de transformação foi realizado sem indicação erros. Por outro lado, os repositórios que devem criar processos exclusivos para muitos de seus AIPs também precisarão gerar métodos exclusivos para validar a integridade e a correção dos AIPs. Isso pode incluir a execução de testes de algum tipo no conteúdo do AIP que podem ser comparados com testes no SIP. Esses testes podem ser simples (contando o número de registros em um arquivo ou executando alguma medida estatística simples), mas podem ser complexos. A documentação deve descrever como é garantida a integridade e a correção dos AIP, começando com o recebimento do produtor e continuando com a criação dos AIPs e apoiando a preservação no longo prazo. Exemplos de abordagens incluem o uso de somas de verificação, teste de que as somas de verificação ainda estão corretas em vários pontos durante a ingestão e preservação, *logs* de que essas verificações foram feitas e quaisquer testes especiais que possam ser necessários para uma instância ou classe AIP específica.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção / conteúdo do repositório.
Texto de suporte	Isso é necessário para permitir a auditoria da integridade da coleção como um todo.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação prevista em 4.2.1 a 4.2.4; acordos documentados negociados entre o produtor e o repositório (ver 4.1.1 - 4.1.8); registros do material recebido e datas de ação associada (recebimento, ação etc.); registros de verificações periódicas.
Discussão	É de responsabilidade do repositório escolher o mecanismo apropriado para verificar a integridade e a correção de suas coleções. Em geral, é provável que um repositório que atenda a todos os critérios anteriores satisfaça esse, sem precisar demonstrar mais nada. Como um requisito separado, demonstra a importância de poder auditar a integridade da coleção como um todo. Por exemplo, se um repositório afirma ter todos os emails enviados ou recebidos pela *The Yoyodyne Corporation* entre 1985 e 2005, é necessário mostrar que: - o conteúdo contido veio dos servidores de e-mail da *Yoyodyne*; - tudo é transformado corretamente em um formato de preservação; - cada SIP mensal de email foi preservado corretamente, incluindo identificadores exclusivos originais, como IDs de mensagem. No entanto, ainda pode não ter como mostrar se isso realmente representa todo o email de *Yoyodyne*. Por exemplo, se houver um período de três dias sem mensagens no repositório, é porque o *Yoyodyne* foi desligado por esses três dias ou porque o email foi perdido antes da construção do SIP? Esse caso pode ser resolvido pelo repositório que altera sua descrição da coleção, mas outros casos podem não ser tão simples. Um mecanismo familiar do mundo dos materiais tradicionais em bibliotecas e arquivos é um registro de acessos ou aquisições independente de outros metadados do catálogo. Um repositório deve poder mostrar, para cada item em seu registro de acessos, quais AIPs contêm conteúdo desse item. Como alternativa, pode ser necessário mostrar que não há AIP para um item, porque a ingestão ainda está em andamento, ou porque o item foi rejeitado por algum motivo. Por outro lado, qualquer AIP deve estar relacionado a uma entrada no registro de aquisições.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.2 Ingest: Criação do AIP
Critério	4.2.10 O repositório deve ter registros contemporâneos de ações e processos de administração relevantes para a criação do AIP.
Texto de suporte	Isso é necessário para garantir que não sejam omitidos do registro nada relevante que possa ser necessário para fornecer um meio independente de verificar se todos os AIPs foram criados corretamente de acordo com os procedimentos documentados (consulte 4.2.1 a 4.2.9) . É de responsabilidade do repositório justificar sua prática a esse respeito.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação escrita de decisões e / ou ações tomadas com *time stamps* (carimbos de horário); metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes.
Discussão	Esses registros devem ser criados na hora das ações a que se referem e estão relacionados às ações associadas à criação do AIP. Os registros podem ser automatizados ou podem ser gravados por indivíduos, dependendo da natureza das ações descritas. Onde padrões comunitários ou internacionais são usados, o repositório deve demonstrar que todas as ações relevantes são realizadas.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.3. Planejamento de preservação
Critério	4.3.1 O repositório deve ter estratégias de preservação documentadas relevantes para suas propriedades.
Texto de suporte	Isso é necessário para que fique claro como o repositório planeja garantir que as informações permaneçam disponíveis e utilizáveis para as gerações futuras e forneça um meio de verificar e validar o trabalho de preservação do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação que identifica cada risco de preservação identificado e a estratégia para lidar com esse risco.
Discussão	Essas estratégias de preservação documentadas descreverão como o repositório atuará sobre os riscos identificados, como parte do plano estratégico de preservação. Essas estratégias de preservação e o plano estratégico de preservação normalmente abordam a degradação da mídia de armazenamento, a obsolescência das unidades de mídia e a obsolescência ou inadequação das Informações de Representação (incluindo formatos) à medida que a base de conhecimento da Comunidade Designada é alterada e protege contra acidentes acidentais ou intencionais de corrupção digital. Por exemplo, se a migração é a abordagem escolhida para alguns desses problemas, também é necessário que haja políticas de preservação sobre o que desencadeia uma migração e que tipos de migração devem resolver o risco de preservação identificado. A estratégia de preservação descreverá a gama de atividades que precisam ser realizadas em caso de migração.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.3. Planejamento de preservação
Critério	4.3.2 O repositório deve ter mecanismos para monitorar seu ambiente de preservação.
Texto de suporte	Isso é necessário para que o repositório possa reagir às alterações e, assim, garantir que as informações preservadas permaneçam compreensíveis e utilizáveis pela Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Pesquisas da Comunidade Designada do repositório.
Discussão	O repositório deve mostrar que possui algum mecanismo ativo para garantir que as informações permanecem compreensíveis e utilizáveis pela Comunidade Designada e que possuem mecanismos de monitoramento e notificação quando a Informação de Representação (incluindo formatos) aproxima-se da obsolescência ou não é mais viável. Para a maioria dos repositórios, a preocupação será com as Informações de Representação utilizadas para preservar a informação, que podem incluir informações sobre como lidar com um formato de arquivo ou software que pode ser usado para compilá-lo ou processá-lo. Às vezes, o formato precisa mudar, porque o repositório não pode mais lidar com aquele formato. Algumas vezes, o formato é mantido e as informações sobre o software que é necessário para processá-lo precisam mudar. Se o mecanismo depende de um mecanismo externo o repositório deve demonstrar como ele utiliza as informações desse registro.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.3. Planejamento de preservação
Critério	4.3.2 O repositório deve ter mecanismos para monitorar seu ambiente de preservação.
Subcritério	4.3.2.1 O repositório deve ter mecanismos para monitoramento e notificação quando as Informações de Representação forem inadequadas para a Comunidade Designada entender os dados armazenados.
Texto de suporte	Isso é necessário para garantir que as informações preservadas permaneçam compreensíveis e utilizáveis pela Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Assinatura de um serviço de registro de Informações de Representação; assinatura de um serviço de vigilância tecnológica, pesquisas entre seus membros da Comunidade Designada, processos de trabalho relevantes para lidar com essas informações.
Discussão	O repositório deve mostrar que possui algum mecanismo ativo para alertar sobre a obsolescência iminente. A obsolescência é determinada em grande parte em termos da base de conhecimento da Comunidade Designada.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.3. Planejamento de preservação
Critério	4.3.3 O repositório deve ter mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.
Texto de suporte	Isso é necessário para que o repositório esteja preparado para mudanças no ambiente externo que possam tornar seus planos de preservação atuais uma péssima escolha, já que o tempo para implementar se aproxima.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Planos de preservação vinculados a observação formal ou informal de tecnologia; planejamento ou processos de preservação programados para intervalos mais curtos (por exemplo, não mais que cinco anos); prova de atualizações frequentes das políticas de preservação e dos planos de preservação; seções das Políticas de Preservação que abordam como os planos podem ser atualizados e com que frequência os planos precisam ser revisados e reafirmados ou atualizados.
Discussão	O repositório deve demonstrar ou descrever como reage às informações do monitoramento, o que às vezes exige que o repositório altere a forma como lida com o material que contém de maneiras que não poderiam ter sido antecipadas em um estágio anterior. O repositório deve revisar periodicamente seus planos de preservação e o ambiente de tecnologia e, se necessário, fazer alterações nesses planos para garantir sua eficácia contínua. Outra resposta possível às informações coletadas pelo monitoramento é que o repositório atualize e crie Informações de Representação e / ou PDI adicionais.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.3. Planejamento de preservação
Critério	4.3.3 O repositório deve ter mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.
Subcritério	4.3.3.1 O repositório deve ter mecanismos para criar, identificar ou coletar qualquer Informação de Representação extra necessária.
Texto de suporte	Isso é necessário para garantir que as informações preservadas permaneçam compreensíveis e utilizáveis pela Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Assinatura de um serviço de registro de formato; assinatura de um serviço de vigilância tecnológica; planos de preservação.
Discussão	O repositório deve ter mecanismos para monitoramento e notificação quando as Informações de Representação (incluindo formatos) se aproximam da obsolescência ou não são mais viáveis, e deve poder mostrar que possui mecanismos para lidar com essas notificações.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.3. Planejamento de preservação
Critério	4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.
Texto de suporte	Isso é necessário para garantir à Comunidade Designada que o repositório poderá disponibilizar as informações e utilizá-las a médio e longo prazo.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Coleta de metadados de preservação apropriados; prova de usabilidade de objetos digitais selecionados aleatoriamente mantidos no sistema; histórico demonstrável para reter objetos digitais utilizáveis ao longo do tempo; Pesquisas comunitárias designadas.
Discussão	O repositório deve ser capaz de demonstrar a preservação continuada, incluindo a compreensibilidade, de suas propriedades. Isso pode ser avaliado em vários graus e depende da especificidade da comunidade designada. Se uma comunidade designada for bastante ampla, um auditor poderá representar o sujeito do teste na avaliação. Comunidades Designadas mais específicas podem exigir esforços significativos.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.4. Preservação AIP
Critério	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit*.
Texto de suporte	Isso é necessário para garantir que as informações possam ser extraídas do AIP no longo prazo.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação do formato dos AIPs; Descrições do EAST e da linguagem de especificação do dicionário de entidades de dados (DEDSL) dos componentes de dados.
Discussão	O repositório deve especificar as informações de representação até o nível de bit de cada componente AIP e deve especificar como os componentes separados são empacotados juntos. As informações de representação devem estar disponíveis para cada AIP e devem estar adequadamente vinculadas ao AIP. Frequentemente, os repositórios são tentados a descrever o conteúdo do AIP apenas em um nível em que um programa será usado para converter as informações em um formato compreensível para as Comunidades Designadas. No entanto, se esses programas falharem em operar, as informações serão perdidas em todos os AIPs que dependem desse programa.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.4. Preservação AIP
Critério	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit.*
Subcritério	4.4.1.1 O repositório deve preservar as informações de conteúdo dos AIPs.
Texto de suporte	Isso é necessário porque é a missão fundamental de um repositório preservar as informações de conteúdo para suas comunidades designadas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação do procedimento de fluxo de trabalho de preservação; documentação de procedimentos de fluxo de trabalho; Documentos da Política de Preservação que especificam o tratamento dos AIPs e em que circunstâncias eles podem ser excluídos; capacidade de demonstrar a sequência de conversões para um AIP para qualquer objeto digital específico ou grupo de objetos ingeridos; documentação que vincula objetos ingeridos e os AIPs atuais.
Discussão	O repositório deve ser capaz de demonstrar que os AIPs refletem fielmente as informações capturadas durante a ingestão e que quaisquer transformações planejadas subsequentes ou futuras continuarão preservando todas as Propriedades de Informação necessárias das Informações de Conteúdo. Uma abordagem para esse requisito pressupõe que o repositório tenha uma política especificando que os AIPs não podem ser excluídos a qualquer momento. Essa implementação particularmente simples e robusta preserva os *links* entre o que foi originalmente ingerido, bem como as novas versões que foram transformadas ou alteradas de alguma forma. Dependendo da implementação, esses objetos mais recentes podem ser AIPs completamente novos ou meramente AIPs atualizados. De qualquer maneira, os *links* persistentes entre o objeto ingerido e o AIP resultante devem ser mantidos.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.4. Preservação AIP
Critério	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit.*
Subcritério	4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs.
Texto de suporte	Isso é necessário para proteger a integridade dos objetos de arquivamento ao longo do tempo.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Informações de fixação (por exemplo, somas de verificação) para cada objeto digital / AIP ingerido; registros de verificações de fixação; documentação de como as informações de AIPs e Fixity são mantidas separadas; documentação de como os AIPs e os registros de adesão são mantidos separados.
Discussão	Um repositório deve ter *logs* que mostrem ações executadas para verificar a integridade dos objetos de arquivamento, a fim de garantir financiadores, produtores e usuários - e permitir que eles auditem / validem - que o repositório está tomando as medidas necessárias para garantir o longo prazo integridade dos objetos digitais. O repositório também deve documentar que as verificações de integridade são realizadas regularmente, a fim de detectar quaisquer alterações nos AIPs o mais rápido possível, para que as ações corretivas possam ser executadas o mais rápido possível. O repositório deve permitir que as partes interessadas verifiquem se esse é o caso. Atualmente, a maioria dos repositórios lida com isso no nível de objetos de informações individuais, usando uma soma de verificação de alguma forma, como *MD5*. Nesse caso, o repositório deve poder e pode querer demonstrar que as informações de *Fixity* (somas de verificação e as informações que as vinculam aos AIPs) são armazenadas separadamente ou protegidas separadamente dos próprios AIPs, para que alterações acidentais do AIP também não danificaria as informações de fixação. Além disso, alguém que possa alterar maliciosamente um AIP, provavelmente, não poderá alterar tão facilmente as informações de fixidez.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.4. Preservação AIP
Critério	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit.*
Subcritério	4.4.2 O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIPs.
Texto de suporte	Isso é necessário para garantir que a documentação não seja omitida, incorreta ou com autenticidade questionável.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação escrita das decisões e / ou medidas tomadas; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes.
Discussão	Os registros podem ser automatizados ou podem ser gravados por indivíduos, dependendo da natureza das ações descritas. Onde padrões comunitários ou internacionais são usados, o repositório deve demonstrar que todas as ações

	relevantes são executadas adequadamente.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.4. Preservação AIP
Critério	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit.*
Subcritério	4.4.2.1 O repositório deve ter procedimentos para todas as ações executadas nos AIPs.
Texto de suporte	Isso é necessário para garantir que quaisquer ações executadas contra um AIP não alterem as informações do AIP de maneira inaceitável para suas Comunidades Designadas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação escrita que descreve todas as ações que podem ser executadas em relação a um AIP.
Discussão	Esta documentação é normalmente criada durante o design do repositório. Ele deve detalhar o manuseio normal dos AIPs, todas as ações que podem ser executadas nos AIPs, incluindo condições de sucesso e falha e detalhes de como esses processos podem ser monitorados.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.4. Preservação AIP
Critério	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit.*
Subcritério	4.4.2.2 O repositório deve ser capaz de demonstrar que quaisquer ações tomadas nos AIPs eram compatíveis com a especificação dessas ações.
Texto de suporte	Isso é necessário para garantir que quaisquer ações executadas contra um AIP não alterem as informações do AIP de maneira inaceitável para suas Comunidades Designadas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes e documentação dessa ação; auditorias processuais do repositório, mostrando que todas as ações estão em conformidade com os processos documentados.
Discussão	A preservação bem-sucedida de informações no arquivo está fortemente ligada a seguir os procedimentos estabelecidos e documentados para concluir todas as ações que afetam os dados do repositório. Quanto mais frequentemente o 'tratamento especial' dos dados do repositório ocorre e mais frequentemente esse 'tratamento especial' não é supervisionado de maneira consistente, mais provável é que os dados mantidos pelo repositório sejam comprometidos. Quando os procedimentos são seguidos, regularmente, qualquer desvio dos procedimentos que provavelmente causariam uma alteração nos dados será mais provável de ser percebido ou, se não for percebido, poderá ser mais provável de ser corrigido, ou o tempo e a provável alteração poderão ser identificados no futuro.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.5 Gestão da Informação
Critério	4.5.1 O repositório deve especificar requisitos mínimos de informação para permitir que a Comunidade Designada descubra e identifique material de interesse.
Texto de suporte	Isso é necessário para permitir a descoberta das propriedades do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Informações descritivas e de recuperação, metadados de descoberta, como Dublin Core, e outras documentações que descrevem o objeto.
Discussão	O repositório deve ser capaz de lidar com os tipos de solicitações que serão provenientes de um usuário típico da Comunidade Designada. Um repositório não precisa necessariamente satisfazer todas as solicitações possíveis. Os metadados de recuperação são diferentes das informações descritivas que descrevem o que foi encontrado.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.5 Gestão da Informação
Critério	4.5.2 O repositório deve capturar ou criar informações descritivas mínimas e garantir que elas estejam associadas ao AIP.
Texto de suporte	Isso é necessário para garantir que as informações descritivas estejam associadas ao AIP.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Metadados descritivos; identificador único ou localizador persistente interno ou externo associado ao AIP (consulte também 4.2.4 sobre identificador exclusivo persistente); documentação do sistema e arquitetura técnica; acordos de depositantes; documentação da política de metadados, incorporando detalhes dos requisitos de metadados e uma declaração descrevendo onde a responsabilidade por sua aquisição se enquadra; documentação do fluxo de trabalho do processo.
Discussão	O repositório deve mostrar que está associado a cada AIP, informações descritivas mínimas que foram recebidas do produtor ou criadas pelo repositório. A associação das informações descritivas com o objeto é importante, embora não exija correspondência individual e possa não ser necessariamente armazenada no AIP. Esquemas hierárquicos de descrição podem permitir que alguns elementos descritivos sejam associados a muitos itens.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.5 Gestão da Informação
Critério	4.5.3 O repositório deve manter uma ligação bidirecional entre cada AIP e suas informações descritivas.
Texto de suporte	Isso é necessário para garantir que todos os AIPs possam ser localizados e recuperados.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Metadados descritivos; identificador ou localizador exclusivo e persistente associado ao AIP; relacionamento documentado entre o AIP e seus metadados; documentação do sistema e arquitetura técnica; documentação do fluxo de trabalho do processo.
Discussão	Os repositórios devem implementar procedimentos para estabelecer e manter relacionamentos para associar informações descritivas para cada AIP, e devem garantir que cada AIP tenha alguma informação descritiva associada a ele e que todas as informações descritivas devem apontar para pelo menos um AIP.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.5 Gestão da Informação
Critério	4.5.3 O repositório deve manter uma ligação bidirecional entre cada AIP e suas informações descritivas.
Subcritério	4.5.3.1 O repositório deve manter as associações entre seus AIPs e suas informações descritivas ao longo do tempo.
Texto de suporte	Isso é necessário para garantir que todos os AIPs possam continuar sendo localizados e recuperados.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Registro detalhando a manutenção contínua ou a verificação da integridade dos dados e seus relacionamentos com as informações descritivas associadas, especialmente após reparo ou modificação do AIP; informações descritivas legadas; persistência do identificador ou localizador; relacionamento documentado entre o AIP e suas informações descritivas; documentação do sistema e arquitetura técnica; documentação do fluxo de trabalho do processo.
Discussão	Os repositórios devem implementar procedimentos que permitam saber quando o relacionamento entre os dados e as informações descritivas associadas é temporariamente interrompido para garantir que eles possam ser restaurados.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.6 Gestão de Acesso
Texto de suporte	O termo 'acesso' possui vários sentidos diferentes, incluindo o acesso dos usuários ao sistema do repositório, por exemplo, segurança física e autenticação do usuário e os diferentes estágios de acesso aos registros (fazendo uma solicitação, verificando os direitos do solicitante e preparar e enviar um Pacote de Informações de Divulgação [DIP]). Esta subseção está relacionada a tudo isso. Ele é dividido em dois requisitos principais, um relacionado à existência e implementação de políticas de acesso e outro com a capacidade do repositório de fornecer objetos comprovadamente autênticos como DIPs. Assim, o primeiro requisito refere-se a solicitações iniciadas por um usuário e como o repositório lida com eles para garantir que os direitos e acordos sejam respeitados, que a segurança seja monitorada, que os pedidos sejam atendidos etc. O segundo requisito refere-se ao que é entregue ao consumidor e a confiança que pode ser depositada nele. Deve-se entender que os recursos e a sofisticação do sistema de acesso variam dependendo da Comunidade Designada do repositório e dos mandatos de acesso do repositório. Devido à variedade de repositórios e mandatos de acesso, esses critérios podem estar sujeitos a perguntas sobre aplicabilidade e interpretação em nível local.
Critério	4.6.1 O repositório deve estar em conformidade com as Políticas de Acesso.
Texto de suporte	Isso é necessário para garantir que o repositório atenda totalmente a todos os aspectos de uso que possam afetar a confiabilidade do repositório, principalmente com referência ao suporte da comunidade de usuários.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito Declarações de políticas disponíveis para as comunidades de usuários; informações sobre recursos do usuário (matrizes de autenticação); *logs* e trilhas de auditoria de solicitações de acesso; testes explícitos de alguns tipos de acesso.
Discussão	Dependendo da natureza do repositório, as Políticas de Acesso podem abranger: - declarações do que é acessível a qual comunidade e em que condições; - requisitos para autenticação e autorização de acessadores; - execução de acordos aplicáveis às condições de acesso; - gravação de ações de acesso. O acesso pode ser gerenciado em parte por computadores e em parte por humanos; a verificação de passaportes, por exemplo, antes de emitir um *ID* de usuário e senha pode ser uma parte apropriada do gerenciamento de acesso para algumas instituições.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.6 Gestão de Acesso
Critério	4.6.1 O repositório deve estar em conformidade com as Políticas de Acesso.
Subcritério	4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias no gerenciamento de acesso.
Texto de suporte	Isso é necessário para identificar ameaças à segurança e falhas no sistema de gerenciamento de acesso.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Registros de acesso, capacidade do sistema de usar ferramentas automatizadas de análise / monitoramento e gerar mensagens de problema / erro; notas de revisões realizadas ou medidas tomadas como resultado de revisões.
Discussão	Um repositório deve ter algum mecanismo automatizado para observar negações anômalas ou incomuns e usá-las para identificar ameaças ou falhas de segurança no sistema de gerenciamento de acesso, como acesso negado a usuários válidos. Isso não significa examinar todos os acessos negados.

Seção	4 Gerenciamento Digital de Objetos
Categoria	4.6 Gestão de Acesso
Critério	4.6.2 O repositório deve seguir políticas e procedimentos que permitam a disseminação de objetos digitais rastreáveis aos originais, com evidências que comprovem sua autenticidade.
Texto de suporte	Isso é necessário para estabelecer uma cadeia auditável de autenticidade do AIP para objetos digitais disseminados.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentos de projeto do sistema; instruções de trabalho (se os DIPs envolverem processamento manual); orientações passo a passo do processo; produção de uma cópia de amostra com evidência de autenticidade; documentação dos requisitos da comunidade para evidências de autenticidade.
Discussão	Autenticidade não é um conceito de "tudo ou nada", mas é uma questão de grau, julgada com base em evidências. Assim, a adequação das evidências é de importância fundamental na avaliação desse requisito. Esse requisito garante que as ações de ingestão, preservação e transformação não percam informações que suportariam uma trilha auditável de autenticidade entre o objeto depositado original e o objeto disseminado eventual. Um repositório deve registrar os processos para construir os DIPs a partir dos AIPs relevantes. Esta é uma parte essencial para estabelecer que os DIPs refletem o conteúdo dos AIPs e, portanto, do material original, de maneira confiável e consistente. Os DIPs podem ser simplesmente uma cópia dos AIPs ou podem resultam de uma transformação de formato simples de um AIP. Mas em outros casos, eles podem ser derivados de maneiras complexas. Um usuário pode solicitar um DIP que consiste nas páginas de título de todos os livros eletrônicos publicados em um determinado período, por exemplo, o que exigirá que estes sejam extraídos de muitos AIPs diferentes. Ou um repositório pode disseminar transcrições geradas automaticamente de gravações de voz. Um repositório que permita solicitações para DIPs tão complexos precisará se esforçar mais para demonstrar como atende a esse requisito do que um repositório que permita apenas solicitações de DIPs que correspondam a um AIP inteiro. Este requisito refere-se apenas à relação entre os

	DIPs e os AIPs dos quais eles derivam; em outro lugar, o link entre os SIPs originais e os AIPs é considerado.
Seção	4 Gerenciamento Digital de Objetos
Categoria	4.6 Gestão de Acesso
Critério	4.6.2 O repositório deve seguir políticas e procedimentos que permitam a disseminação de objetos digitais rastreáveis aos originais, com evidências que comprovem sua autenticidade.
Subcritério	4.6.2.1 O repositório deve registrar e agir de acordo com os relatórios de problemas sobre erros nos dados ou respostas dos usuários.
Texto de suporte	Isso é necessário para que os usuários considerem o repositório uma fonte confiável de informações.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentos de projeto do sistema; instruções de trabalho (se os DIPs envolverem processamento manual); orientações passo a passo do processo; registros de pedidos e produção DIP; documentação dos relatórios de erros e as ações tomadas.
Discussão	O objetivo do gerenciamento de acesso é garantir que um usuário receba uma versão utilizável e correta do(s) objeto(s) digital(is), (ou seja, DIP) que ele solicitou. Um repositório deve mostrar que quaisquer problemas que ocorrem e são trazidos à sua atenção são investigados e resolvidos. Essa capacidade de resposta é essencial para que o repositório seja considerado confiável.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Texto de suporte	Isso é necessário para garantir uma infraestrutura segura e confiável.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Inventário de infraestrutura de componentes do sistema; avaliações periódicas de tecnologia; estimativas da vida útil dos componentes do sistema; exportação de registros autênticos para um sistema independente; uso de software fortemente suportado pela comunidade, como Apache, iRODS, Fedora); recriação de arquivos a partir de backups.
Discussão	O repositório deve conduzir ou contratar avaliações dos riscos relacionados à infraestrutura de hardware e software e procedimentos operacionais. O repositório deve fornecer mecanismos que minimizem o risco de dependências na infraestrutura do sistema proprietária ou obsoleta e de erro operacional. O grau de suporte necessário refere-se à criticidade do(s) subsistema(s) envolvido(s) na preservação no longo prazo. O repositório deve manter um sistema escalável (por exemplo, capaz de lidar com volumes futuros previstos de bytes e arquivos) sem uma grande interrupção do sistema. O repositório deve manter um sistema que seja evoluído. Ou seja, o sistema deve ser projetado de tal maneira que os principais componentes do sistema possam ser substituídos por tecnologias mais recentes sem grandes interrupções no sistema como um todo. O sistema de repositório deve ser extensível. Ou seja, o sistema deve ser projetado para acomodar formatos futuros (mídia e arquivos) sem grandes interrupções no sistema como um todo. O repositório deve poder exportar suas participações para um custodiante futuro. O

	repositório deve poder recriar os arquivos após um erro operacional que substitui ou exclui os acervos digitais.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Texto de suporte	Isso é necessário para rastrear quando os componentes de hardware ou software ficarão obsoletos e a migração é necessária para a nova infraestrutura.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Gerenciamento de relatórios periódicos de avaliação de tecnologia. Comparação da tecnologia existente com cada nova avaliação.
Discussão	O objetivo é entender quando qualquer subsistema representa um risco de obsolescência e permitir o planejamento da migração para novas tecnologias antes que os mecanismos de interoperabilidade não estejam mais disponíveis. Isso pode ser causado por dependências de software proprietário (o fornecedor não oferece mais suporte ao componente do subsistema) e pelo surgimento de novos protocolos (o mecanismo para acessar o sistema tornou-se obsoleto e não é mais suportado).

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.1 O repositório deve ter tecnologias de hardware adequadas aos serviços que fornece às comunidades designadas.
Texto de suporte	Isso é necessário para fornecer níveis esperados, contratados, seguros e persistentes de serviço, incluindo: facilidade de ingestão e disseminação por meio de depositantes e interfaces de usuário e tecnologias apropriadas, como mecanismos de *upload*; gerenciamento contínuo de objetos digitais; abordagens e soluções de preservação, como migração; e segurança do sistema
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Manutenção de tecnologia comunitária designada, expectativas e perfis de uso atualizados; fornecimento de largura de banda adequada para suportar demandas de ingestão e uso; obtenção sistemática de feedback sobre adequação de hardware e serviço; manutenção de um inventário de hardware atual.
Discussão	O repositório deve estar ciente dos tipos de serviços de armazenamento, gerenciamento de arquivos, preservação e acesso esperados por sua Comunidade Designada, incluindo onde aplicável, os tipos de mídia a serem entregues e precisa garantir que seus recursos de hardware possam suportar esses serviços. O objetivo é rastrear quando as mudanças nos requisitos de serviço das comunidades

	designadas exigem uma mudança correspondente na tecnologia de hardware, quando as mudanças nas políticas de ingestão exigem recursos expandidos e quando as mudanças nas políticas de preservação exigem novos recursos de preservação. Isso pode ser causado por mudanças nos requisitos de capacidade (o tempo necessário para ler toda a mídia é maior que a vida útil da mídia), por mudanças nos mecanismos de entrega (novos clientes para exibir registros autênticos) e por mudanças no número e tamanho dos registros arquivados.
Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.2 O repositório deve ter procedimentos para monitorar e receber notificações quando forem necessárias alterações na tecnologia de hardware.
Texto de suporte	Isso é necessário para garantir níveis esperados, contratados, seguros e persistentes de serviço.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Auditorias de capacidade versus uso real; auditorias das taxas de erro observadas; auditorias de gargalos de desempenho que limitam a capacidade de atender aos requisitos de acesso à comunidade de usuários; documentação de avaliações de vigilância tecnológica; documentação de atualizações de tecnologia de fornecedores.
Discussão	O repositório deve realizar ou contratar varreduras ambientais frequentes em relação ao hardware status, fontes de falha e interoperabilidade entre os componentes de hardware. O repositório também deve estar em contato com seus fornecedores de hardware em relação à atualização tecnológica, pontos de provável falha, e como novos componentes podem afetar a integração e o desempenho do sistema. O objetivo é rastrear quando há mudanças nas necessidades de serviço das comunidades designadas requerem uma mudança correspondente na tecnologia de hardware, quando há mudanças na ingestão políticas exigem capacidades ampliadas, e quando mudanças nas políticas de preservação exigem novas capacidades de preservação. Isto pode ser impulsionado por mudanças nas necessidades de capacidade (o tempo necessário para ler todas as mídias é maior que a vida útil da mídia), por mudanças na entrega (novos clientes para exibição de registros autênticos), e alterações no número e tamanho dos registros arquivados.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.3 O repositório deve ter procedimentos para avaliar quando são necessárias alterações no hardware atual.
Texto de suporte	Isso é necessário para garantir que o repositório tenha a capacidade de tomar decisões informadas e oportunas quando as informações indicarem a necessidade de novo hardware.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Procedimentos de avaliação em vigor; experiência documentada da equipe em cada subsistema de tecnologia.
Discussão	Dadas as informações de vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia, o repositório deve ter procedimentos e conhecimentos para avaliar esses dados e tomar boas decisões com relação à necessidade de novo hardware. O objetivo é rastrear quando os provedores de tecnologia desenvolveram subsistemas que minimizam riscos, minimizam custos ou melhoram o desempenho. Isso é necessário para rastrear tecnologias emergentes e planejar atualizações antes que os limites de capacidade ocorram. A avaliação deve identificar quando o risco de usar a nova tecnologia supera o benefício esperado e quando a nova tecnologia está suficientemente madura para minimizar o risco.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.4 O repositório deve ter procedimentos, comprometimento e financiamento para substituir o hardware quando a avaliação indicar a necessidade de fazê-lo.
Texto de suporte	Isso é necessário para garantir a substituição do hardware em tempo hábil, a fim de evitar falhas no sistema ou inadequação de desempenho. Sem esse compromisso e, o que é mais importante, sem recursos financeiros comprometidos ou um fluxo de financiamento seguro, as vigilâncias e notificações de tecnologia são de pouco valor. O repositório deve ter mecanismos para avaliar a eficácia dos novos sistemas antes da implementação no sistema de produção.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Declaração de compromisso em fornecer os níveis de serviço esperados e contratados; evidência de ativos financeiros em andamento reservados para compras de hardware; demonstração de economia de custos através do custo amortizado do novo sistema.
Discussão	O objetivo é demonstrar que o repositório tem a capacidade de incorporar novas tecnologias, tanto financeiramente através de compromissos de financiamento ou redução de custos, quanto operacionalmente por meio da verificação das

	capacidades dos novos sistemas.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.5 O repositório deve ter tecnologias de software apropriadas aos serviços que fornece às comunidades designadas.
Texto de suporte	Isso é necessário para fornecer níveis esperados, contratados, seguros e persistentes de serviço, incluindo: facilidade de ingestão e disseminação por meio de depositantes e interfaces de usuário e tecnologias apropriadas, como mecanismos de *upload*; gerenciamento contínuo de objetos digitais; abordagens e soluções de preservação, como migração; e segurança do sistema.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Manutenção de tecnologia comunitária designada, expectativas e perfis de uso atualizados; fornecimento de sistemas de software adequados para suportar demandas de ingestão e uso; obtenção sistemática de *feedback* sobre adequação de software e serviço; manutenção de um inventário de software atual.
Discussão	O objetivo é rastrear quando alterações nos requisitos de serviço das comunidades designadas exigem uma alteração correspondente nos componentes de software, quando alterações nas políticas de ingestão exigem suporte para novos formatos de dados e quando alterações na tecnologia de software exigem novos recursos de migração de formatos. Isso pode ser causado por mudanças nos requisitos de acesso (novos clientes que exigem novos formatos de dados se tornam preferidos), por alterações nos mecanismos de entrega (novos mecanismos de transferência de dados) e alterações no número e no tamanho dos registros arquivados que requerem software mais escalável.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.6 O repositório deve ter procedimentos para monitorar e receber notificações quando forem necessárias alterações de software.
Texto de suporte	Isso é necessário para garantir níveis esperados, contratados, seguros e persistentes de serviço.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Auditorias de capacidade versus uso real; auditorias das taxas de erro observadas; auditorias de gargalos de desempenho que limitam a capacidade de atender aos requisitos de acesso à comunidade de usuários; documentação de avaliações de vigilância tecnológica; documentação de atualizações de software de fornecedores.
Discussão	O objetivo é rastrear quando as mudanças nos requisitos de serviço das comunidades designadas exigem uma mudança correspondente na tecnologia de software, quando as mudanças nas políticas de ingestão exigem recursos expandidos e quando as mudanças nas políticas de preservação exigem novos recursos de preservação. Isso pode ser causado por atualizações de segurança (correções fornecidas pelo fornecedor a vulnerabilidades recém-identificadas), por alterações nos mecanismos de entrega (novos clientes de software para exibição de registros autênticos) e por alterações no número e tamanho dos registros arquivados (requisitos expandidos do banco de dados). O repositório deve realizar ou contratar varreduras ambientais frequentes relacionadas à evolução do software, pontos prováveis de falha e interoperabilidade entre os componentes de software e hardware.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.7 O repositório deve ter procedimentos para avaliar quando são necessárias alterações no software atual.
Texto de suporte	Isso é necessário para garantir que o repositório tenha a capacidade de tomar decisões informadas e oportunas quando as informações indicarem a necessidade de novo software.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Procedimentos de avaliação em vigor; conhecimento especializado da equipe em cada subsistema de tecnologia de software.
Discussão	Dadas as informações de vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia, o repositório deve ter procedimentos e conhecimentos para avaliar esses dados e tomar boas decisões com relação à necessidade de novo software. O objetivo é rastrear quando os provedores de tecnologia desenvolveram uma infraestrutura de software que minimiza riscos, minimiza custos ou melhora o desempenho. Isso é necessário para rastrear tecnologias emergentes e planejar atualizações antes que os limites de capacidade ocorram. A avaliação deve identificar quando o risco de usar a nova tecnologia supera o benefício esperado e quando a nova tecnologia está suficientemente madura para minimizar o risco.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.1.8 O repositório deve ter procedimentos, comprometimento e financiamento para substituir o software quando a avaliação indicar a necessidade de fazê-lo.
Texto de suporte	Isso é necessário para garantir a substituição do software em tempo hábil, a fim de evitar falhas no sistema ou inadequação de desempenho. Sem esse compromisso e, o que é mais importante, sem recursos financeiros comprometidos ou um fluxo de financiamento seguro, as vigilâncias e notificações de tecnologia são de pouco valor. O repositório deve ter mecanismos para avaliar a eficácia dos novos sistemas antes da implementação no sistema de produção.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Declaração de compromisso em fornecer os níveis de serviço esperados e contratados; evidência de ativos financeiros em andamento reservados para compras de software; demonstração de economia de custos através do custo amortizado do novo sistema.
Discussão	O objetivo é demonstrar que o repositório tem a capacidade de incorporar novas tecnologias, tanto financeiramente através de compromissos de financiamento ou redução de custos, quanto operacionalmente através da verificação das capacidades dos novos sistemas.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.2 O repositório deve ter suporte de hardware e software adequado para a funcionalidade de backup suficiente para preservar o conteúdo do repositório e rastrear as funções do repositório.
Texto de suporte	Isso é necessário para garantir o acesso contínuo e o rastreamento das funções de preservação aplicadas aos objetos digitais sob sua custódia.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação do que está sendo feito backup e com que frequência; *log* de auditoria / inventário de backups; validação de backups concluídos; plano, política e documentação de recuperação de desastres; exercícios contra incêndio; teste de backups; contratos de suporte para hardware e software para mecanismos de backup; preservação demonstrada dos metadados do sistema, como controles de acesso, localização de réplicas, trilhas de auditoria, valores de soma de verificação.
Discussão	O repositório deve ser capaz de demonstrar a adequação dos processos, hardware e software para seus sistemas de backup e toda a gama de funções de ingestão, preservação e disseminação necessárias para um repositório encarregado da preservação no longo prazo. Mecanismos de backup simples devem preservar não apenas o conteúdo principal do repositório, mas também os metadados do sistema gerados pelas funções de preservação. Os repositórios precisam desenvolver planos de backup que garantam a continuidade das operações em todos os modos de falha.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.3 O repositório deve ter mecanismos eficazes para detectar corrupção ou perda de bits.
Texto de suporte	Isso é necessário para garantir que os AIPs e os metadados não sejam corrompidos ou que quaisquer perdas de dados sejam detectadas e caiam dentro das tolerâncias estabelecidas pela política de repositório (consulte 3.3.5).
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentos que especificam os mecanismos de detecção e correção de erros de bits usados; análise de risco; relatórios de erro; análise de ameaças; análise periódica da integridade das reservas de repositório.
Discussão	O objetivo é um tratamento abrangente das fontes de perda de dados e de sua complexidade no mundo real. Quaisquer dados ou metadados perdidos (temporariamente) devem ser recuperáveis a partir de backups. Falhas sistemáticas de rotina não devem acumular e causar perda de dados além das tolerâncias estabelecidas pelas políticas do repositório. Mecanismos como somas de verificação (assinaturas MD5) ou assinaturas digitais devem ser reconhecidos por sua eficácia na detecção de perda de bits e incorporados à abordagem geral do repositório para validar a integridade.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.3.1 O repositório deve registrar e relatar à sua administração todos os incidentes de corrupção ou perda de dados e devem ser tomadas medidas para reparar / substituir dados corrompidos ou perdidos.
Texto de suporte	Isso é necessário para garantir que a administração do repositório seja mantida informada sobre incidentes e ações de recuperação e para permitir a identificação de fontes de corrupção ou perda de dados.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Procedimentos relacionados ao relato de incidentes aos administradores; registros de metadados de preservação (por exemplo, PDI); comparação de *logs* de erros com relatórios para administração; procedimentos de encaminhamento relacionados à perda de dados; rastreamento de fontes de incidentes; ações de remediação tomadas para remover fontes de incidentes.
Discussão	Ter mecanismos eficazes para detectar corrupção e perda de bits em um sistema de repositório é fundamental, mas é apenas a etapa inicial de um processo maior. Além de registrar, relatar e reparar o mais rápido possível todas as violações da integridade dos dados, esses incidentes e as ações de recuperação e seus resultados devem ser relatados aos administradores e disponibilizados a toda a equipe relevante. Dada a identificação das fontes de perda de dados, é necessária uma avaliação das revisões dos sistemas de software e hardware, procedimentos operacionais ou políticas de gerenciamento para minimizar o risco futuro de perda

	de dados.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
Microcritério	5.1.1.4 O repositório deve ter um processo para registrar e reagir à disponibilidade de novas atualizações de segurança com base em uma avaliação de risco-benefício.
Texto de suporte	Isso é necessário para proteger a integridade dos objetos de arquivo contra alterações ou exclusões não autorizadas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Registro de riscos (lista de todos os *patches* disponíveis e análise da documentação de riscos); evidência de processos de atualização (por exemplo, *server update manager daemon*); documentação relacionada às instalações de atualização.
Discussão	As decisões de aplicar atualizações de segurança provavelmente serão o resultado de uma avaliação de risco-benefício; os *patches* de segurança são frequentemente responsáveis por perturbar aspectos alternativos do sistema funcionalidade ou desempenho. Pode não ser necessário um repositório para implementar todas e a aplicação de qualquer um deles deve ser cuidadosamente considerada. Cada atualização de segurança implementada pelo repositório deve ser documentada com detalhes sobre como ela é concluída; tanto as atualizações automáticas quanto as manuais são aceitáveis. Atualizações de segurança significativas podem pertencer a outros softwares que não os sistemas operacionais principais, como aplicações de banco de dados e servidores Web, e estes também devem ser documentados. As atualizações de segurança não estão limitadas a atualizações de segurança de software. Atualizações para o hardware real ou para o *firmware* do sistema de *hardware* estão incluídas. Com o tempo, é provável que também sejam necessárias atualizações de segurança para o repositório. processos e pela sua segurança física. Embora as atualizações de segurança possam ser consideradas como uma parte do controle de mudança, eles são identificados separadamente aqui porque muitas vezes existem fora serviços que compilam e circulam informações sobre questões de segurança e atualizações. No mínimo, os repositórios devem estar monitorando esses serviços para garantir que os repositórios sejam mantidos os dados não estão sujeitos a comprometimento por ameaças identificadas.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.5 O repositório deve ter processos definidos para a mídia de armazenamento e / ou alteração de hardware (por exemplo, atualização, migração).
Texto de suporte	Isso é necessário para garantir que os dados não sejam perdidos quando a mídia falhar ou o *hardware* de suporte não puder mais ser usado para acessar os dados.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação de processos de migração; políticas relacionadas ao suporte, manutenção e substituição de hardware; documentação dos ciclos de vida de suporte esperados do fabricante do hardware; políticas relacionadas à migração de registros para sistemas de hardware alternativos.
Discussão	O repositório deve ter estimativas da velocidade de acesso e da quantidade de informações para cada tipo de mídia de armazenamento. Depois com estimativas da vida útil confiável do meio de armazenamento e informações de carregamento do sistema, etc., o repositório pode estimar o tempo necessário para migração de mídias de armazenamento, ou refrescamento ou cópia entre mídias sem reformatar o *bit stream*. O repositório pode então definir os gatilhos para iniciar a ação em um momento apropriado para que as ações sejam concluídas antes que os dados sejam perdidos. A cópia de grandes quantidades de dados pode levar muito tempo e pode afetar outras métricas de desempenho do sistema. Os repositórios também devem considerar a obsolescência de todo e qualquer componente de hardware dentro do sistema de repositório como potenciais eventos de acionamento para migração. Cada vez mais, no longo prazo, apoio apropriado para componentes de hardware do sistema é difícil de obter, expondo os repositórios a riscos e responsabilidades, caso optem por continuar a operar o hardware para além do fabricante ou garantias de suporte de terceiros. Os repositórios provavelmente precisarão realizar migração de mídia para de alguns tipos de mídia em mídia melhor suportada com base na vida útil estimada de suporte de hardware em vez de na vida mais longa esperada da mídia. É importante que o processo inclui uma verificação de que a cópia foi feita corretamente.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.6 O repositório deve ter identificado e documentado processos críticos que afetam sua capacidade de cumprir com suas responsabilidades obrigatórias.
Texto de suporte	Isso é necessário para garantir que os processos críticos possam ser monitorados para garantir que eles continuem cumprindo as responsabilidades obrigatórias e para garantir que quaisquer alterações nesses processos sejam examinadas e testadas.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Matriz de rastreabilidade entre processos e requisitos obrigatórios.
Discussão	Exemplos de processos críticos incluem gerenciamento de dados, acesso, armazenamento de arquivo, processamento e processos de segurança. A rastreabilidade possibilita entender quais processos do repositório são necessários para atender a cada uma das responsabilidades obrigatórias.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.6 O repositório deve ter identificado e documentado processos críticos que afetam sua capacidade de cumprir com suas responsabilidades obrigatórias.
Microcritério	5.1.1.6.1 O repositório deve ter um processo documentado de gerenciamento de mudanças que identifique alterações nos processos críticos que potencialmente afetam a capacidade do repositório de cumprir suas responsabilidades obrigatórias.
Texto de suporte	Isso é necessário para garantir que o repositório possa especificar não apenas os processos atuais, mas também os processos anteriores que foram aplicados às reservas do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Documentação do processo de gerenciamento de mudanças; avaliação de risco associado a uma mudança de processo; análise do impacto esperado de uma mudança de processo; comparação de *logs* de mudanças reais nos processos versus análises associadas de seu impacto e criticidade.
Discussão	Exemplos disso incluem mudanças nos processos de gerenciamento de dados, acesso, arquivamento armazenamento, ingestão e segurança. O realmente importante é poder saber o que muda foram feitas e quando elas foram feitas. Rastreabilidade permite entender o que foi afetados por mudanças particulares nos sistemas. Se consequências não intencionais forem posteriores descoberto, então ter esse registro pode tornar possível reverter as mudanças ou pelo menos documentar as mudanças que foram introduzidas. O gerenciamento de mudanças é um componente do tópico mais amplo de gerenciamento de configuração descrito pela ISO 10007:2003 que inclui planejamento de gerenciamento de configuração, identificação de configuração, controle de mudanças, contabilidade do status de configuração e auditoria de

	configuração. Esforços de gerenciamento da configuração deve resultar em uma trilha de auditoria completa das decisões e modificações de projeto.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.1 O repositório deve identificar e gerenciar os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
Subcritério	5.1.1.6 O repositório deve ter identificado e documentado processos críticos que afetam sua capacidade de cumprir com suas responsabilidades obrigatórias.
Microcritério	5.1.1.6.2 O repositório deve ter um processo para testar e avaliar o efeito das alterações nos processos críticos do repositório.
Texto de suporte	Isso é necessário para proteger a integridade dos processos críticos do repositório, de forma que eles continuem em sua capacidade de atender aos requisitos obrigatórios do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Procedimentos de teste documentados; documentação dos resultados de testes anteriores e comprovação de alterações feitas como resultado de testes; análise do impacto de uma mudança de processo.
Discussão	As alterações nos sistemas críticos devem ser, sempre que possível, pré-testadas separadamente, os comportamentos esperados documentados e os procedimentos de reversão preparados. Após as alterações, os sistemas devem ser monitorados quanto a comportamentos inesperados e inaceitáveis. Se esse comportamento for descoberto, as alterações e suas consequências deverão ser revertidas. Teste de sistema inteiro ou de unidade pode atender a esse requisito; testes complexos de segurança não são necessários. Os testes podem ser muito caros, mas deve haver algum reconhecimento do fato de que um regime completamente aberto, onde nenhuma alteração é avaliada ou testada, terá problemas.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.2 O repositório deve gerenciar o número e o local das cópias de todos os objetos digitais.
Texto de suporte	Isso é necessário para afirmar que o repositório está fornecendo uma cópia autêntica de um objeto digital específico.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Testes de recuperação aleatória; validação da existência do objeto para cada local registrado; validação de um local registrado para cada objeto nos sistemas de armazenamento; informações de verificação de procedência e fixação; registro / registro de localização de objetos digitais em comparação com o número esperado e localização de cópias de objetos específicos.
Discussão	Um repositório pode ter políticas de preservação diferentes para diferentes classes de objetos, dependendo de fatores como o produtor, o tipo de informação ou seu valor. Os repositórios podem exigir um número diferente de cópias para cada classe ou gerenciar as versões necessárias para atender aos requisitos de acesso. Pode haver requisitos adicionais de identificação se os mecanismos de integridade de dados usarem cópias alternativas para substituir cópias com falha. A localização de cada objeto digital deve ser descrita de modo que o objeto possa ser localizado com precisão, sem ambiguidade. O local pode ser um local físico absoluto ou um local lógico em uma mídia de armazenamento ou um subsistema de armazenamento. As informações de procedência sobre como copiar e mover os dados devem ser mantidas / atualizadas, incluindo a identificação dos responsáveis. Isso é necessário para rastrear a cadeia de custódia e afirmar que o repositório está fornecendo uma cópia autêntica de um objeto digital específico. O repositório deve ser capaz de distinguir entre versões de objetos ou cópias e cópias idênticas. Isso é necessário para que um repositório possa afirmar que está fornecendo uma cópia autêntica da versão correta de um objeto.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.1 Gestão de Riscos de Infraestrutura Técnica
Critério	5.1.2 O repositório deve gerenciar o número e o local das cópias de todos os objetos digitais.
Subcritério	5.1.2.1 O repositório deve ter mecanismos para garantir que qualquer / várias cópias de objetos digitais sejam sincronizadas.
Texto de suporte	Isso é necessário para garantir que várias cópias de um objeto digital permaneçam idênticas, dentro de um prazo estabelecido como aceitável pelo repositório, e que uma cópia possa ser usada para substituir uma cópia corrompida do objeto.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	Fluxos de trabalho de sincronização; análise do sistema quanto tempo leva para as cópias serem sincronizadas; procedimentos / documentação dos processos de sincronização.
Discussão	O plano de recuperação de desastre deve abordar o que fazer se um desastre e uma atualização coincidirem. Por exemplo, se uma cópia de um objeto for alterada e ocorrer um desastre enquanto a segunda estiver sendo atualizada, é necessário haver um mecanismo para garantir que a cópia seja atualizada na primeira oportunidade disponível. Os mecanismos para sincronizar cópias de objetos digitais devem ser capazes de detectar corrupção de bits e validar as verificações de

	correção antes da tentativa de sincronização.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.2. Gestão de Riscos de Segurança
Critério	5.2.1 O repositório deve manter uma análise sistemática dos fatores de risco à segurança associados aos dados, sistemas, pessoal e instalações físicas.
Texto de suporte	Isso é necessário para garantir um serviço contínuo e ininterrupto à Comunidade Designada.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	O repositório emprega os códigos de prática encontrados na lista de controle de sistemas da série ISO 27000; análise de risco, ameaça ou controle.
Discussão	O repositório deve realizar avaliações regulares de risco e manter a proteção de segurança adequada, a fim de fornecer níveis de serviço esperados e contratados, seguindo códigos de práticas como a ISO 27000. 'Sistema' aqui se refere a mais do que sistemas de TI, como hardware, software, equipamentos e instalações de comunicação e firewalls. Os sistemas de proteção contra incêndio e detecção de inundação também são significativos, assim como meios para avaliar os procedimentos de pessoal, gerenciamento e administração, recursos, bem como operações e prestação de serviços. Perda de receita, orçamento e reputação são ameaças significativas para as operações gerais, assim como a perda de mandato. Uma avaliação interna e externa contínua deve ser conduzida para avaliar a qualidade do serviço e a relevância para a comunidade de usuários atendida e auditorias financeiras periódicas devem ser asseguradas para verificar a prática ética e legal e a manutenção dos fundos operacionais necessários. As práticas de direitos de propriedade intelectual também devem ser revisadas regularmente, bem como a responsabilidade do repositório por não conformidade regulamentar, conforme aplicável. O repositório deve avaliar as habilidades de sua equipe em relação às exigidas no ambiente em evolução do repositório digital e garantir a aquisição de novas equipes ou a reciclagem da equipe existente, conforme necessário. A avaliação regular de riscos também deve abordar ameaças externas e ataques de negação de serviço e perda ou qualidade inaceitável de serviços de terceiros. O repositório pode realizar avaliações gerais de risco com ferramentas como DRAMBORA.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.2. Gestão de Riscos de Segurança
Critério	5.2.2 O repositório deve ter implementado controles para abordar adequadamente cada um dos riscos de segurança definidos.
Texto de suporte	Isso é necessário para garantir que os controles estejam em vigor para atender às necessidades de segurança do repositório.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	O repositório emprega os códigos de prática encontrados na série de normas ISO 27000; lista de controle do sistema; análises de risco, ameaça ou controle; e adição de controles com base na detecção e avaliação de riscos em andamento. O repositório mantém a certificação ISO 17799.
Discussão	O repositório deve mostrar como ele lidou com seus requisitos de segurança. Se é mais provável que alguns tipos de material sejam atacados, o repositório precisará fornecer mais proteção, por exemplo. Os repositórios que sofreram incidentes podem registrar tais instâncias, incluindo os momentos em que os sistemas ou o conteúdo foram afetados e descrever os procedimentos que foram implementados para evitar ocorrências semelhantes no futuro. Repositórios também podem conduzir uma variedade de exercícios de desastre que podem envolver a organização dos pais ou a comunidade em geral. Os planos de contingência são especialmente importantes e precisam ser testados, atualizados e revisados regularmente.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.2. Gestão de Riscos de Segurança
Critério	5.2.3 A equipe do repositório deve ter funções, responsabilidades e autorizações delineadas relacionadas à implementação de mudanças no sistema.
Texto de suporte	Isso é necessário para garantir que os indivíduos tenham autoridade para implementar mudanças, que recursos adequados tenham sido designados para o esforço e que os responsáveis sejam responsáveis pela implementação de tais mudanças.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	O repositório emprega os códigos de prática encontrados na série de normas ISO 27000; organograma; documentação de autorização do sistema. O repositório mantém a certificação ISO 17799.
Discussão	As autorizações são sobre quem pode fazer o quê: quem pode adicionar usuários, quem tem acesso a metadados alterados, quem pode acessar logs de auditoria. É importante que as autorizações sejam justificadas, que a equipe entenda o que está autorizado a fazer, que a equipe tenha habilidades requeridas associadas a várias funções e autorizações e que exista uma visão consistente disso em toda a organização.

Seção	5 Gestão de Riscos de Infraestrutura e Segurança
Categoria	5.2. Gestão de Riscos de Segurança
Critério	5.2.4 O repositório deve ter planos adequados de preparação e recuperação de desastres por escrito, incluindo pelo menos um backup externo de todas as informações preservadas, juntamente com uma cópia externa do(s) plano(s) de recuperação.
Texto de suporte	Isso é necessário para garantir a disponibilidade de recursos suficientes de backup e recuperação para facilitar a preservação e o acesso contínuos aos sistemas e seu conteúdo, com interrupção limitada dos serviços.
Exemplos de maneiras pelas quais o repositório pode demonstrar que está atendendo a esse requisito	O repositório emprega os códigos de prática encontrados na série de normas ISO 27000; planos de desastre e recuperação; informações e prova de pelo menos uma cópia externa das informações preservadas; plano de continuidade de serviço; documentação vinculando papéis com atividades; dados geológicos, geográficos ou meteorológicos locais ou avaliações de ameaças. O repositório mantém a certificação ISO 17799.
Discussão	O nível de detalhe em um plano de desastre e os riscos específicos abordados precisam ser adequados à localização e às expectativas de serviço do repositório. O fogo é uma preocupação quase universal, mas os terremotos podem não exigir planejamento específico em todos os locais. O plano de desastre deve, no entanto, lidar com situações não especificadas que teriam consequências específicas, como falta de acesso a um prédio ou doença generalizada entre funcionários críticos. No caso de um desastre no repositório, o repositório pode entrar em contato com os órgãos de recuperação de desastre locais e / ou nacionais para obter assistência. Os repositórios também podem realizar uma variedade de exercícios de desastre que podem envolver a organização dos pais ou a comunidade em geral.

APÊNDICE E - MODELO DE MATURIDADE DE CAPACIDADE (DPCMM) - CINCO ETAPAS DA CAPACIDADE DE PRESERVAÇÃO DIGITAL[130]

Como outros modelos de maturidade de capacidade, o DPCMM utiliza uma abordagem de cinco níveis ou estágios. Seus níveis variam do Nominal na extremidade mais baixa ao Ótimo na extremidade mais alta, conforme mostra a Figura 1.

Em uma organização que opera em um Nível Nominal de Capacidade de Preservação Digital (Fase 1), um programa sistemático de gerenciamento de registros eletrônicos e/ou preservação digital ainda não foi realizado ou um programa de preservação digital existe apenas em papel. Em contraste, o nível mais alto (Etapa 5 - Otimização) da Capacidade de Preservação Digital representa uma organização com capacidades sustentáveis e confiáveis que são, sistematicamente, gerenciadas por meio da melhoria e otimização de processos.

FIGURA 1 - Cinco Estágios de Capacidade de Preservação Digital

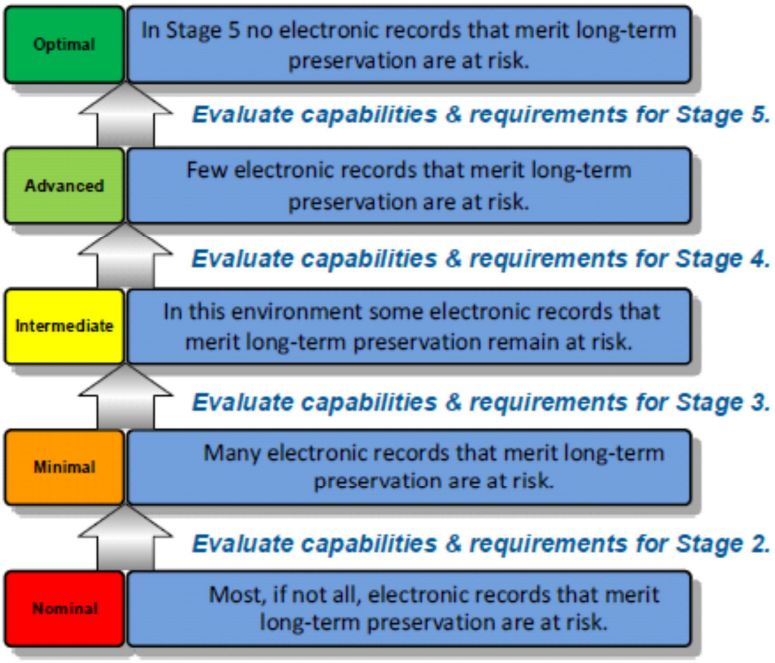


Figure 1. Five Stages of Digital Preservation Capability

FONTE: DPCMM, 2015. Tradução nossa.

A conformidade com os requisitos da ISO 14721 e os critérios de auditoria da ISO 16363 para todos os 15 componentes DPCMM é necessária para alcançar a capacidade Intermediária (Fase 3 - Capacidade).

Etapa 5: Ótima Capacidade de Preservação Digital

A Etapa 5 é o mais alto nível de preparação para a preservação digital que uma organização pode alcançar. Ela inclui um foco estratégico nos resultados da preservação digital, melhorando, continuamente, a maneira pela qual o gerenciamento do ciclo de vida dos registros eletrônicos é executado. A capacidade de preservação digital da Etapa 5 também envolve *benchmarking*[131] de infraestrutura e serviços em relação a outros programas de preservação digital "melhores da classe" e a realização de monitoramento proativo para tecnologias inovadoras que podem permitir que o programa melhore seu desempenho de preservação digital. Na Etapa 5, poucos ou nenhum registro eletrônico que mereça preservação no longo prazo está em risco.

Etapa 4: Capacidade Avançada de Preservação Digital

A capacidade da Fase 4 é caracterizada por uma organização com uma infraestrutura robusta e serviços de preservação digital baseados nas especificações ISO 14721 e TRAC, a Auditoria e Certificação de Repositório de Confiança: Critérios e lista de verificação e/ou ISO 16363. Nessa etapa, a preservação de registros eletrônicos é enquadrada inteiramente dentro de um ambiente colaborativo no qual há múltiplas partes interessadas participantes. As lições aprendidas com essa estrutura colaborativa servem como base para adaptar e melhorar as capacidades de identificar e trazer proativamente registros eletrônicos de longo prazo sob controle e gerenciamento do ciclo de vida. Alguns registros eletrônicos que merecem preservação no longo prazo ainda podem estar em risco.

Etapa 3: Capacidade de Preservação Digital Intermediária

Na Etapa 3, descreve-se um ambiente que abrange as especificações ISO 14721 e outros padrões e esquemas de melhores práticas e, assim, estabelece a base para

sustentar capacidades aprimoradas de preservação digital, ao longo do tempo. Essa base inclui a conclusão bem sucedida de projetos e resultados que apoiam as capacidades de preservação digital empresarial e fomentam a colaboração, incluindo recursos compartilhados, entre unidades produtoras de registros e entidades responsáveis pelo gerenciamento e manutenção de repositórios digitais confiáveis. Nesse ambiente, muitos registros eletrônicos que merecem preservação de longo prazo, provavelmente, permanecerão em risco.

Etapa 2: Capacidade Mínima de Preservação Digital

Na Etapa 2, descreve-se um ambiente onde ainda não existe um repositório de preservação baseado na ISO 14721. Um repositório de preservação de substitutos para registros eletrônicos está disponível para alguns produtores de registros que satisfazem algumas das especificações da ISO 14721, mas não todas. Há algum entendimento das questões e estratégias de preservação digital, mas ele está limitado a relativamente poucos indivíduos. Pode não haver praticamente nenhuma relação entre o sucesso ou fracasso de uma iniciativa de preservação digital e o sucesso ou fracasso de outra. O sucesso é, em grande parte, o resultado de ações excepcionais (talvez até heróicas) de um indivíduo ou de uma equipe de projeto. O conhecimento sobre tal sucesso não é amplamente compartilhado ou institucionalizado. A maioria dos registros eletrônicos que merece preservação no longo prazo está em risco.

Etapa 1: Capacidade de Preservação Digital Nominal

Na Etapa 1, descreve-se um ambiente no qual as especificações da ISO 14721 e outras normas podem ser conhecidas, aceitas em princípio ou em consideração, mas não foram, formalmente, adotadas ou implementadas pela unidade responsável pela preservação (ou seja, a função de Arquivo ou Gerenciamento de Registros) ou pelos produtores de registros. Geralmente, pode haver algum entendimento sobre questões e preocupações relativas à preservação digital, mas é provável que esse entendimento consista em práticas *ad hoc* de gerenciamento de registros eletrônicos e iniciativas e infraestrutura de continuidade digital. Embora possa haver alguns casos isolados de indivíduos que tentam preservar registros eletrônicos em uma rede ou mídia de armazenamento removível (por exemplo, DVD ou disco rígido), praticamente todos os registros eletrônicos que merecem preservação no longo prazo estão em risco.

Escopo do Modelo de Maturidade de Capacidade de Preservação Digital

Este modelo de maturidade de capacidade consiste em quinze (15) componentes, ou áreas-chave do processo, que são necessários para a continuidade, acesso e preservação, no longo prazo, de registros eletrônicos autênticos, acessíveis e confiáveis. Cada componente é descrito e são identificadas métricas para cada um dos cinco (5) níveis de capacidade de preservação digital. A conformidade e o desempenho sustentado em qualquer nível são necessários antes que o próximo nível superior possa ser alcançado.

O objetivo do modelo é fornecer uma estrutura de processo e desempenho (benchmark) em relação aos padrões de melhores práticas e princípios fundamentais de gerenciamento de registros, governança da informação e ciência de arquivos. Os cinco níveis de capacidade identificados para cada um dos componentes do DPCMM oferecem uma maneira de as organizações verem qual nível de esforço sustentado é necessário para passar para o próximo nível superior.

Observe que o modelo tem três características de alto nível separadas, mas inter-relacionadas: Infraestrutura de Preservação Digital, Repositório de Preservação e Serviços de Preservação Digital. As páginas seguintes incluem notas de escopo para os elementos gráficos no diagrama DPCMM.

FIGURA 2 -Modelo de Maturidade de Capacidade de Preservação Digital

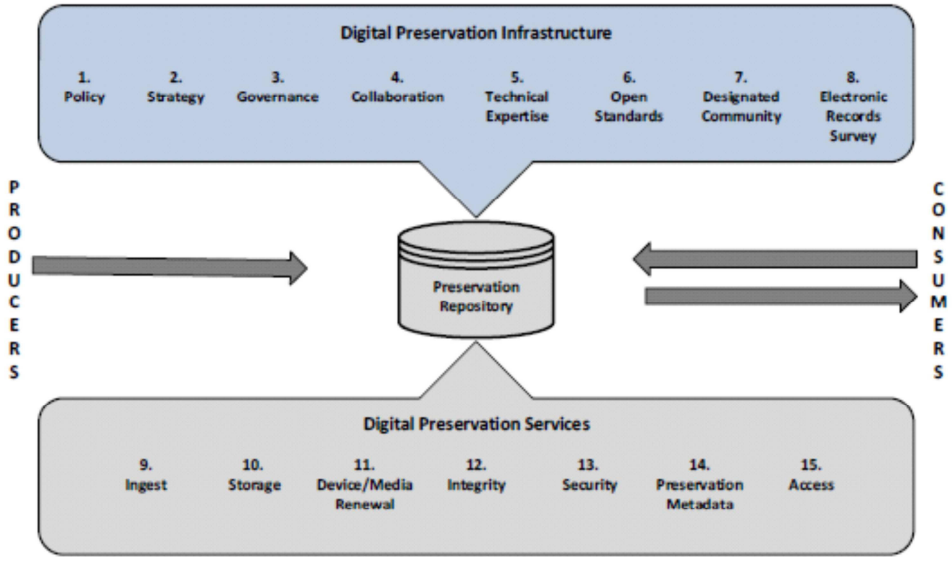


Figure 2. Digital Preservation Capability Maturity Model© (DPCMM)

FONTE: DPCMM, 2015. Tradução nossa.

6.4.1 Produtores

Produtores é o termo utilizado para referenciar criadores e proprietários externos de registros eletrônicos que têm a obrigação de manter registros de longo prazo (10+ anos) e/ou registros permanentes armazenados em formato digital. Essas partes interessadas têm a responsabilidade de fornecer informações suficientes sobre a origem e o uso dos registros ao repositório e de se engajar na preservação ativa sempre que possível. Os produtores podem ter a obrigação ou a opção de transferir registros eletrônicos permanentes e de longo prazo para um ou mais repositórios de preservação especificados para guarda e acesso.

6.4.2 Repositório de Preservação

Garantir a continuidade dos registros eletrônicos e possibilitar o projeto, operação e gestão de ambientes de preservação requer a integração de pessoas, processos e tecnologias. O ambiente de preservação digital mais completo é baseado em modelos e critérios de desempenho que incluem ISO 14721, ISO 16363 e práticas operacionais, geralmente aceitas. A organização que tem a custódia dos registros pode gerenciar o repositório ou pode contratar um terceiro externo. Uma variedade de sistemas, ferramentas e serviços pode ser combinada para facilitar o fluxo de trabalho de ponta a ponta dos registros, desde a ingestão até o acesso.

Um repositório de preservação pode variar, desde um sistema simples que envolve um servidor de arquivos de baixo custo e softwares que fornecem serviços de preservação não-integrados até sistemas complexos compostos de centros de dados e fazendas de servidores e redes de comunicação interoperáveis. É provável que muitas organizações, inicialmente, confiem nos recursos e serviços de preservação digital "substituto" que se aproximam, mas não oferecem todas as funcionalidades de transferência, gerenciamento de dados e acesso de um sistema em conformidade com a ISO 14721.

6.4.3 Consumidores

Os consumidores ou usuários ou registros eletrônicos compreendem uma Comunidade Designada composta por indivíduos ou grupos externos com interesse e/ou direito de acesso aos registros no repositório de preservação. Essas partes interessadas, provavelmente, representarão uma variedade de interesses e suas exigências de acesso, provavelmente, mudarão com o tempo.

Infraestrutura de Preservação Digital

Há oito (8) componentes de infraestrutura que são essenciais para assegurar um compromisso organizacional sustentado, incluindo recursos adequados e sustentados, para a preservação no longo prazo dos registros eletrônicos:

1. Política de Preservação Digital
2. Estratégia de Preservação Digital
3. Governança
4. Colaboração
5. Especialização técnica
6. Formatos de Tecnologia Padrão Aberta Neutra ("OS/TN")
7. Comunidade Designada
8. Levantamento de Registros Eletrônicos

Os oito componentes de infraestrutura de preservação digital se concentram no que uma organização como entidade distinta faz para identificar registros e coleções que requerem preservação e permitir que um repositório de preservação execute as ações de preservação digital apropriadas. Ou, dito de outra forma, um repositório de preservação confiável executa serviços dentro das restrições da infraestrutura de preservação digital de uma organização.

6.4.5. Serviços de Preservação Digital

Existem sete (7) áreas-chave do processo empresarial necessárias para o monitoramento contínuo de ambientes externos e internos a fim de planejar e tomar ações de preservação que sustentem a integridade, segurança, usabilidade e acessibilidade das informações e registros eletrônicos armazenados em repositórios de preservação:

9. Admissão
10. Armazenamento de arquivos
11. Renovação de Mídia/Dispositivo
12. Integridade
13. Segurança
14. Metadados de Preservação
15. Acesse

Os sete serviços de preservação digital concentram-se em uma gama de ações necessárias para ingerir e manter registros eletrônicos permanentes e de longo prazo e monitorar, continuamente, o ambiente técnico do qual eles dependem. A capacidade de planejar e executar eficientemente ações de preservação para sustentar a integridade, segurança, usabilidade e acessibilidade dos registros armazenados, no repositório, depende da organização produtora de registros para identificar e transferir, sistematicamente, registros eletrônicos de valor de longo prazo, bem como fornecer orientação estratégica e recursos suficientes.

6.4.6. Pontuação do Índice de Capacidade de Preservação Digital

Cada um dos 15 componentes DPCMM tem cinco métricas de desempenho de capacidade associadas a ele. Cada métrica de capacidade de preservação digital tem um valor entre 0 e 4. Se um exercício de autoavaliação determinar que uma pontuação de desempenho de 3 para um componente específico é apropriada, para a Política de Preservação Digital, por exemplo, ela se torna o valor índice para a capacidade da Política de Preservação Digital da organização. Esse procedimento é repetido para os catorze componentes restantes da DPCMM, o que resulta em uma pontuação agregada da capacidade de preservação digital. A gama de índices compostos de pontuação organizada por cada um dos cinco níveis é:

FIGURA 3 - Gama de Pontuação do Índice de Capacidade de Preservação Digital

	Capability Levels	Composite Index Score
	Nominal Digital Preservation Capability	0
	Minimal Digital Preservation Capability	1 - 15
	Intermediate Digital Preservation Capability	16 - 30
	Advanced Digital Preservation Capability	31 - 45
	Optimum Digital Preservation Capability	46 – 60

6.4.7. Componentes e Métricas de Capacidade de Preservação Digital

O DPCMM é composto por 15 componentes. Esta seção descreve cada componente e o conjunto associado de cinco métricas de capacidade de preservação digital. As definições podem ser encontradas no Glossário de Termos (Anexo A). Ao longo da seção de métricas, usamos os termos "organização" e "produtor de registros" para designar a pessoa jurídica (empresa, instituição, associação, agência, indivíduo, etc.) que está

encarregada ou assumiu a tarefa de possibilitar a continuidade e preservação de registros de longo prazo e/ou permanentes.

O termo "repositório de preservação" é usado para denotar as pessoas, processos e tecnologias integradas encarregadas de ingerir, armazenar, proteger, gerenciar e fornecer acesso aos registros eletrônicos. Essa função pode ser fornecida por uma unidade interna de negócios ou tecnologia, operada como um ou mais repositórios autônomos sob o controle de uma unidade de Arquivos ou Gerenciamento de Registros, incluir a participação em um sistema de repositório federado ou regional, e/ou incluir o uso de serviços de preservação digital fornecidos por um ou mais terceiros. Os indivíduos ou grupos que buscam acesso aos registros eletrônicos no repositório de preservação são referidos como "usuários". Reconhecemos e reconhecemos que diferentes unidades organizacionais ou funcionais e/ou partes interessadas podem ter essas responsabilidades. Encorajamos o uso de termos alternativos para essas convenções onde isso for desejável.

A conformidade com a ISO 14721 requer capacidades sustentadas em níveis mais baixos, conforme descrito, pelo uso de uma barra azul (ver abaixo) nas tabelas de métricas.

FIGURA 4 - Limiar de Conformidade

Level	Digital Preservation Capability Metrics
0	
1	
2	
	ISO 14721 Conformance
3	
4	

6.4.7.1. Infraestrutura de Preservação Digital: Componentes 1 - 8

1. Política de Preservação Digital

A preservação de registros eletrônicos acessíveis, autênticos e utilizáveis para o futuro, tanto quanto necessário, depende das tecnologias de informação digital, mas depende igualmente do compromisso e das práticas organizacionais. A organização encarregada de garantir a preservação e o acesso a registros legais, fiscais e/ou históricos de longo prazo e permanentes deve declarar sua política por escrito, comunicar a política a todos os interessados e auditar, periodicamente, a política de conformidade.

Uma política de preservação digital escrita inclui o propósito, escopo, responsabilidade e abordagem para a transferência de registros e a gestão operacional e sustentabilidade de repositórios de preservação confiáveis.

Nível	Política de Preservação Digital Métricas de Capacidade
0	A organização não tem uma política de preservação digital escrita.
1	A organização tem uma política de preservação digital em desenvolvimento, mas ainda não foi aprovada ou emitida.
2	Na organização, emitiu-se uma política de preservação digital e ela é amplamente divulgada às partes interessadas.
	Conformidade ISO 14721
3	Pela organização, realiza-se, anualmente, uma autoavaliação e relata a adesão à política de preservação digital a seu órgão dirigente.
4	A organização organiza uma revisão periódica por pares ou auditoria externa da política de preservação digital e revisa a política conforme apropriado.

2. Estratégia de Preservação Digital

A organização encarregada da preservação dos registros eletrônicos permanentes e de longo prazo deve abordar proativamente os riscos associados à obsolescência da tecnologia. Embora nenhuma estratégia única seja apropriada para todas as organizações, tipos de informação e recursos, deve haver planos para, periodicamente, atualizar dispositivos de armazenamento, mídias de armazenamento e formatos de arquivo.

Se não for verificado, a obsolescência dos dispositivos de armazenamento e das mídias eventualmente renderá os fluxos de bits de registros eletrônicos não legíveis. A obsolescência inevitável dos formatos de arquivos, especialmente os nativos, proprietários, significa que, com o tempo, as aplicações de software não serão capazes de renderizar fluxos de bits em registros eletrônicos compreensíveis e utilizáveis.

A estratégia geralmente aceita é a de mitigar a obsolescência dos dispositivos/mídia de armazenamento, por meio de renovação planejada e periódica, que, ao longo do tempo, garante que os "fluxos de bits" possam ser lidos pela tecnologia corrente (ver Componente 11). A estratégia geralmente aceita para a mitigação do formato de arquivo obsolescência é a dependência de formatos interoperáveis e abertos, neutros em termos de tecnologia padrão, que são de outra forma considerados "formatos de preservação preferidos" (ver Componente 5).

Nível	Métricas de Capacidade da Estratégia de Preservação Digital de Nível
0	Na organização, não se tem uma estratégia formal, para enfrentar a obsolescência tecnológica.
1	A estratégia exige a aceitação de registros eletrônicos em formatos nativos em uma base ad hoc e manter os fluxos de bits vivos até que software e outros recursos

	estejam disponíveis para transformar os registros em formatos de arquivo neutros em tecnologia padrão aberto.
2	Com a estratégia exige incentivar os produtores de discos a converter os registros eletrônicos de longo prazo e valor permanente em sua custódia para formatos de "preservação pronta" no ou perto do momento do recebimento e da criação. A estratégia inclui o monitoramento ad hoc das mudanças em tecnologias que podem impactar as coleções de registros digitais na custódia dos produtores de discos e repositórios de preservação.
	Conformidade ISO 14721
3	Além da promoção de registros de "preservação pronta", a estratégia exige transformação de registros eletrônicos em cinco (5) formatos de arquivos nativos selecionados para os preferenciais formatos de preservação na ingestão e monitoramento proativo das mudanças nas tecnologias que afetam a preservação dos registros eletrônicos.
4	A estratégia exige a transformação de registros eletrônicos em formatos de arquivos nativos para dez (10) ou mais formatos de preservação preferidos a ingerir. Registros eletrônicos no armazenamento de arquivos são, automaticamente, transformados em novas formas interoperáveis à medida que substituem as atuais. Monitoramento proativo das mudanças nas tecnologias que afetam a preservação de registros está em andamento.

3. Governança

Uma organização com um mandato de preservação digital deve ter um processo formal de tomada de decisão alinhado com sua estrutura de governança de informação empresarial que atribui responsabilidade e autoridade para a preservação de registros eletrônicos com valor permanente, e articula abordagens e práticas para repositórios de preservação suficientes para atender às necessidades das partes interessadas. Essa capacidade aproveita de forma ideal regras organizacionais, práticas e protocolos existentes, bem como envolve as partes interessadas interfuncionais.

A preservação, em longo prazo, no entanto, pode exigir a criação de novas autoridades para enfrentar as ameaças de obsolescência tecnológica. Um repositório de preservação pode ser administrado por uma unidade de negócios ou de tecnologia, operado como um ou mais repositórios autônomos sob o controle de uma unidade de Gerenciamento de Registros ou Arquivos, incluem a participação em um sistema de repositório federado ou regional, e/ou o uso de arquivos digitais serviços de preservação prestados por um ou mais terceiros.

A organização exerce a governança da preservação digital em conjunto com arquivos, informações funções de gestão/tecnologia, e com outros custodiantes e partes interessadas na preservação digital tais como produtores e usuários de discos. A estrutura de governança permite o cumprimento do repositório de preservação com leis aplicáveis, regulamentos, cronogramas de retenção de registros, disposição autoridades, e normas. Planos e decisões resultantes das atividades de governança, incluindo as estatísticas

operacionais do repositório, são compartilhadas com as partes interessadas internas e operadores de terceiros.

Nível	Métricas de Capacidade de Governança de Nível
0	As atividades atuais de governança de informação da organização não tratam especificamente requisitos de preservação digital.
1	A organização tem uma estrutura de governança de preservação digital limitada, baseada em projetos que esteja operacional ou que tenha sido concluída com sucesso.
2	A organização está desenvolvendo uma estrutura de governança empresarial que identifica papéis e responsabilidades pelo gerenciamento do ciclo de vida dos registros eletrônicos e preservação digital.
	Conformidade ISO 14721
3	Na organização, adotou-se uma estrutura de governança de preservação digital empresarial que inclui políticas e procedimentos abrangentes e especifica um compromisso contínuo de a sustentabilidade de um ou mais repositórios de preservação.
4	A estrutura de governança da preservação digital empresarial suporta um ou mais de preservação e é revista e atualizada pelo menos a cada dois anos para tecnologias e requisitos organizacionais em mudança de conta.

4. Colaboração

A preservação digital é uma disciplina multifacetada, que leva em conta as informações da organização ambiente de arquitetura e tecnologia, bem como normas e melhores práticas aceitas. Um com um mandato para preservar os registros eletrônicos é bem servido, mantendo e promovendo colaboração entre suas muitas partes interessadas.

Planos para diferentes tipos de registros, modelos para abordagens e critérios de preservação, e uma estrutura de componentes e serviços de repositório exigem uma cooperação e um compromisso mais estreito entre componentes e serviços de longa data, parceiros tais como TI, organizações pares, fornecedores de software e serviços, e outros suportes funções. A colaboração deve reconhecer as interdependências entre elas e as operações de produtores de registros, requisitos legais e estatutários, políticas de tecnologia da informação e governança, e responsabilidade histórica.

O engajamento ativo em enfrentar os desafios da preservação digital, em longo prazo faz o melhor uso de recursos e lições aprendidas. A estrutura de colaboração evolui em resposta às mudanças em tecnologias da informação e as operações comerciais dos Produtores de discos.

Essa colaboração estrutura procura alavancar recursos financeiros, humanos e técnicos, promover a administração, e trocar conhecimentos sobre o estado atual e futuro das iniciativas digitais. Essa colaboração pode se estender além da organização para incluir outros repositórios, federais ou outras agências públicas setoriais, bem como consórcios de outras organizações com uma missão semelhante ou compartilhada.

Nível	Métricas de Capacidade de Colaboração de Nível
0	Não existe um ambiente colaborativo de preservação digital dentro ou através da organização.
1	A organização está atualmente trabalhando para estabelecer uma estrutura para a preservação digital colaborativa engajamento em questões de gerenciamento de registros eletrônicos e preservação digital.
2	Sob sua estrutura de preservação digital colaborativa, a organização tem tido sucesso engajado ou está atualmente engajado com entidades interessadas selecionadas para tratar proativamente requisitos de preservação digital. Estes compromissos podem incluir financiamento externo iniciativas colaborativas de preservação digital.
	Conformidade ISO 14721
3	Sob sua estrutura de preservação digital colaborativa, a organização tem tido sucesso engajado ou está atualmente engajado com a maioria das partes interessadas para identificar e atender proativamente seus requisitos de preservação digital.
4	A organização monitora e atualiza continuamente sua colaboração em preservação digital para apoiar a divulgação proativa a todas as partes interessadas a fim de identificar e atender seus requisitos de preservação digital.

5. Especialização técnica

Uma capacidade de preservação digital viável requer que as organizações tenham experiência suficiente em eletrônica gestão de registros e preservação digital para suportar toda a infraestrutura e a chave necessária processos, incluindo o desenvolvimento profissional contínuo para o pessoal e a certificação do repositório. A experiência técnica pode existir dentro do pessoal interno ou contratado, pode ser fornecida por um bureau de serviços centralizado, ou por prestadores de serviços externos.

NOTA: É provável que muitas organizações iniciem um programa de preservação digital de longo prazo com um ou mais aplicações de gerenciamento de registros eletrônicos (RMA) que estejam em conformidade com o nível nacional ou regional tais como a Diretiva 5015.2-STD do Departamento de Defesa (DoD), Requisitos do Modelo para o Gerenciamento de Registros Eletrônicos (MoReq2010), e *Victorian Electronic Records Strategy* versão 2(VERS2). Estes sistemas podem suportar algumas funções, mas não todas, da ISO 14721.

Nível	Métricas de Capacidade Técnica de Especialização de Nível
0	A organização tem pouco ou nenhum acesso operacional a profissionais técnicos especializados experiência em preservação digital ou gerenciamento de registros eletrônicos.
1	A organização tem acesso a conhecimentos técnicos profissionais internos ou externos que apóia apenas iniciativas de preservação digital baseadas em projetos estritamente definidos. Isto também pode incluir experiência técnica na implantação de aplicações de gerenciamento de registros eletrônicos (RMA) certificado segundo uma ou mais normas.
2	A organização tem acesso a conhecimentos técnicos profissionais internos ou externos que auxiliar os produtores de registros na criação de registros prontos para preservação e/ou suporte serviços de armazenamento substituto de ingestão e arquivamento.
	Conformidade ISO 14721
3	A organização tem acesso a conhecimentos técnicos profissionais internos ou externos que suporta todas as funções de um repositório de preservação ISO 14721.
4	A organização tem acesso a conhecimentos técnicos profissionais internos ou externos que suporta todas as funções de um repositório de preservação ISO 14721, juntamente com a capacidade de avaliar o impacto das tecnologias emergentes que devem ser levadas em conta no longo prazo atividades de planejamento de preservação digital.

6. Formatos neutros de tecnologia padrão aberta

Um requisito para um programa de preservação digital sustentável que garanta o acesso registros eletrônicos compreensíveis, em longo prazo, é a atenuação da obsolescência do formato do arquivo. As melhores práticas atuais para a mitigação da obsolescência de formato do arquivo envolve três ações separadas, mas relacionadas.

A primeira ação é apoiar um Programa de Vigilância Tecnológica sobre a sustentabilidade do arquivo formatos. Isso pode ser alcançado, por meio de um serviço externo como a Biblioteca do Congresso dos EUA ou PRONOM, o registro técnico dos Arquivos Nacionais do Reino Unido.

A segunda ação envolve o compromisso do repositório de preservação em adotar formatos de arquivo neutros em tecnologia padrão ("OS/TN") para usar como formatos de preservação.

A terceira ação diz respeito ao engajamento proativo e às relações de trabalho colaborativo com produtores de Registros para aconselhá-los sobre o uso de formatos de arquivos prontos para preservação, quando eles criam e mantêm registros eletrônicos de longo prazo e permanentes registros históricos, legais ou valor financeiro que será transferido para a custódia de um repositório de preservação.

Arquivos padrão-aberto e neutros, em relação à plataforma, são desenvolvidos em um ambiente aberto e público, são emitidos por uma organização de padrões, e têm poucas ou nenhuma dependências tecnológicas. Arquivo OS/TN atual preferido. Os formatos incluem:

- CSV para planilhas;
- HTML, Texto simples, XML, ODF, e PDF/A para texto;
- JPGE 2000 para fotografias;
- PDF/A, PNG, e TIFF para imagens escaneadas;
- SVG para gráficos;
- MPEG-4 e Motion JPEG2000 para vídeo;
- WAVE_BWF LPCM para áudio;
- WARC para páginas web;

Com o tempo, surgirão ferramentas e soluções de preservação digital que exigirão um novo padrão aberto, formatos de arquivo padrão neutros em termos de tecnologia. Os formatos padrão-aberto de tecnologia neutra são retrógrados compatíveis para que possam suportar a interoperabilidade entre plataformas tecnológicas, durante um período prolongado de tempo e espaço.

Nível	Formatos Padrão Abertos de Tecnologia Neutra Métricas de Capacidade
0	A organização ainda não adotou nenhum formato de arquivo de tecnologia padrão-aberto (OS/TN) como um formato de preservação preferido.
1	A organização adotou pelo menos um formato de arquivo OS/TN como um formato de preservação preferido formato.
2	A organização não adotou mais do que três formatos OS/TN como formato de preservação preferencial formatos.
	Conformidade ISO 14721
3	A organização adotou não mais do que cinco formatos abertos e neutros em termos de tecnologia padrão como formatos preferidos de preservação digital (texto, planilhas, imagens escaneadas, vetoriais gráficos, fotos digitais, áudio, vídeo e páginas web). É utilizado um Programa de Vigilância Tecnológica para monitorar a sustentabilidade destes formatos de arquivo OS/TN.
4	A organização adotou dez ou mais formatos OS/TN neutros como formatos de preservação digital preferidos e monitora continuamente o surgimento de novos formatos de arquivo OS/TN e os adota como apropriados para uso como formatos preferenciais de preservação digital.

7. Comunidade Designada

A organização que tem responsabilidade pela preservação e acesso aos registros eletrônicos permanentes é bem servida, por meio de uma divulgação e engajamento proativos com sua Comunidade Designada de Registros produtores e usuários. Embora essa atividade, tradicionalmente, tenha sido realizada com representantes dos registros produtores, na forma de avaliação de registros e revisão do cronograma de retenção e autorização de disposição, os desafios da preservação digital exigem que os profissionais de gerenciamento de registros se engajem em ações adicionais "a montante"

na gestão do ciclo de vida da eletrônica de longo prazo e registros permanentes. Os acordos de submissão e protocolos de transferência devem ser padronizados e o nível de serviço, acordos definidos para operações de repositório.

Acordos e procedimentos formais com registros os produtores documentam o conteúdo, os direitos e as condições sob as quais o repositório de preservação ingerir, preservar e fornecer acesso a registros eletrônicos. Garantias específicas são dadas para garantir privacidade e proteção da propriedade intelectual, conforme apropriado.

A organização mantém procedimentos escritos relativos ao acesso a suas coleções eletrônicas. Os Pacotes de Informação de Divulgação (DIPs) são desenvolvidos e atualizados em conjunto com suas comunidades de usuários (por exemplo, estudiosos, genealogistas, o público, etc.).

Os procedimentos são revisados, regularmente e atualizados para levar em conta as mudanças nas práticas comerciais dos produtores de Registros, bem como a pesquisa interesses e capacidades de acesso dos usuários.

Nível	Métricas de Capacidade Comunitária Designada de Nível
0	A organização não possui documentação formal que defina os direitos, obrigações, e responsabilidades da Comunidade Designada para os registros eletrônicos a serem transferidos para ou mantido por um repositório de preservação.
1	A organização tem acordos ad hoc com produtores de discos selecionados que apóiam o transferência de registros eletrônicos para um repositório de preservação.
2	A organização tem acordos formais e escritos com alguns poucos produtores de registros que apoiam a transferência de SIPs substitutos e se estende proativamente para selecionar usuários para identificar suas necessidades e exigências específicas de acesso aos registros eletrônicos sob sua custódia.
	Conformidade com a ISO 14721
3	A organização se envolve com a maioria dos produtores de registros em seu domínio mandatado para estabelecer acordos escritos sobre seus direitos, obrigações e responsabilidades de transferência dos Pacotes de Informações de Submissão (SIPs) para o repositório de preservação. A organização trabalha de perto com a maioria dos usuários para estabelecer perfis DIP que atendam às suas necessidades e exigências.
4	A organização engaja ativamente todos os produtores de registros em seu domínio mandatado para estabelecer acordos escritos sobre seus direitos, obrigações e responsabilidades pela transferência de PIS. Os perfis de conformidade dos PIS são regularmente revisados e atualizados para levar em conta mudando as práticas comerciais dos produtores de Registros. A organização trabalha em estreita colaboração com todos usuários para estabelecer perfis DIP que atendam às suas necessidades e exigências em evolução.

8. Levantamento de Registros Eletrônicos

Todas as organizações públicas e privadas são responsáveis pelos registros criados, recebidos ou adquiridos que são provas de suas atividades comerciais, independentemente do formato ou da mídia utilizada. Eles têm a obrigação de assegurar a

autenticidade, integridade, usabilidade e confiabilidade dos registros, durante o tempo que for necessário.

Registros com requisitos de retenção em longo prazo ou valor permanente eram tradicionalmente transferidos de uma área ou unidade de operações para a custódia de uma Administração de Registros e/ou Arquivos centralizada função de preservação. Em razão da fragilidade dos registros eletrônicos, as organizações são aconselhadas a tratar proativamente a preservação digital tão próxima do momento da criação ou captura de registros eletrônicos como praticável. Isso é especialmente importante para registros operacionais de longo prazo, ou seja, registros que permanecem na custódia da unidade de operações e são considerados registros "ativos".

Uma maneira eficaz de realizar a preservação pró-ativa é manter um inventário abrangente de registros e sistemas eletrônicos, bem como as relações de trabalho colaborativo entre as partes interessadas que incluem produtores de registros, Jurídico/Compliance, Arquivos, Gerenciamento de Registros, Informação Serviços/Tecnologia e aplicações, soluções e prestadores de serviços de terceiros.

Uma característica chave da conformidade dos repositórios digitais ISO 14721 é a confiança na tecnologia de padrão aberto formatos neutros. Durante o processo de ingestão, os registros eletrônicos em formatos proprietários são transformados em formatos de preservação preferenciais que a organização e/ou repositório adotou. Ao longo do tempo e com volumes crescentes de registros eletrônicos, a transformação do formato, durante o processo de ingestão pode se tornar um fardo. Essa obrigação pode ser mitigada em parte se os registros de "preservação pronta", ou seja, registros que estão em formatos interoperáveis padrão aberto, neutros em termos de tecnologia, são feitos em ou perto de os produtores de registros de tempo criam ou capturam os registros.

O objetivo de uma Pesquisa de Registros Eletrônicos é identificar três grandes categorias de registros eletrônicos com requisitos de retenção de dez (10) anos ou mais, a fim de apoiar o planejamento e a preservação de atividades:

-Registros eletrônicos "Preservação Prontos".

-Registros "Quase Prontos para Preservação", ou seja, registros eletrônicos em formatos para os quais as ferramentas estão disponíveis que pode exportar documentos em formato nativo para tecnologia interoperável padrão aberta formatos neutros. Um exemplo é

o Microsoft Word 2007 que contém uma ferramenta para transformar o Word documentos em formato PDF/A.

-Registros "Legados", ou seja, registros eletrônicos em um formato nativo próprio para o qual não há exportação ferramentas existem. Transformação de formatos nativos proprietários em padrões abertos, interoperáveis e formatos tecnologicamente neutros é provável que seja necessário escrever código para suportar essa transformação, o que, por sua vez, pode ser caro. A coleta e análise de dados para uma Pesquisa de Registros Eletrônicos pode ser realizada por uma variedade de meios, incluindo pesquisas via web com produtores de registros, entrevistas com unidades de negócios selecionadas ou terceiros que rotineiramente criam, recebem ou adquirem registros eletrônicos, revisão da retenção de registros e programação da disposição, análise do portfólio de tecnologia da informação da organização, assim como o uso de mecanismos de busca e algoritmos para identificar formatos de arquivo específicos atualmente utilizados na captura e armazenamento de registros eletrônicos em drives de rede.

As descrições de capacidade para a Pesquisa de Registros Eletrônicos são fornecidas abaixo.

Nível	Métricas de Capacidade de Levantamento de Registros Eletrônicos de Nível
0	A organização tem pouca ou nenhuma capacidade ou recursos para coletar e analisar informações sobre o volume, localização, mídia, tipos de formato e requisitos de gerenciamento do ciclo de vida para registros eletrônicos.
1	A organização usa os cronogramas de retenção existentes para identificar os registros eletrônicos de valor histórico, fiscal e legal permanente na custódia dos produtores de registros. Pode também conduzir entrevistas e pesquisas pontuais e pontuais para identificar outros registros eletrônicos de valor histórico, fiscal e legal permanente.
2	A organização utiliza entrevistas sistemáticas, pesquisas e análises retrospectivas de cronogramas de retenção para identificar registros eletrônicos de registros históricos, fiscais e legais permanentes valor na custódia de produtores de discos selecionados. Este esforço pode ser aprimorado focalizando em registros eletrônicos "em risco" identificados.
	Conformidade ISO 14721
3	A organização complementa a análise dos registros eletrônicos "em risco" através da coleta de informações sobre o volume e localização, mídia e tipos de formato (preservação pronta e quase pronta para conservação) de registros eletrônicos permanentes na custódia dos registros produtores.
4	A organização identificou e categorizou todas as conservas prontas, quase conservadas prontos, e registros eletrônicos permanentes legados na custódia de todos os produtores de registros.

Serviços de Preservação Digital: Componentes 9- 15

O DPCMM foi projetado para organizações e repositórios encarregados da preservação de longo prazo e registros eletrônicos permanentes, para comparar suas

capacidades com as especificações da ISO 14721, ISO 16363 e a comunidade de preservação digital aceitaram práticas baseadas no mapeamento dessas capacidades para as métricas de desempenho DPCMM. A DPCMM usa métricas de desempenho para distinguir entre capacidades que elevam o nível de conformidade OAIS (ISO 14721) e infraestrutura de preservação digital e serviços que não estão em total conformidade.

Um corolário da diferenciação entre as métricas de desempenho substituto e, totalmente, em conformidade é a conceito de "propriedades e ações significativas" associadas aos pacotes de informação OAIS (Pacotes de Submissão de Informação - SIPs, Pacotes de Informação de Arquivo - AIPs, e Pacotes de Divulgação de Informação - DIPs) que são críticos para a preservação de produtos acessíveis, utilizáveis, compreensíveis e registros eletrônicos confiáveis em longo prazo e permanentes. "Propriedades significativas" são metadados de preservação enquanto as ações são tarefas de preservação digital que devem ser executadas.

As propriedades estão organizadas em categorias:
Administração (ADM)
Técnica (TEC)
Proveniência (PRO)
Descrição da Preservação (PRE)
Descrição do conteúdo (CON)
Informações sobre embalagens (PAC)
Acesso (ACC)

9. Admissão

Um repositório de preservação que está em conformidade com as especificações funcionais da ISO 14721 e com as melhores práticas têm a capacidade de ingerir (receber e aceitar), sistematicamente, registros eletrônicos dos produtores de registros, na forma de Pacotes de Informação de Submissão (SIPs).

O repositório de preservação aceita SIPs de produtores de registros, valida os acordos e a integridade do conteúdo digital, move os SIPs para uma área de preparação onde verificações de vírus e conteúdo e formato são realizadas e validadas, os registros eletrônicos são transformados em formatos de preservação designados como apropriado, metadados dos SIPs são extraídos e os escreve para Informação de Descrição para Preservação (PDI), cria Pacotes de Informações de Arquivo (AIPs) e transfere os AIPs para a função de armazenamento do repositório.

Nível	Métricas de capacidade de invenção de nível
0	A organização não possui um repositório de preservação digital capaz de receber ou ingerir registros eletrônicos permanentes e de longo prazo.
1	O repositório de preservação recebe registros eletrônicos dos produtores de registros com base em anúncios acordos pontuais sem considerar o formato, integridade, verificações de vírus e qualidade de metadados. Nada disto se eleva ao nível de um SIP em conformidade com a ISO 14721.
2	O repositório recebe SIPs substitutos que são mantidos em uma área de preparação enquanto a presença de vírus é verificada e as validações de formato são executadas manualmente. Os AIPs substitutos são criados manualmente e transferido para o armazenamento de arquivos.
	Conformidade ISO 14721
3	O repositório de preservação injeta SIPs através de meios semi-automatizados que validam a completude das propriedades significativas da Administração, Técnica, Proveniência, Descrição do Conteúdo e Descrição de Preservação. As propriedades significativas são extraídas dos SIPs e escritas para a Informação de Descrição para Preservação (PDI). Os Pacotes de Informação de Arquivo (AIPs) são criados e transferidos para a função de armazenamento do repositório.
4	O repositório de preservação injeta SIPs através de meios automatizados que validam a completude das propriedades significativas da Administração, Técnica, Proveniência, Descrição do Conteúdo e Descrição de Preservação. As propriedades significativas são extraídas dos SIPs e escritas para Informação de Descrição para Preservação (PDI). Os Pacotes de Informação de Arquivo (AIPs) são criados e transferidos para a função de armazenamento do repositório.

10. Armazenamento de arquivos

O modelo de referência do sistema de informação de arquivo aberto ISO 14721 delineia uma série de serviços de armazenamento automatizado que apoiam o recebimento e validação de transferência bem sucedida de AIPs de ingest, criação de Informações de Descrição de Preservação (PDI) para cada AIP que confirma sua fixidez (ou seja, não corrupção ocorreu) durante qualquer ação de preservação, por meio da captura e manutenção do erro logs, atualizações no PDI, incluindo a transformação (ou seja, migração) de registros eletrônicos para novos formatos, múltiplas instâncias de repositórios geograficamente separados, produção de Informações de Divulgação Pacotes (DIPs) para acesso, e coleta de estatísticas operacionais.

O armazenamento de arquivos depende de outros serviços de preservação representados no modelo de maturidade da capacidade incluindo Renovação de Dispositivos/Mídia, Integridade e Proteções de Segurança, e sobre a disponibilidade e aplicação dos padrões de Metadados de Preservação.

Nível	Métricas de Capacidade de Armazenamento de Nível de Arquivo
0	O repositório de preservação ou não acessa registros eletrônicos ou seu acervo consistem de armazenamento de arquivos primitivos (por exemplo, uma unidade compartilhada ou CDs/DVDs) onde ele está disponível.
1	Uma única instância de um repositório de preservação suporta o armazenamento de AIPs de substituição com metadados limitados que podem ser mapeados para Informações de Descrição de Preservação (PDI).
2	Uma única instância de um repositório de preservação de substitutos suporta o armazenamento de substitutos AIPs que incluem a captura manual de algumas propriedades significativas da Administração, Informações técnicas, de Proveniência e de Conteúdo, e ações de preservação repetíveis.
	Conformidade ISO 14721
3	Uma única instância de um repositório de preservação suporta o armazenamento de AIPs. Semiautomatizado ferramentas confirmam a completude de propriedades significativas e capturam todas propriedades de ações de preservação repetíveis. Os resultados são transferidos para Preservação Descrição Informação, que constitui uma cadeia auditável de custódia eletrônica.
4	Duas ou mais instâncias geograficamente separadas de um repositório de preservação apoiam o armazenamento de AIPs. As ferramentas automatizadas confirmam a completude de propriedades significativas e captura de todas as propriedades de ações de preservação repetíveis. Os resultados são transferidos para Descrição da Preservação Informação, que constitui uma cadeia auditável de informações eletrônicas custódia. A captura do armazenamento do repositório de preservação e as estatísticas operacionais suportam a planejamento abrangente de preservação digital.

11. Renovação de Mídia/Dispositivo

Não há nenhum dispositivo digital ou meio de armazenamento conhecido que seja invulnerável à decadência e obsolescência. A capacidade básica de preservação digital para uma organização que tem a responsabilidade de preservar registros eletrônicos de valor permanente e, em longo prazo, garante a legibilidade dos fluxos de *bits* subjacentes aos registros eletrônicos. A ISO 14721 especifica que o armazenamento de um dispositivo e meios de armazenamento de repositórios digitais de confiança devem ser monitorados e renovados ("réplica"/"reembalagem"), periodicamente, para garantir que os fluxos de *bits* permaneçam legíveis ao longo do tempo.

A decomposição dos meios de armazenamento magnéticos e óticos é inevitável. Testes de envelhecimento acelerado predizem que a maioria dos meios magnéticos e ópticos de armazenamento têm uma expectativa de vida útil de 100 anos ou mais, se armazenados em um ambiente controlado. No entanto, a expectativa de vida prevista de centenas ou mesmo milhares de anos para a mídia é de pouco benefício prático, porque a questão fundamental em dispositivos e meios de armazenamento para a preservação é a obsolescência da tecnologia. É provável que isto ocorra quando:

- Há uma mudança no fator da forma física (por exemplo, de bobinas de 10,5 polegadas de fita magnética para cartuchos de fita).

- Há uma mudança no método de codificação física da informação na superfície de gravação que torna impossível a transferência de conteúdo eletrônico de uma fita obsoleta ou unidade de disco para um contemporâneo.
- Um fornecedor decide descontinuar um produto.
- Um sistema legado ou aplicação é desativado sem exportar registros eletrônicos para o novo ambiente computacional.

Um repositório de preservação deve suportar um programa robusto de renovação de dispositivos/armazenamento de mídia. Dependendo dos recursos disponíveis, este programa de renovação pode variar de dispositivos/armazenamento não rede de armazenamento para baseados em rede local, a terceiros externos que fornecem serviços de armazenamento que incluem renovação de dispositivos/armazenamento de mídia. Independentemente de como e quando ocorre a renovação do dispositivo/armazenamento, um requisito crítico é que um protocolo que obriga a captura e preservação dos resultados da validação periódica da integridade dos registros eletrônicos antes e depois da conclusão da renovação do dispositivo/armazenamento digital.

As descrições de capacidade para a renovação de mídia/dispositivo são fornecidas na página seguinte.

Nível	Métricas de capacidade de renovação de mídia/dispositivo de nível
0	O repositório de preservação não tem dispositivo formal e protocolo de renovação de mídia em vigor.
1	O repositório de preservação exige a renovação do dispositivo/recuperação da mídia quando eles estão a ponto de tornando-se obsoletos.
2	O repositório de preservação exige a renovação de dispositivos/meios de comunicação em uma base regularmente programada (por exemplo, a cada dez anos).
	Conformidade ISO 14721
3	O dispositivo atual e o programa de renovação da mídia apoiam uma inspeção anual da mídia que identifica os meios de armazenamento do repositório de preservação diante de catástrofes iminentes perda de dados e executam a renovação de dispositivos/meios de comunicação, conforme apropriado.
4	O dispositivo atual e o programa de renovação de mídia monitoram continuamente a perda potencial da legibilidade dos registros eletrônicos e substitui automaticamente os dispositivos/meios de armazenamento e grava os registros em novas mídias de armazenamento, conforme apropriado.

12. Integridade

Uma capacidade chave em conformidade com os repositórios de preservação ISO 14721 é garantir a integridade ("fixidez") de registros em sua custódia. Alterações acidentais ou intencionais podem ocorrer, durante a renovação do dispositivo/mídia, transferências internas de dados, e outras ações de preservação. Uma maneira de

estabelecer a integridade é por meio do uso de resumos criptográficos de *hash* que são impressões digitais de registros eletrônicos em um SIP, um AIP ou alguma agregação deles.

Um resumo criptográfico de hash computado antes de uma operação de preservação digital e após sua conclusão detectará qualquer mudança, mesmo que seja mínima. Os resumos de hash são armazenados em Informações de Descrição de Preservação (PDI) onde podem ser revistas para confirmar que não ocorreram mudanças, durante renovação de dispositivos / mediais, transferências internas de dados e outras ações de preservação, apoiando assim uma cadeia inquebrável de custódia eletrônica. A força dos resumos de *hash* varia, sendo os mais baixos MD5 e o mais alto é o SHA-3.

Os resumos de hash não suportam a cadeia de custódia eletrônica, quando a ação de preservação envolve transformação de formato, porque os fluxos de bits subjacentes dos registros digitais transformados não corresponderão os fluxos de bits antes de serem transformados. No entanto, isso pode ser compensado com o coleta de informações sobre todas as ações de preservação empreendidas em relação às AIPs e armazenando essas informações na AIP Informação de Descrição de Preservação. A afixação de uma assinatura digital nas AIPs encapsuladas em XML após cada ação de preservação também fornece uma forte cadeia eletrônica de custódia.

Nível	Métricas de Capacidade de Integridade de Nível
0	O repositório de preservação não tem procedimento documentado para a proteção da integridade de registros eletrônicos em sua custódia.
1	O repositório de preservação gera e preserva os resumos de hash MD-5 de registros eletrônicos antes e depois da renovação do dispositivo/mídia e outras ações de preservação do armazenamento de arquivos.
2	O repositório de preservação gera e preserva os resumos de hash SHA-1 antes e depois de renovação de dispositivos/mídia e outras ações de preservação interna.
	Conformidade ISO 14721
3	O repositório de preservação gera e valida os resumos de hash SHA-2 antes e depois de todas as ações repetíveis de preservação de propriedades significativas de preservação para AIPs por meio de semi-automatização e os armazena em Informações de Descrição de Preservação (PDI).
4	O repositório de preservação gera e valida os resumos de hash SHA-2 antes e depois todas as ações repetíveis de preservação de propriedades significativas de preservação para AIPs através de meios automatizados, encapsula-os em XML, e os assina com uma assinatura digital. Procedimentos de proteção de Integridade são continuamente avaliados e atualizados como novas ferramentas e se tornam disponíveis.

13. Segurança

A preservação digital requer processos que restrinjam o acesso ao repositório físico onde o conteúdo digital é armazenado, garantam a segurança dos registros eletrônicos através de técnicas que bloqueiam acesso, protejam a confidencialidade e a

privacidade dos registros e direitos de propriedade intelectual, apoiem o backup periódico de registros eletrônicos que são armazenados em repositórios de armazenamento fora do local, e suportem a recuperação de desastres e continuidade dos negócios.

Nível	Métricas de Capacidade de Segurança de Nível
0	O repositório de preservação não possui recuperação formal de desastres procedimentos de backups ou firewall em vigor para proteger a segurança dos registros eletrônicos.
1	O repositório de preservação suporta a segurança dos registros eletrônicos em sua custódia através de procedimentos de recuperação de desastres.
2	O repositório de preservação suporta a segurança dos registros eletrônicos em sua custódia através de uma proteção abrangente de firewall.
	Conformidade ISO 14721
3	O repositório de preservação suporta a segurança dos registros eletrônicos em sua custódia através de gestão abrangente baseada em direitos de acesso.
4	O repositório de preservação suporta a segurança dos registros eletrônicos em sua custódia por monitoramento contínuo dos processos de proteção de segurança e sua revisão em resposta a evolução das capacidades tecnológicas e mudanças nas exigências comerciais.

14. Metadados de Preservação

Um repositório de preservação coleta e mantém metadados que descrevem as ações de preservação associadas à custódia de registros eletrônicos permanentes. Os metadados de preservação incluem uma trilha de auditoria que as ações de preservação de documentos realizadas, por que e quando foram realizadas, como foram realizadas e com que resultados.

Uma melhor prática atual é o uso de um esquema de metadados de preservação baseado em PREMIS para todos os registros eletrônicos, para suportar uma cadeia de custódia eletrônica que documenta a autenticidade, ao longo do tempo como ações de preservação são executadas. Captura de todos os metadados relacionados, transferência dos metadados para qualquer novo formatos/sistemas, e o armazenamento seguro de metadados é fundamental. Todos esses metadados associados são armazenados em as Informações de Descrição de Preservação (PDI) e logicamente mapeados para AIPs.

Nível	Métricas de Capacidade de Preservação de Nível de Metadados
0	Um repositório de preservação primitivo tem poucos ou nenhuns metadados de preservação para registros em sua custódia.
1	O repositório de preservação suporta um esquema de metadados de preservação ad hoc e estabelece uma cadeia mínima de custódia para registros eletrônicos em sua custódia.
2	O repositório de preservação suporta um esquema PREMIS substituto para os registros eletrônicos em sua custódia que suporta uma cadeia de custódia limitada.
	Conformidade ISO 14721
3	O repositório de preservação suporta um esquema semi-automatizado baseado no PREMIS para a maioria registros eletrônicos em sua custódia que suportam uma

	sistemática cadeia de custódia auditável.
4	O repositório de preservação suporta um esquema PREMIS automatizado para todos os sistemas eletrônicos registros em sua custódia que suportam uma sistemática cadeia de custódia auditável.

15. Acesso

O objetivo da preservação digital é garantir que os registros eletrônicos sejam utilizáveis, compreensíveis, confiáveis e acessíveis no futuro, sujeitos a quaisquer restrições impostas pelos produtores de registros. Consequentemente, as comunidades de usuários devem ter acesso a Pacotes de Disseminação de Informação (DIPs) derivados dos Pacotes de Informação de Arquivo (AIPs) que um repositório digital confiável, depósito devidamente conserva. Em alguns casos, o repositório pode colocar DIPs irrestritos em seu website. Com base nas expectativas e interesses dos usuários, o repositório pode optar por limitar as "propriedades significativas e ações associadas" incluídas nos DIPs com o entendimento de que elas estarão disponíveis se solicitadas.

Essa capacidade de acesso pode incluir a criação e manutenção de metadados pesquisáveis pelo usuário que podem ser consultadas para identificar informações de interesse e de livre divulgação (redatadas para proteger a privacidade, confidencialidade, e outros direitos, quando apropriado). Em nenhum caso, os usuários terão acesso direto a Pacotes de Informações de Arquivo (AIPs) ou Informações de Descrição de Preservação.

Nível	Métricas de Capacidade de Acesso de Nível
0	O repositório de preservação ou não tem registros eletrônicos em sua custódia ou não tem capacidade de suportar o acesso a registros eletrônicos em sua custódia.
1	O repositório de preservação suporta o acesso a registros eletrônicos em um único formato (por exemplo, JPEG ou PDF) enquanto aplica todas as restrições de acesso.
2	O repositório de preservação suporta o acesso a registros eletrônicos em pelo menos três formatos de arquivos com padrão aberto de tecnologia neutra (por exemplo, PDF/A, JPEG e TIFF), enquanto aplica todas as restrições de acesso.
	Conformidade ISO 14721
3	O repositório de preservação tem uma robusta funcionalidade de busca integrada que suporta produção semiautomatizada de DIPs juntamente com suas propriedades significativas associadas. Documentação auditável para a produção de DIPs é capturada e as tendências de consulta do usuário são usadas para identificar a necessidade de ferramentas de acessibilidade atualizadas.
4	O repositório de preservação tem uma robusta funcionalidade de busca integrada que suporta produção automatizada de DIPs e suas propriedades significativas associadas. Consultas do usuário são utilizadas para identificar a necessidade de ferramentas de acessibilidade atualizadas e auditar os resultados da produção de DIPs.

APÊNDICE F - *INTO THE ARCHIVE* - UM GUIA PARA A TRANSFERÊNCIA DE INFORMAÇÕES PARA UM REPOSITÓRIO DIGITAL [132]

Into the Archive é, de acordo com Caplan, Pawletko, Kehoe (2009), um guia produzido na Alemanha pelo Grupo de trabalho NESTOR, sobre normas de preservação em longo prazo. Seu objetivo é semelhante ao de PAIMAS, mas é mais curto e mais simples, e de uma forma mais prática do que orientação teórica. Assim como PAIMAS, o Guia NESTOR estipula que o produtor e o arquivo elaborem um acordo vinculativo sobre o Ingest. Quanto aos objetivos, NESTOR (2009) orienta que:

> Dentro do Arquivo visa esclarecer os objetivos e os aspectos únicos da ingestão de informações em um sistema de repositório digital: os dados precisam ser transferidos de um repositório geralmente heterogêneo e contextos organizacionais específicos, de tal forma que, mesmo assim, permanecerá compreensível e utilizável em contextos completamente diferentes no futuro[133] (NESTOR, 2009, p. 2. Tradução nossa).

O Guia *Into Archive orienta que* as comunidades designadas incluem:

-Instituições de memória que, junto com os produtores de informação ou as instituições provedoras de informação, desejam realizar uma transferência e precisam de uma base comum para iniciá-la.

-Produtores de informação ou instituições provedoras de informação que desejam submeter seus objetos de informação a um repositório digital para preservação de longo prazo e estão procurando informações sobre as tarefas futuras.

-Instituições de memória que possuem uma infraestrutura de preservação de longo prazo e agora estão prestes a ingerir informações pela primeira vez.

-Instituições de memória que estão planejando uma infraestrutura de preservação de longo prazo e que, portanto, estão abordando a questão da ingestão.

Objetos

Seleção de informações a serem arquivadas

O repositório digital deve selecionar as entidades intelectuais a serem ingeridas. Para instituições públicas, a seleção das informações a serem arquivadas com base no conteúdo deriva, geralmente, da missão da instituição. O repositório digital tem que tomar as decisões técnicas necessárias sobre a seleção em colaboração com o produtor. Isso envolve, principalmente, a seleção e o acordo sobre os formatos de arquivo adequados para a preservação de longo prazo, que são necessários para a representação de objetos de informação no sistema de arquivo digital, e também a seleção dos formatos de metadados necessários.

Em alguns casos, as funções de exportação padrão dos sistemas de produção não são capazes de exportar os objetos de informação na forma desejada pelo repositório digital. O sistema do produtor deve então ser estendido por seu fornecedor para atender aos requisitos adicionais, que geralmente são muito caros. Todo o processo de ingestão é mais simples e barato para o produtor e para o arquivo, se funções de exportação adequadas ou interfaces de arquivo já forem levadas em consideração e implementadas quando os sistemas eletrônicos estiverem sendo planejados e adquiridos. O repositório digital deve, portanto, ser informado sobre a aquisição de um novo sistema de computador, desde o estágio inicial e ser envolvido em seu projeto e planejamento.

Objetivo: A partir do material fornecido pelo produtor, o repositório digital deve selecionar as entidades intelectuais que serão ingeridas de forma permanente, imutável e segura como objetos de arquivo. Esta seleção é baseada em critérios de avaliação específicos resultantes do mandato legal ou contratualmente definido de um repositório digital.
Procedimento: Os repositórios digitais coletam informações que podem ser lidas e interpretadas por pessoas e que são armazenadas em formato digital. Nesse nível de conteúdo, é permitido usar terminologia derivada da experiência cotidiana no manuseio de objetos de informação (por exemplo, documentos, arquivos, filmes, fotos, banco de dados do Escritório Federal de Estatísticas etc.). Naturalmente, definir o estoque de arquivo primário tem consequências no nível técnico.

Objetivo: O repositório digital e o produtor devem analisar as possibilidades da interface de exportação do sistema produtor. Se, após a exportação, os dados não estiverem disponíveis de uma forma que o repositório digital possa tornar acessível de forma permanente, medidas adequadas (por exemplo, conversão) são planejadas.
Procedimento: Os dados por si só não constituem um objeto de informação que possa ser lido e interpretado por seres humanos. Ele contém informações codificadas que precisam ser interpretadas corretamente e representadas por um ambiente de hardware / software adequado. O equipamento técnico necessário para a apresentação de certos objetos de informação pode ser muito caro. Isso pode ser devido aos custos envolvidos na aquisição do equipamento técnico necessário e na sua manutenção, ou resultar da vida útil limitada do equipamento. Se o repositório digital não vê possibilidade de ser capaz de garantir a representação dos objetos de informação na forma oferecida pela interface de exportação, o arquivo e o produtor terão de negociar formatos alternativos para os objetos de informação.

Objetivo: Deve haver acordo entre o arquivo e o produtor quanto às adaptações necessárias, caso os objetos de informação não possam ser arquivados em sua forma existente.
Procedimento: O repositório digital e o produtor podem ser obrigados a submeter os objetos de informação, a ingeri-los e a preservá-los no longo prazo. A rejeição geral da ingestão devido à falta de instalações técnicas por parte do arquivo não é uma opção neste caso. Os dados são alterados em caso de migração. As propriedades significativas da entidade intelectual devem permanecer intactas, no entanto, apesar de quaisquer alterações. A seleção de um formato de dados que seja capaz de preservar as propriedades significativas do formato original e que também seja adequado para a preservação de longo prazo no arquivo é uma das decisões críticas na preservação digital de longo prazo. O formato de destino deve ser aberto e bem documentado. A representação deve ser possível com significativamente menos equipamento técnico do que o exigido pelo formato original. Migrar dados para um formato diferente representa uma tarefa adicional que apresenta seus próprios riscos. O produtor e o arquivo devem esclarecer quem deve assumir quais responsabilidades e quais custos. A seleção da tecnologia necessária para realizar a migração pode ter um impacto significativo na qualidade dos objetos de informação e no custo de ingestão. Os programas de conversão que pretendem criar o mesmo formato de destino não produzem necessariamente resultados idênticos. Eles podem usar tecnologias completamente diferentes (por exemplo, algoritmos de compressão), todas as quais estão em conformidade com a definição de formato, ou implantar métodos proprietários sem declarar isso expressamente. A emulação ou suplementos ao ambiente de software / hardware do repositório digital são outras opções possíveis além da migração para apresentar os objetos de informação ingeridos.

Seleção de metadados

De acordo com o padrão OAIS, a ingestão não está completa até que um "pacote de informações de arquivamento" (AIP) completo tenha sido criado. Os principais

constituintes de um AIP são o próprio objeto de conteúdo mais os metadados. Ambos são necessários para fornecer, de forma permanente, informações suficientes sobre o objeto de arquivo (AIP), ou seja, permitir que ele seja encontrado, apresentado e compreendido e interpretado em contexto com outros objetos de arquivo.

Crucial para a preservação, em longo prazo é a informação que ajuda entidades intelectuais (por exemplo, artigos de revistas, arquivos, fotos etc.) a serem criadas a partir de objetos de informação que podem ser interpretados por seres humanos. Essa informação deve conter referências aos ambientes técnicos necessários para apresentação, deve identificar o formato dos dados tão claramente quanto possível (por exemplo, nome do formato do arquivo e versão) e deve, pelo menos, conter uma referência a uma descrição técnica abrangente do formato do arquivo (por exemplo, padrão ISO, RFC, registro de formato de arquivo). No caso de objetos de informação complexos que consistem em vários arquivos, a estrutura do objeto de informação deve ser descrita de maneira compreensível. Somados a isso, estão os metadados necessários para o gerenciamento técnico dos dados na memória, como o nome do arquivo,

Também são necessários metadados que descrevam o conteúdo (por exemplo, autor e título no caso de publicações) de um objeto de arquivo (AIP), e também a origem de um objeto de arquivo (por exemplo, informações que indicam de qual pessoa de qual autoridade submeteu um arquivo eletrônico ao arquivo a que horas). Um outro fator importante para a preservação digital confiável são as informações sobre as mudanças nos objetos de informação que são feitas quando são exportados do sistema do produtor. O quão detalhadas essas informações são representadas nos metadados depende das necessidades do arquivo e do produtor e do tipo de objetos de informação que estão sendo ingeridos.

Nem todos os tipos de metadados descritos acima existem, imediatamente após um objeto de informação ser exportado do sistema de um produtor. Alguns metadados são gerados, apenas, durante a inserção no arquivo e alguns devem ser solicitados ao produtor. Por essa razão, antes de definir um pacote de transferência, o arquivo deve decidir quais informações requer tanto do produtor quanto do sistema do produtor.

Objetivo:
O repositório digital e o produtor devem definir todos os metadados exigidos nos objetos de informação selecionados no AIP. O resultado é uma seleção de todas as informações necessárias para criar um AIP suficientemente abrangente.

Procedimento:

As informações sobre a tecnologia necessária e os vínculos estruturais entre os arquivos de objetos de informação são necessárias para a representação autêntica e de longo prazo dos objetos de informação. Informações para descrever o conteúdo semântico e o contexto do objeto de informação também são necessárias. Deve ser considerada toda uma gama de diferentes tipos de metadados a serem fornecidos pelo produtor. Além dos metadados-padrão usados para descrever o conteúdo, e dos metadados estruturais já mencionados, também podem ser metadados técnicos e de administração.

Os formatos de metadados também podem ser distinguidos por critérios baseados em conteúdo, por exemplo, metadados descritivos de conteúdo (no campo das bibliotecas: metadados bibliográficos), metadados técnicos e metadados jurídicos. Existem padrões específicos para metadados de descrição de conteúdo, como MAB2 e MARC21 para o setor de bibliotecas e padrões gerais, como Dublin Core. Dublin Core pode ser estendido na forma de perfis, portanto os parceiros devem concordar em usar apenas Dublin Core Simple ou um perfil específico. Para metadados técnicos e estruturais, existem PREMIS, METS, LMER.

O seguinte está incorporado no modelo OAIS para metadados de administração:
- Proveniência: quem fez o quê e quando? A história de um objeto.
- Contexto: as relações do conteúdo fora do pacote. Por que foi produzido, que relação tem com outros conteúdos e embalagens?
- Referência: Identificador: Cadeias de caracteres numéricos ou alfanuméricos que referenciam exclusivamente as entidades intelectuais e também os objetos de informação relacionados e os identificam dentro do arquivo.
- Fixidade: Proteção contra mudanças não autorizadas, por exemplo, somas de verificação.

Objetivo:
O repositório digital e o produtor devem chegar a um acordo sobre quem fornecerá os metadados necessários.

Procedimento:

Nem todos os metadados necessários precisam ser fornecidos pelo produtor e enviados ao repositório digital. Faz mais sentido se a descrição da tecnologia necessária para exibir um objeto de informação no arquivo for fornecida pelo próprio arquivo. Se o produtor migra os objetos de informação para o formato de arquivo PDF / A antes de transferi-los para o arquivo, isso gera metadados que descrevem o processo de migração do produtor e que também devem ser inseridos no arquivo. Quando o arquivo verifica se os arquivos PDF / A enviados estão em conformidade com o padrão, isso resulta em mais metadados - desta vez no arquivo - que podem ser integrados ao AIP.

Identificação de propriedades significativas das entidades intelectuais e dos objetos de informação

A fim de manter as entidades intelectuais mantidas em formatos digitais acessíveis, por longos períodos de tempo, os objetos de informação devem ser representados em ambientes técnicos em mudança. As características dos dados, certamente mudarão, independentemente de a estratégia de preservação ser baseada em emulação ou migração. As propriedades significativas são aquelas características que devem permanecer constantes em todas as circunstâncias.

Objetivo: O arquivo e o produtor devem elaborar uma definição das propriedades significativas dos objetos de informação selecionados.
Procedimento: O arquivo e o produtor devem decidir quais desvios de apresentação são aceitáveis e quais não são. As necessidades dos usuários do arquivo (comunidade designada) devem ser o critério principal. O projeto InSPECT lista as subdivisões comuns das propriedades significativas como: " - conteúdo, por exemplo: texto, imagem, slides, etc. - contexto, por exemplo: quem, quando, por quê. - aparência, por exemplo: fonte e tamanho, cor, layout, etc. - estrutura, por exemplo: arquivos incorporados, paginação, títulos, etc. - comportamento, por exemplo: links de hipertexto, cálculos de atualização, links ativos, etc.

Objetivo: Para cada entidade intelectual que o arquivo ingere do produtor, ele deve registrar as propriedades relevantes que devem permanecer permanentemente intactas nos metadados. Essas informações podem ser usadas posteriormente para verificar se uma migração futura ou um novo emulador é adequado para a preservação de longo prazo dos objetos.
Procedimento: É responsabilidade de cada arquivo individual determinar em que forma as propriedades significativas de um objeto são registradas. Valores técnicos rígidos (por exemplo, resolução da imagem, largura da imagem, espaços de cores, etc.) podem ser usados ou a impressão sensorial de uma entidade intelectual pode ser descrita.

Processos

Definição de pacotes de transferência

Uma vez que o repositório digital e o produtor tenham identificado o que deve ser arquivado, deve-se decidir em quais unidades o conteúdo é transferido para o repositório digital: os pacotes de transferência devem ser definidos. Isso determina a relação entre os dados transferidos, os metadados e os objetos de informação, garantindo assim que cada objeto possa ser reconstituído a partir de suas várias partes. Os pacotes de transferência

podem ser formatos de contêineres que contêm as partes constituintes, ou arquivos puramente descritivos que simplesmente fazem referência aos dados e metadados, tornando-os assim disponíveis para o arquivo. Um exemplo de pacote de transferência de contêiner para sites pode ser todos os arquivos e metadados de um site sendo transferidos junto com um arquivo XML descritivo em um arquivo ZIP.

No modelo OAIS, esses pacotes de transferência são chamados de SIPs (Pacotes de Informações de Submissão) e podem diferir dos pacotes de saída estruturados de forma diferente (DIPs, Pacotes de Informações de Disseminação) e pacotes usados internamente (AIPs, Pacotes de Informações de Arquivo) do próprio arquivo. Os pacotes de transferência também se distinguem terminologicamente dos formatos de pacote (que representam o formato técnico dos pacotes de transferência) e dos modelos de objeto (que são usados para transmitir as propriedades lógicas / conceituais dos objetos de informação).

É importante especificar o pacote de transferência, pois os repositórios e produtores digitais não representam, com toda a probabilidade, objetos de informação da mesma maneira. Portanto, é necessária uma definição conjunta do que constitui uma única unidade a ser transferida. Os repositórios digitais geralmente já possuem seus próprios padrões para pacotes de transferência.

Objetivo: A relação entre um objeto de informação e um ou mais pacotes deve ser definida.
Procedimento: Idealmente, um objeto de informação consistirá em um único pacote, pois isso reduz a complexidade. No entanto, por razões técnicas ou outras, essa relação 1: 1 nem sempre é sensata ou viável, o que significa que os objetos de informação geralmente consistem em vários pacotes ou que um pacote contém vários objetos de informação. Por esta razão, é necessário definir um método (incluindo os metadados correspondentes) que estabeleça a relação entre pacotes e objetos de informação. - Pode ser necessário distribuir grandes objetos de informação em vários pacotes diferentes como resultado de limites técnicos de tamanho. - Também pode ser desejável dividir um objeto de informação em um número de pacotes diferentes se os pacotes enviados forem semelhantes aos pacotes de saída eventuais e apenas um único acesso a partes individuais de um objeto de informação é necessário para cenários de uso relevantes. - Se certos dados pertencerem a um grande número de objetos de informação, pode ser mais eficiente transferir um único pacote que é então referenciado por muitos objetos de informação e outros pacotes. Os arquivos de modelo de formato para grandes sites ou coleções de documentos seriam exemplos.

Objetivo: Deve ser possível reconstruir os relacionamentos de dados com base nos metadados estruturais contidos no pacote.
Procedimento: Os dados não são inicialmente relacionados a outros dados ou a seus metadados. O que constitui uma relação relevante para a formação de um objeto de informação depende do ambiente técnico e, portanto, deve ser explicitado. Os arquivos podem ser mantidos em um diretório de arquivos comum ou ser nomeados de acordo com um sistema uniforme, expressando a relação técnica e lógica entre eles. Quando isso não for suficientemente definido por formatos, pode ser necessário descrever explicitamente a relação entre metadados e arquivos de documento ou dependências de arquivos de site em um arquivo de modelo de formato. METS [Ref. 8], LMER [Ref. 9] e PREMIS [Ref. 3] por exemplo, forneça opções adequadas aqui.

Objetivo: Deve ser possível para o produtor e o repositório digital identificar o pacote.
Procedimento: A identificação pode ser fornecida pelo identificador do objeto de informação ou identificadores de pacote de arquivo associados. Lembre-se, no entanto, de que não é necessário haver uma relação 1: 1 entre os pacotes e os objetos de informação. Assim, cada pode precisar de seu próprio identificador. O identificador deve estar contido na embalagem; do ponto de vista técnico, no entanto, a identificação ao nível do protocolo de transferência também é concebível. Identificadores persistentes [Ref. 10] são preferíveis. Os pacotes de arquivos podem ser identificados pelos URNs dos documentos neles contidos. Todos os padrões de metadados conhecidos oferecem possibilidades para isso.

Validação

Em razão da facilidade com que é possível manipular objetos digitais, uma verificação deve ser feita após a transferência, para garantir que eles ainda contenham o que deveriam. A validação também faz parte das outras fases do processo de arquivamento. Basicamente, a validação é necessária após qualquer transferência - para uma instalação diferente, para um novo formato, para um novo suporte de dados. A validação é sempre uma comparação. O objetivo é documentar a autenticidade do objeto (ou seja, o objeto é o que afirma ser) e seu funcionamento correto. É feita uma distinção entre duas categorias de objetivos de comparação associados ao objeto a ser validado:

- O objeto a ser validado é verificado em relação ao seu objeto "pai" (por exemplo, os valores *hash* do arquivo de destino e do arquivo original são comparados após a migração do portador de dados).

- O objeto a ser validado é verificado em termos de suas especificações formais ou de conteúdo (por exemplo, um formato de arquivo é comparado com a descrição do formato).

É possível verificar todo um grupo de objetos, e não apenas um único objeto. No entanto, por razões de simplicidade, a palavra generalizada "objeto" é usada abaixo.

Objetivo: Definição dos processos de validação individuais.
Procedimento: A tarefa de validação pode ser subdividida em etapas ou processos individuais. Um processo é uma verificação para garantir que uma ou mais características do objeto ingerido foram / foram retidas. Isso pode ser feito automaticamente ou manualmente. Os processos devem ser descritos e nomeados, e linhas divisórias claras traçadas entre eles. Por exemplo: - A entrega contém todos os objetos acordados? - Os objetos estão intactos (eles correspondem aos valores de *hash* previamente estabelecidos)? - Os objetos estão livres de vírus? - Os arquivos são válidos / sem erros em relação ao formato de arquivo?

Objetivo: O arquivo deve definir o grau de conformidade exigido para cada processo de validação individual e as consequências da não conformidade.
Procedimento: O objetivo de alguns processos de validação pode ser, simplesmente, determinar o cumprimento / não cumprimento de uma característica (por exemplo, valores *hash*). Em outros casos, são possíveis transições graduais. Nesse caso, os resultados geralmente não atendem mais às expectativas especificadas por completo (por exemplo, nuances de cor). Às vezes, não é possível que o objeto original e o objeto de destino sejam idênticos (por exemplo, após migrações do formato de arquivo). É ainda difícil implementar um padrão (por exemplo, ISO 19005 - PDF / A) por completo. O grau de cumprimento a ser alcançado deve, portanto, ser definido para cada processo. O que deve acontecer se este não for o caso também deve ser definido. Uma consequência poderia ser a rejeição de um objeto e seu retorno ao produtor (junto com a solicitação de envio de um objeto perfeito). Outra opção seria apenas registrar desvios até um nível definido nos metadados do arquivo (em um relatório de validação). PREMIS refere-se a isso como "peculiaridades". Possíveis exemplos de processos de validação com diferentes níveis de cumprimento: - n% entradas com defeito em um campo de banco de dados são toleradas - n% características não documentadas do banco de dados ainda podem ser aceitas

Objetivo: Os indivíduos envolvidos e os equipamentos usados devem ser nomeados para cada processo de validação.
Procedimento: Deve-se primeiro esclarecer quais tarefas são realizadas por quem e quais ferramentas podem ser usadas para cada processo. Por razões metodológicas, a fim de detectar erros relacionados ao método e à ferramenta, também pode ser necessário usar outros métodos e ferramentas de software para validação do que para gerar o pacote de transferência. - Quem realiza a validação: o produtor ou o arquivo? - Há terceiros (especialistas, representantes da comunidade designada) envolvidos? - Quais ferramentas e métodos são usados para a validação? - Onde ocorre a validação (no sistema do produtor ou no arquivo)?

Objetivo: Os processos de validação devem seguir uma sequência cronológica plausível.
Procedimento: Os processos de validação são realizados em fases individuais durante a ingestão. A divisão das fases e o número delas podem diferir de arquivo para arquivo; principalmente, porém, há uma divisão em duas fases. Na primeira fase, é esclarecido se os objetos atendem aos requisitos básicos imediatamente após terem sido incluídos no arquivo. Se houver desvios do resultado esperado, a ingestão dos objetos é rejeitada. Essas características, portanto, têm uma função desqualificadora. Os processos de validação mais detalhados são realizados na segunda fase subsequente. Somente aqui os processos desempenham um papel que não determina um resultado claro sim / não.

Transferência de dados do sistema do produtor

De grande importância para a transferência dos dados do produtor para o repositório digital é a transmissão completa e correta de todos os dados exigidos pelo repositório para reconstruir os objetos de informação relevantes e para a gestão, preservação e acessibilidade de longo prazo das entidades intelectuais. Uma vez que os dados foram transferidos, o repositório digital deve ser capaz de determinar com precisão de quem é a entrega (autenticidade), em que forma os dados e metadados devem ser submetido (validade) e quão grande as entregas de dados devem ser (completude). As condições legais e contratuais são decisivas aqui, podendo variar consoante o caso. Os requisitos legais e a tecnologia usada para a transferência devem ser harmonizados.

Objetivo:
O quadro legal e / ou contratual para uma transferência deve ser analisado e definido pelo produtor e pelo arquivo.

Procedimento:

Os requisitos para uma transferência em relação a aspectos como transferência segura de dados, validade contínua de assinaturas qualificadas, etc. [Ref. 12] [Ref. 13] pode variar. Arquivos entregues por uma agência governamental, por exemplo, podem ter diferentes níveis de confidencialidade.

Objetivo:
O produtor e o arquivo devem estar cientes das possibilidades técnicas e organizacionais disponíveis para a transferência. Ambos devem saber se as instalações técnicas permitem uma transferência conforme os requisitos ou não. Se necessário, deve-se chegar a um acordo sobre os ajustes necessários.

Procedimento:

Ambos os lados devem conhecer suas capacidades técnicas e realizar verificações, especialmente nos casos em que ainda não foi feita nenhuma transferência entre os parceiros. Antes da primeira transferência, em particular, as possibilidades técnicas do produtor e do arquivo podem não estar em conformidade com os requisitos legais. A conformidade deve ser verificada, cuidadosamente, pois as condições de segurança de TI também estão sujeitas a mudanças permanentes. Por exemplo, a criptografia e os protocolos de assinatura qualificados perdem sua eficácia contra a manipulação maliciosa com o tempo.

Objetivo:
As etapas de trabalho individuais da transferência entre o produtor e o arquivo devem ser coordenadas e testadas com precisão.

Procedimento:

O processo de transferência é crítico para a autenticidade do objeto de informação. A adesão exata a um processo de transferência acordado aumenta a confiabilidade do arquivo. No caso de transferências regulares e automáticas, o processo de transferência precisa ser implementado tecnicamente nos sistemas do produtor e do arquivo. O produtor e o arquivo estipulam o tamanho máximo do arquivo para a transferência, concordam com os relatórios técnicos que devem ser criados, o método de transferência (transferência de dados com protocolo, ou em portador de dados com formato de informação fornecido por meio de entrega), o período de tempo da transferência, todos os identificadores e senhas necessários e os protocolos de segurança necessários.

As ferramentas técnicas acordadas devem ser implementadas nos sistemas das instituições parceiras e coordenadas. Por segurança, o produtor e o repositório digital geram em conjunto pacotes de transferência de teste e conduzem testes de transferência controlada. Somente sob condições controladas pode ser determinado se a transferência acordada e implementada está funcionando corretamente.

Gerenciamento

Identificação de condições legais e contratuais

Regulamentações estatutárias entre o produtor e o arquivo devem existir, ou ser criadas, antes que qualquer objeto digital seja inserido no arquivo, a fim de garantir um planejamento de longo prazo e segurança jurídica para ambas as partes. Colocam-se aqui questões jurídicas, que não estão diretamente relacionadas com a ingestão, mas que, no entanto, precisam ser esclarecidas, sobre a ingestão de um objeto para regular a permanência do arquivamento e as condições de manuseio dos objetos arquivados. O esclarecimento de outras questões legais que afetam a relação produtor-arquivo é, portanto, uma pré-condição para uma ingestão eficaz e bem-sucedida. Após a análise da base das relações jurídicas entre o produtor e o arquivo, as questões de direitos autorais são o próximo foco principal nesse campo.

Objetivo: Todas as partes atuando em uma capacidade legal e as pessoas autorizadas a representá-las devem ser identificadas ou nomeadas.
Procedimento: A tarefa de arquivamento deve ser estabelecida em uma base legal, a fim de fornecer segurança jurídica e de planejamento tanto para o produtor quanto para o arquivo. Deve ser esclarecido se tais regulamentos estatutários existem. Se tal base jurídica existe, sua natureza deve ser determinada. Deve ser estabelecido se a atividade de arquivamento é, ou será, baseada em um mandato estatutário ou em um acordo legal entre o arquivo e o produtor. Se não houver base legal na forma de uma obrigação de depósito legal, um acordo (acordo de licença) precisa ser criado entre o produtor e o arquivo, pelo menos no que diz respeito a questões de direitos autorais. Para que o arquivo execute o seu trabalho de forma eficaz, ele deve ter os direitos necessários para o arquivamento planejado e uso na forma de um regulamento legal ou um acordo contratual.

Objetivo: Devem ser conhecidas as obrigações do arquivo e / ou produtor com relação ao manuseio do material a ser arquivado.
Procedimento: Deve ser determinado se os requisitos vinculativos relativos ao armazenamento e uso dos objetos a serem arquivados, ou seu conteúdo, derivam dos regulamentos legais. Uma lei de arquivo pode, por exemplo, especificar quantas cópias de um objeto devem ser armazenadas no arquivo e se o produtor deve deletar os documentos originais. Além disso, é possível que os requisitos de proteção de dados possam impedir uma pesquisa abrangente dos estoques de arquivos ou o fornecimento de material de arquivo a terceiros. As possíveis responsabilidades legalmente regulamentadas por parte do produtor podem incluir a obrigação de oferecer ou entregar os objetos digitais ao arquivo. A distribuição dos custos também deve ser regulamentada legalmente, incluindo o transporte para o arquivo, os custos de arquivamento e cuidados, e os custos de geração de cópias em nome do produtor.

Objetivo:
O arquivo deve estar ciente das condições de direitos autorais associados ao material a ser arquivado e registrá-los permanentemente.

Procedimento:

Os direitos do proprietário dos direitos autorais do objeto a ser arquivado devem ser esclarecidos. Sob certas circunstâncias, o material a ser arquivado pode estar sujeito a direitos de propriedade intelectual. Se as regulamentações relevantes se aplicarem, o arquivamento digital só é permitido na Alemanha em circunstâncias altamente restritas, pois o arquivamento de objetos digitais sempre inclui a duplicação, conforme definido na Lei de Direitos Autorais (UrhG). Essa duplicação deve sempre ser coberta por um regulamento correspondente da Lei de Direitos Autorais ou pela transferência dos direitos de uso relevantes do proprietário dos direitos para o repositório digital.

Na Alemanha, as disposições da Lei de Direitos Autorais (UrhG) só se aplicam se uma obra tiver um certo limite de originalidade e se enquadrar no período de proteção legalmente definido. Um regulamento de propriedade está contido no art. 53 da Lei Alemã de Direitos Autorais, o chamado regulamento de arquivo, que permite a duplicação para fins de transferência para o arquivo da própria organização. No entanto, o regulamento do arquivo só permite a duplicação para efeitos de recolha, armazenamento e conservação, mas não para utilização dos objetos arquivados por terceiros.

Objetivo:
O produtor e o arquivo devem ter analisado o conteúdo dos requisitos de direitos autorais e, se necessário, estabelecido os regulamentos apropriados.

Procedimento:

Se as questões de direitos autorais estão associadas aos objetos digitais a serem arquivados, vários problemas de preservação de longo prazo precisam ser levados em consideração que precisam ser regulamentados em uma base legal ou exigem um acordo legalmente válido entre o proprietário estabelecido dos direitos relevantes e o arquivo. Para permitir que o arquivo execute seu trabalho, ele deve ter os direitos necessários para as formas planejadas de arquivamento e uso na forma de um regulamento legal ou um acordo contratual. As responsabilidades do produtor e do arquivo precisam ser definidas com precisão em uma base legal e / ou por meio de acordos vinculativos.

A migração de objetos digitais para outros formatos de arquivo, por exemplo, poderia ser permitida por uma regulamentação legal especial. A remoção do gerenciamento de direitos digitais (DRM) precisa ser regulamentada contratualmente entre o produtor e o arquivo se não houver base legal para isso. O arquivo e o produtor / proprietário dos direitos podem especificar em um contrato de licença que os objetos arquivados devem ser disponibilizados a um determinado grupo de usuários.

Objetivo:
Questões de garantia e responsabilidade devem ser reguladas entre o produtor e o arquivo.

Procedimento:

Deve ser estabelecido quando as reivindicações de danos podem ser pressionadas, por qual parte e quais deveres de cuidado devem ser observados. Também deve ser

esclarecido se existem regulamentos que se aplicam quando os direitos de terceiros são violados pelo produtor ou pelo arquivo.

Ingerir acordos e documentação

A documentação dos padrões e especificações de ingestão acordados, e do relato dos procedimentos de ingestão, conferem transparência a uma parte da proveniência dos objetos a serem arquivados. Dessa forma, eles ajudam a garantir a integridade e autenticidade desses objetos, conforme exigido pelo catálogo de critérios de repositórios confiáveis. Os mesmos requisitos se aplicam ao arquivamento e aos dados primários.

Objetivo: O produtor e o arquivo devem estabelecer um acordo de ingestão. Este é um acordo vinculativo que regula todos os aspectos da ingestão de informações.
Procedimento: O acordo deve ser aprovado pelo produtor e pelo repositório digital. Ele registra os resultados do planejamento de ingestão conforme descrito em detalhes neste documento. O contrato serve como um manual obrigatório para o processo de ingestão real. Quaisquer mudanças nos elementos do processo estabelecidos no acordo devem ser feitas em um procedimento regulamentado e documentado. Em particular, o acordo deve conter: - a lista das entidades intelectuais a serem arquivadas, incluindo a definição de suas propriedades significativas; - a lista de objetos de informação e dados que representam essas entidades intelectuais; o ambiente técnico necessário para arquivá-los e quaisquer acordos de migração; - a lista de metadados necessários, informando quem os forneceu; - o formato do pacote de transferência, incluindo os metadados necessários, o identificador e a atribuição dos objetos de informação aos pacotes; - a transferência e sua implementação técnica; - a definição dos processos de validação individuais incluindo o grau de cumprimento requerido, as consequências em caso de não cumprimento, as pessoas e ferramentas envolvidas e a sequência cronológica; - a informação que serve de base à análise de risco; especialmente as estimativas da quantidade de dados, capacidade do computador e tempo de computação necessários para *ingest* e estimativas de custo; - as partes atuando na capacidade jurídica, suas relações e as normas relativas aos direitos autorais e responsabilidade; - o cronograma para a realização da ingestão.

Objetivo: Um relatório deve ser feito em cada ingestão, desde o início até o arquivamento. Este protocolo deve ser preservado pela mesma duração que os próprios objetos no arquivo.
Procedimento: O protocolo pode conter as seguintes informações, por exemplo: - Lista de todas as entidades intelectuais ingeridas, mais os objetos de informação correspondentes; - Nome do produtor; - Hora e data de início da transferência;

- Hora e data de chegada do pacote de transferência ao arquivo;
- Hora e data de arquivamento;
- Transformações realizadas em objetos de informação;
- Resultados de validações individuais.

Gestão de qualidade, segurança, processo e risco

Objetivos das atividades de gestão: A ingestão de informação digital é um processo crítico que requer atividades de gestão relevantes e adequadas para atingir o nível de qualidade exigido e para lidar com os riscos de forma adequada, no que diz respeito à segurança e aos custos. A gestão deve ter uma visão geral de todo o sistema e garantir que ele seja eficaz, ou seja, que as metas sejam realistas e tenham sido definidas, de acordo com as especificações do organismo patrocinador e do legislador, que uma estrutura organizacional e infraestrutura adequadas tenham sido definidas para atingir as metas e que todos os processos foram harmonizados. Para isso, é necessário estabelecer uma série de sistemas de gerenciamento diferentes, mas compatíveis. O objetivo aqui é evitar o monitoramento da ingestão de forma isolada, o que resulta em flutuações desnecessárias na qualidade.

Gestão da qualidade: O objetivo principal de um sistema de gestão da qualidade é a satisfação do cliente, mas também a satisfação das outras partes interessadas e dos prestadores de serviços públicos ou da sociedade como um todo. As principais tarefas de um sistema de gestão da qualidade são reconhecer os requisitos atuais e futuros dos clientes e implementar suas demandas. Uma organização precisa estabelecer uma política de qualidade e metas de qualidade para isso. Os processos e responsabilidades necessários para atingir as metas de qualidade precisam ser definidos. Os recursos necessários também devem ser determinados e fornecidos (cf. gerenciamento de processos). A eficácia e eficiência dos processos devem ser verificadas e as causas dos erros analisadas e remediadas. No contexto da ingestão, a gestão da qualidade garante, por exemplo:

- padrões básicos para todos os processos de ingestão e validação em conformidade com as metas de qualidade da organização.
- fornecimento de todos os recursos necessários para os processos de gestão da qualidade, incluindo validação.
- alta qualidade dos recursos necessários.
- revisão da política de qualidade e das metas de qualidade, caso não sejam alcançáveis.

- verificação padronizada de todos os processos de validação.
- padrões básicos para a documentação de todos os processos de ingestão.
- integração de quaisquer processos terceirizados na gestão da qualidade.
- identificação e aplicação de padrões de qualidade adequados.

Gerenciamento da segurança da informação: O objetivo do gerenciamento da segurança é evitar ameaças que coloquem em risco o cumprimento das metas gerais e, em última análise, também a confiabilidade da organização. A tarefa do gerenciamento de segurança é assumir a responsabilidade geral - nesse caso, pela segurança da informação. Uma política de segurança e metas de segurança precisam ser estabelecidas para isso. Os processos e responsabilidades relevantes devem ser determinados para a implementação e os recursos necessários disponibilizados. De importância primordial são o reconhecimento das ameaças e o cálculo do potencial de risco. A eficácia e eficiência dos processos de segurança também devem ser verificados e as causas dos erros analisadas e corrigidas. No contexto do processo de ingestão, o gerenciamento de segurança da informação fornece, por exemplo:

- política de segurança e metas de segurança que foram coordenadas com produtores e fornecedores e estabelecidas em acordos.
- normas que levam em consideração os riscos específicos de categorias de *ingest* (auto arquivamento de uma comunidade, acesso anônimo, ingestão de objetos executáveis, materiais classificados ou objetos virtuais etc.).
- condições organizacionais apropriadas (por exemplo, nomeação de um oficial de segurança, definição de responsabilidades para a emissão de senhas).
- fornecimento (possivelmente conjunto), operação e monitoramento de uma infraestrutura de segurança adequada (por exemplo, infraestrutura de chave pública, definição de metadados adequados).
- identificação e aplicação de padrões de segurança ou requisitos legais.

Gestão de processos: O objetivo da gestão de processos é a implementação eficaz e eficiente das metas organizacionais. Assegura a transparência interna e externa, contribuindo para a eficácia e fiabilidade de uma organização. As tarefas de gerenciamento de processos incluem resumir todas as atividades do processo, levando em consideração as dependências temporais, espaciais e lógicas de sequência, permitindo, assim, que

declarações economicamente significativas sejam feitas. Essa tarefa é baseada nas metas da organização. Os processos formam a base para alocar recursos e responsabilidades e para especificar o desempenho necessário em cada caso. Isso permite que as interfaces organizacionais e técnicas sejam definidas com mais precisão. As tarefas de gerenciamento de processos também incluem a integração de diferentes processos de gerenciamento. No contexto da ingestão, a gestão do processo garante, por exemplo:

- destacando todos os efeitos de ingestão nos processos subsequentes, especialmente no armazenamento de arquivos e no fornecimento de informações.
- a prevenção de efeitos irregulares em outros processos, através de medidas que visem a garantia da qualidade, segurança ou aumento da eficiência da ingestão.
- consideração dos processos que precedem a ingestão. O conhecimento disso ou, melhor ainda, a capacidade de influenciá-lo, pode ter um impacto positivo na ingestão (seleção de formatos de conteúdo e metadados, conhecimento sobre contextos de criação técnica e intelectual).
- a inclusão de *ingests* realizados ou preparados com base no projeto em "processos padrão" por meio de configuração apropriada e gerenciamento de mudanças.
- ajuste dos processos de ingestão existentes às condições técnicas e organizacionais alteradas, tanto no arquivo quanto no lado do cliente, por meio de configuração adequada e gerenciamento de alterações.

Gestão de riscos: Além dos riscos para a qualidade e segurança, podem surgir riscos adicionais dependendo da forma como os alimentos são organizados. O objetivo da gestão de riscos é registrar e avaliar os riscos, para minimizá-los, controlá-los e monitorá-los de forma contínua. Cinco estratégias diferentes de gerenciamento de risco são distinguidas entre: evitar, reduzir, limitar, mudar e aceitar riscos. O gerenciamento de riscos é um processo iterativo e cobre todo o processo de ingestão. Envolve o produtor e o arquivo. No contexto da ingestão, os seguintes riscos devem ser considerados:

- Riscos financeiros: Cada processo de ingestão (e cada aspecto do processo de ingestão descrito neste manual) exige recursos do produtor e do arquivo e gera uma necessidade de recursos adicionais para o arquivamento

permanente dos dados inseridos. O planejamento detalhado e o orçamento de um processo de ingestão servem de base para o gerenciamento dos riscos financeiros. Os riscos financeiros afetam os recursos humanos e financeiros.

- Recursos humanos: A mão de obra de uma variedade de funcionários com diferentes habilidades é necessária para realizar o processo de ingestão. O arquivamento permanente dos dados assimilados requer mais recursos humanos para qualquer migração necessária e para o processamento dos dados para uso.
- Recursos financeiros: O processo de ingestão gera custos para atransferência de dados, armazenamento provisório e o computador necessário, capacidade. O arquivamento permanente dos dados ingeridos gera custos de armazenamento de memória, backup de dados e proteção de dados, capacidade do computador e memória temporária para uso dos dados, e tempo de computação e memória temporária para quaisquer migrações.
- Riscos jurídicos: A absorção de informação por um arquivo ocorre no âmbito de várias disposições legais e / ou contratuais (conforme definido em "Identificação das condições legais e contratuais"). A não observância dessas disposições pode resultar em uma série de sanções.
- Riscos de reputação. Além de considerações legais, um arquivo também pode estar sujeito a certas obrigações morais em relação ao armazenamento de longo prazo de dados digitais. Consequentemente, a reputação do arquivo pode ser prejudicada por não ingerir esses dados ou por ingerir os dados, mas não garantir sua preservação.

APÊNDICE G - FASES DAS INTERAÇÕES PRODUTOR-ARQUIVO

As Interações Produtor-Arquivo consistem, de acordo com CCSDS (2004, p. 3-1), em quatro fases diferentes:

- A Fase Preliminar,
- A Fase de Definição Formal;
- A Fase de Transferência;e
- A Fase de Validação.

Cada uma das quatro fases detalhadas pode ser dividida em subfases. Nesse caso, as subfases devem ser tratadas na ordem apresentada e são caracterizadas por ações devidamente identificadas. As ações, entretanto, podem ser realizadas em qualquer ordem.

Fase Preliminar (Pre-Ingest)

A Fase Preliminar leva, segundo CCSDS (2004), a um documento resumido sobre a viabilidade do Projeto Produtor-Arquivo e aprova o procedimento para a fase de definição formal (ou a interrupção do projeto).

Os objetivos da fase Preliminar são os seguintes:

- identificar as informações primárias que o Arquivo deve preservar;
- estabelecer uma definição preliminar dos diferentes Objetos de Dados que serão transmitidos ao Arquivo pelo Produtor;
- analisar todos os aspectos de viabilidade;
- decidir sobre a viabilidade do Projeto Produtor-Arquivo, tanto do ponto de vista do Produtor como do Arquivo;
- fazer uma estimativa dos recursos necessários;
- Elaborar um Documento Sumário e, se apropriado, um acordo preliminar (CCSDS, 2004, p. 3-1);

Um Projeto Produtor-Arquivo é, segundo CCSDS (2004), um conjunto de atividades e os meios utilizados pelas informações Produtor e o Arquivo para ingerir um determinado conjunto de informações no Arquivo. Nos termos do acordo entre o Produtor e o Arquivo, o Produtor concorda em fornecer um conjunto de informações definidas no âmbito de um Projeto Produtor-Arquivo. As seguintes informações estão contidas dentro deste conjunto:

- as informações primárias que devem ser preservadas;

> - as informações complementares, que são necessárias para que os Pacotes de Informações de Arquivo (AIPs) sejam constituídos, por exemplo, informações fornecidas pelo Produtor dentro do contexto do Projeto Produtor-Arquivo em questão; informações fornecidas pelo mesmo Produtor dentro do contexto do Projeto Produtor- Arquivo anterior; informações entregues por outra instituição (para normas, por exemplo); e informações entregues pelo próprio Arquivo (Referência, Informações de Fixidade de AIPs) (CCSDS, 2004, p. 2-3).

A Fase Preliminar é composta, de acordo com CCSDS (2004, p. 3-1), de três subfases:

- Primeiro contato;
- Definição preliminar, estudo de viabilidade e avaliação do Projeto Produtor-Arquivo;
- Elaboração de um Acordo Preliminar.

Resumo da Fase Preliminar	
Sub-fase	Tabela de Ação
Primeiro Contato	Primeiro Contato
Definição preliminar, viabilidade e avaliação	Informação a ser arquivada
	Referências do objeto
	Quantificação
	Condições de Segurança
	Aspectos Contratuais e Legais
	Operações de Transferência
	Validação
	Cronograma
	Impacto permanente no arquivo
	Resumo dos custos e riscos
Elaboração de um acordo preliminar	Estabelecimento de um acordo preliminar

Id	**Fase Preliminar: Primeiro Contato**
P-1	Identifique as pessoas de contato e a organização de trabalho
P-2	Troca de informações gerais
Id	**Fase Preliminar: Informações a Serem Arquivadas**
P-3	Identifique as informações de conteúdo a serem preservadas
P-4	Identifique as informações complementares
P-5	Identifique a comunidade designada
P-6	Defina o acesso do consumidor às informações
P-7	Avalie a duração planejada da preservação desta informação por este Arquivo
P-8	Avalie a viabilidade e os custos induzidos pelas ações anteriores
Id	**Fase Preliminar: Objetos Digitais e Padrões Aplicados a estes objetos**
P-9	Faça uma identificação preliminar dos objetos de dados relacionados às diferentes categorias de informações a serem arquivadas
P-10	Defina as regras e padrões relacionados a esses objetos que são aceitos pelo Arquivo
P-11	Descreva as ferramentas disponíveis para a aplicação das regras e padrões conhecidos pelo Arquivo
P-12	Fornece as regras e padrões aplicados aos Objetos de Dados pelo Produtor

P-13	Descreva as ferramentas disponíveis para aplicação das regras e padrões conhecidos pelo Produtor
P-14	Avalie a compatibilidade e estude as soluções
P-15	Avalie os esforços a serem feitos e os custos associados

Id	**Fase Preliminar: Referências de Objeto**
P-16	Elabore um inventário das informações sobre as regras de identificação existentes ou nomenclatura dentro do domínio, disposições legais e padrões
P-17	Defina as regras que podem ou devem ser aplicadas no contexto do Projeto Produtor-Arquivo
P-18	Avalie os custos associados
Id	**Fase Preliminar: Quantificação**
P-19	Estime o volume de dados a ser transmitido ao Arquivo
P-20	Avalie o volume de dados permanente para armazenar
P-21	Avalie a capacidade de armazenamento necessária para o processo de ingestão
P-22	Avalie os custos associados
Id	**Fase Preliminar: Condições de Segurança**
P-23	Identificar os requisitos de confidencialidade das informações e de autenticação da fonte das informações na transferência entre o produtor e o arquivo.
P-24	Identificar os requisitos para a segurança dos acervos nos Arquivos.
P-25	Identificar os requisitos de confidencialidade das informações e de autenticação da fonte das informações na transferência entre o arquivo e o consumidor
P-26	Identifique os padrões e ferramentas que podem ser usados.
P-27	Avalie os custos associados.
Id	**Fase Preliminar: Aspectos Legais e Contratuais**
P-28	Defina a natureza das relações entre o arquivo e o produtor
P-29	Avalie o problema da propriedade intelectual
P-30	Defina as condições de acesso aos dados
P-31	Certificação de arquivo de endereços
P-32	Fornece os padrões e ferramentas usadas
P-33	Avalie os custos associados
Id	**Fase Preliminar: Operações de Transferência**
P-34	Faça uma definição preliminar dos SIPs
P-35	Trocar os requisitos e restrições com relação à transferência de objetos de dados e identificar possíveis soluções
P-36	Avalie os custos associados
Id	**Fase Preliminar: Validação**
P-37	Fornecer ao produtor informações sobre os procedimentos de validação SIP, os procedimentos de rejeição e as ferramentas que são aplicadas pelo arquivo
P-38	Estude o desenvolvimento ou modificação das ferramentas de validação necessárias
P-39	Estude a implementação de métodos de qualidade (e ferramentas) para atender às necessidades
P-40	Avalie os custos associados
Id	**Fase Preliminar: Cronograma**
P-41	Defina um cronograma preliminar
Id	**Fase Preliminar: Impacto Permanente no Arquivo**
P-42	Avalie o impacto permanente e os custos associados no arquivo
Id	**Fase Preliminar: Resumo de Custos, Riscos**
P-43	Realizar um resumo de custos e estimar os riscos
Id	**Fase Preliminar: Pontos Críticos**
P-44	Avalie os pontos críticos

Id	Fase Preliminar: Estabelecimento de um Acordo Preliminar
P-45	Elabore um documento que resuma a fase preliminar, com uma avaliação de viabilidade e uma recomendação sobre como prosseguir com a fase de definição formal (ou interrompê-la)
P-46	Faça um acordo preliminar para prosseguir para a próxima fase

Fase De Definição Formal

Objetivou-se, nesta fase, a negociação do "Acordo de Submissão", que inclui uma definição completa e precisa de:

- os dados a serem entregues ao Arquivo pelo Produtor;
- os aspectos contratuais e legais;
- os elementos complementares necessários para definir o processo de transferência e validação;
- o cronograma (CCSDS, 2004, 3-16).

A Fase de Definição formal é composta, de acordo com CCSDS (2004) de três subfases: a organização da fase de definição formal;a definição formal e a elaboração do Contrato de Submissão para aprovação do Produtor e do Arquivo.

Resumo da fase de definição formal		
Fase de definição	Organização do Formal	
Definição formal	Informações a serem preservadas e Modelo de Objetos de dados a serem entregue	Contexto geral do projeto e definição de Objetos de informação
		Criação de um Dicionário de dados
		Construção de um modelo formal
	Formalização dos aspectos contratuais e legais	
	Definição das condições de transferência	
	Definição de validação	
	Cronograma de entrega	
	Gerenciamento de mudanças após a conclusão de Contrato de Submissão.	
	Avaliação de viabilidade, custos e riscos	
Acordo de Submissão	Acordo de Submissão	

Tabela de resumo para a fase de definição formal

Id	Definição formal Fase: Organização da Fase de Definição Formal
F-1	Configure a gestão da fase de definição formal
F-2	Especifique os pontos levantados anteriormente que devem ser explicitados na fase de definição formal
Id	**Definição formal Fase: Contexto Geral do Projeto e Definição de Informações Objetos**
F-3	Defina o contexto geral do projeto, bem como a lista e o conteúdo dos elementos de informação a serem entregues

F-4	Defina os formatos, regras de codificação e padrões a serem aplicados para os objetos a serem entregues
F-5	Defina os indicadores de volume
F-6	Defina as referências para os objetos a serem entregues
F-7	Escolha as ferramentas do lado do produtor
F-8	Escreva uma descrição dos Objetos de Informação referindo-se a um Dicionário de Dados e um modelo (parte do acordo final)

Id	**Fase de Definição Formal: Criação de um Dicionário de Dados**
F-9	Defina as classes de objeto e seus atributos, configure o Dicionário de Dados associado
F-10	Codifique o Dicionário de Dados
Id	**Fase de definição formal: construção de um modelo formal**
F-11	Defina o modelo dos dados a serem entregues
F-12	Desenhe uma representação do modelo
Id	**Fase de definição formal: formalização dos aspectos contratuais e jurídicos**
F-13	Elaborar acordos legais e contratuais entre o Arquivo e o produtor em relação aos dados (parte do acordo final)
Id	**Fase de definição formal: definição das condições de transferência**
F-14	Defina os procedimentos de comunicação (rede digital, protocolos, mídia, etc.)
F-15	Defina as informações de embalagem dos objetos entregues (de que forma os dados são entregues)
F-16	Definir uma sessão de transferência (estrutura funcional e temporal da transferência de objetos digitais)
F-17	Defina o teste de transferência inicial
F-18	Identifique as ferramentas que podem ser usadas durante a fase de transferência
F-19	Escreva uma descrição dos procedimentos de transferência (com base em F-14 a F-18).
Id	**Fase de definição formal: definição de validação**
F-20	Definir plano de validação imediata
F-21	Defina um plano de validação aprofundado
F-22	Definir os procedimentos para rejeição, retransferência, aceitação de objetos (formulários, formulários de anomalia, aprovações técnicas, análises, etc).
F-23	Defina o teste de validação inicial
F-24	Identifique as ferramentas de validação
F-25	Escreva uma descrição dos procedimentos de validação
Id	**Fase de definição formal: cronograma de entrega**
F-26	Defina um cronograma de entrega de referência (parte do acordo final)
F-27	Definir os procedimentos a serem implementados em caso de não cumprimento do cronograma
Id	**Fase de definição formal: gerenciamento de mudanças após a conclusão do contrato de envio**
F-28	Identifique a origem (quem) e as causas da mudança
F-29	Identifique os cenários para gerenciar a mudança
F-30	Avalie o trabalho a ser executado, o custo e a viabilidade por cenário
F-31	Tome decisões relevantes após a discussão
F-32	Definir e executar plano de ação
Id	**Fase de definição formal: Viabilidade, avaliação de custos e riscos**
F-33	Validar a viabilidade do projeto
F-34	Avalie os custos para o arquivo e o produtor

F-35	Estimar os riscos
Id	**Fase de definição formal: Acordo de submissão**
F-36	Elabore o Acordo de Submissão

Fase de Transferência

O objetivo desta fase é a transferência real dos Objetos de Dados entre o Produtor e o Arquivo.

Durante uma sessão de apresentação de dados, um ou mais SIPs são entregues. O SIP é, por sua vez, composto de um ou mais objetos de dados, cujas características são descritos no Dicionário de Dados.

Cada objeto entregue é em referência a um objeto que foi, previamente, identificado tendo por base o modelo de dados.

Não há nenhuma subfase associada à fase de transferência. Os assuntos da fase de transferência são tratados de forma mais precisa sob a forma de listas de ações a serem realizadas.

Resumo da fase de transferência
Tabela de ação
Realizar o teste de transferência
Gerenciar a transferência

Tabela de resumo da fase de transferência

Id	**Fase de transferência: realizar o teste de transferência**
T-1	Teste de transferência inicial
Id	**Fase de transferência: Gerenciar a transferência**
T-2	Garantir a execução adequada da operação de transferência de dados de ambos os lados do produtor e do arquivo

Fase de Validação

O objetivo desta fase é realizar a validação dos objetos entregues, gerenciar as anomalias detectadas, e aceitar todos os objetos transferidos.

Não há nenhuma subfase associada à fase de validação. Os sujeitos da validação são tratadas de forma mais precisa nas seguintes subseções, sob a forma de listas de ações a serem realizadas.

Resumo da Fase de Validação
Tabela de ação
Realizar o teste de validação
Gerenciar a validação

Tabela de resumo para a fase de validação

Id	Fase de validação: realizar o teste de validação
V-1	Teste de validação inicial
Id	**Fase de validação: gerenciar a validação**
V-2	Aplicar as validações
V-3	Gerenciar os resultados da validação

APÊNCIDE H - QUADRO COMPARATIVO ENTRE RDC-ARQ X TRAC

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**a. Governança e viabilidade organizacional**	**A1. Governança e viabilidade organizacional**
Requisitos em análise	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	A1.1 O repositório possui uma declaração de missão que reflete um compromisso com a retenção a longo prazo, gerenciamento e acesso a informações digitais.
Agente da ação de preservação	O repositório Essa missão	O repositório
Ação de preservação	- ter -é	- possuir
Objeto da ação de preservação	- a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais. - claramente identificada por todos os interessados no repositório e envolve: mandato legal, contexto organizacional e requisitos regulatórios.	a retenção a longo prazo, gerenciamento e acesso a informações digitais.
Comparação	Os agentes da ação de preservação são os mesmos. As ações de preservação expressam o mesmo sentido: Ter / possuir Os objetos da ação de preservação não são os mesmos. O RDC-Arq é taxativo ao falar em preservação. O TRAC fala em reter por período prolongado. Ainda assim, considerou-se tais ações sinônimas. A segunda oração, apresentada no RDC_Arq, não apresenta uma oração correspondente no TRAC.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**a. Governança e viabilidade organizacional**	**A1. Governança e viabilidade organizacional**
Requisitos em análise	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.	A1.2 O repositório possui um plano de sucessão formal apropriado, planos de contingência e / ou acordos de custódia em vigor no caso do repositório deixar de operar ou o governo ou instituição financiadora alterarem substancialmente seu escopo.
Agente da ação de preservação	O repositório	O repositório
Ação de preservação	ter	possuir
Objeto da ação de preservação	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.	um plano de sucessão formal apropriado, planos de contingência e / ou acordos de custódia em vigor no caso do repositório deixar de operar ou o governo ou instituição financiadora alterarem substancialmente seu escopo.
Comparação	Os agentes da ação de preservação são os mesmos. As ações de preservação expressam o mesmo sentido: Ter / possuir. Os objetos alvo da ação de preservação são os mesmos. Ambos os modelos de requisitos visam a necessidade de planos de sucessão formais, 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. .	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**a. Governança e viabilidade organizacional**	**A2. Estrutura organizacional e pessoal**
Requisitos em análise	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.	A2.1 O Repositório identificou e estabeleceu as funções que deve desempenhar e tem pessoal nomeado com competências e experiência adequadas ao desempenho destas funções.
		A2.2 O repositório tem o número adequado de funcionários para apoiar todas as funções e serviços.
		A2.3 O Repositório dispõe de um programa de desenvolvimento profissional ativo que proporciona ao pessoal oportunidades de desenvolvimento de competências e conhecimentos.
Agente da ação de preservação	O repositório	O repositório
Ação de preservação	- Ter; - Manter;	- Identificar, Estabelecer; -Ter; -Dispõe;
Alvo da ação de preservação	uma equipe dotada de qualificação e formação necessárias.	pessoal nomeado com competências e experiência adequadas ao desempenho destas funções.
Alvo da ação de preservação	número suficiente para garantir todos os serviços e funcionalidades pertinentes ao repositório.	número adequado de funcionários para apoiar todas as funções e serviços.
Alvo da ação de preservação	um programa de desenvolvimento profissional contínuo.	um programa de desenvolvimento profissional ativo que proporciona ao pessoal oportunidades de desenvolvimento de competências e conhecimentos.
Comparação	Os agentes das ações de preservação são os mesmos. As ações de preservação, apesar de diferentes, tem por alvo ações de preservação comuns entre si. O RDC-Arq apresenta um requisito único que equivale aos critérios TRAC A2.1, A2.2 e A2.3.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Definir a comunidade alvo e sua base de conhecimento;	A3.1 O Repositório definiu a(s) sua(s) comunidade(s) designada(s) e os conhecimentos associados e dispõe de definições e políticas acessíveis ao público para ditar a forma como seus serviços de preservação serão cumpridos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que se trata do" repositório".	O reposiótio
Ação de preservação	- Definir	- Definir
Objeto da ação de preservação	a comunidade alvo e sua base de conhecimento	a(s) sua(s) comunidade(s) designada(s) e os conhecimentos associados
Comparação	Os agentes das ações de preservação, as ações de preservação, os objetos das ações de preservação sujeitos, verbos e alvos das ações de preservação são similares.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Possuir políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;	A3.1 O Repositório definiu a(s) sua(s) comunidade(s) designada(s) e os conhecimentos associados e dispõe de definições e políticas acessíveis ao público para ditar a forma como seus serviços de preservação serão cumpridos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que se trata do ”repositório”.	O reposiótio
Ação de preservação	- possuir	- dispor
Objeto da ação de preservação	políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;	definições e políticas acessíveis ao público para ditar a forma como seus serviços de preservação serão cumpridos;
Comparação	Os agentes das ações de preservação, as ações de preservação, os objetos das ações de preservação sujeitos, verbos e alvos das ações de preservação são similares. Importante salientar que o RDC-Arq apresentou subdivididos o critério TRAC A3.1, o que propicia uma análise mais pormenorizada, contribuindo para ações de auditoria e certificação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Possuir políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem;	A3.2 O Repositório tem procedimentos e políticas em vigor e mecanismos para a sua revisão, atualização, e desenvolvimento à medida que o repositório cresce e à medida que a tecnologia e a prática comunitária evoluem.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	- Possuir	- Ter
Objeto da ação de preservação	políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem;	procedimentos e políticas em vigor e mecanismos para a sua revisão, atualização, e desenvolvimento à medida que o repositório cresce e à medida que a tecnologia e a prática comunitária evoluem.
Comparação	Os sujeitos, verbos e alvos das ações de preservação são idênticos.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Documentar permissões legais - por meio de acordos de custódia, normas de procedimentos e outros - que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;	A3.3 O Repositório mantém políticas escritas que especificam a natureza de quaisquer autorizações legais necessárias para preservar os conteúdos digitais ao longo do tempo, e o repositório pode demonstrar que estas autorizações tem sido adquiridas quando necessário.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	- Documentar;	- Manter; - Poder;
Objeto da ação de preservação	permissões legais que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;	políticas escritas que especificam a natureza de quaisquer autorizações legais necessárias para preservar os conteúdos digitais ao longo do tempo
Comparação	Ambos os requisitos tutelam sobre a necessidade de manter documentação a respeito da custódia da informação ali armazenada, bem como de autorizações /permissões para alteração decorrentes das ações/estratégias de preservação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Relacionar o registro histórico, acima referido, com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;	A3.4 O Repositório compromete-se a proceder a uma revisão e avaliação formal e periódica para assegurar capacidade de resposta aos desenvolvimentos tecnológicos e à evolução das necessidades.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Relacionar;	Proceder;
Objeto da ação de preservação	o registro histórico com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;	revisão e avaliação formal e periódica para assegurar capacidade de resposta aos desenvolvimentos tecnológicos e à evolução das necessidades.
Comparação	Os requisitos versam sobre a necessidade do repositório manter registros formais atualizados sobre as ações de preservação, bem como prever efeitos das mudanças tecnológicas e mesmo das estratégis adotadas sobre as informações digitais armazenadas.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;	A3.5 O Repositório tem políticas e procedimentos para assegurar que as reações dos produtores e utilizadores sejam buscadas e abordadas ao longo do tempo.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do “Repositório”.	O Repositório
Ação de preservação	Demonstrar;	Ter;
Objeto da ação de preservação	a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;	políticas e procedimentos para assegurar que as reações dos produtores e utilizadores sejam buscadas e abordadas ao longo do tempo.
Comparação	Os requisitos em análise tratam da necessidade constante de avaliação do repositório pela comunidade designada e pelos produtores da informação digital preservada.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	fazer o registro histórico das mudanças de procedimentos, de *software* e *hardware*;	A3.6 O Repositório tem um histórico documentado das alterações às suas operações e procedimentos, softwares e hardwares que, se for caso disso, estejam ligados à estratégias de preservação relevantes e descreve os efeitos potenciais na preservação dos conteúdos digitais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Fazer;	Ter;
Objeto da ação de preservação	o registro histórico das mudanças de procedimentos, de *software* e *hardware*;	um histórico documentado das alterações às suas operações e procedimentos, softwares e hardwares que, se for caso disso, estejam ligados à estratégias de preservação relevantes e descreve os efeitos potenciais na preservação dos conteúdos digitais.
Comparação	Os requisitos orientam sobre a obrigação dos repositórios em documentar e armazenar alterações de procedimentos ligados a software e hardware.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise		A3.7 O Repositório compromete-se a garantir a transparência e a responsabilidade em todas as ações de apoio à operação e gestão do repositório, especialmente às que afetam a preservação de conteúdos digitais ao longo do tempo.
Agente da ação de preservação		O Repositório
Ação de preservação		Comprometer-se a garantir;
Objeto da ação de preservação		a garantir a transparência e a responsabilidade em todas as ações de apoio à operação e gestão do repositório, especialmente às que afetam a preservação de conteúdos digitais ao longo do tempo.
Comparação	O RDC-Arq não apresentou requisito semelhantepara este critério do Manual TRAC.	
Resultado	Sem correspondências similares.	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia;	A3.8 O Repositório compromete-se a definir, recolher, acompanhar e fornecer, a pedido, suas medições de integridade da informação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Estar comprometido;	Comprometer;
Objeto da ação de preservação	definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia	a definir, recolher, acompanhar e fornecer, a pedido, suas medições de integridade da informação.
Comparação	Os requisitos lidam com a necessidade de manter e disponibilizar informes sobre a integridade dos objetos digitais sob sua responsabilidade	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Estar comprometido em realizar regularmente uma autoavaliação de seu funcionamento e renovar sua certificação; e Estar comprometido em notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu *status* de certificação (no caso de repositórios já certificados).	A3.9 O Repositório compromete-se a cumprir um calendário regular de autoavaliação e certificação e, se certificado, compromete-se a notificar os organismos de certificação de alterações operacionais que irão mudar ou anular o seu estatuto de certificação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Estar comprometido;	Comprometer-se;
Objeto da ação de preservação	- autoavaliação de seu funcionamento e renovar sua certificação; - notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu *status* de certificação	- um calendário regular de autoavaliação e certificação; - notificar os organismos de certificação de alterações operacionais que irão mudar ou anular o seu estatuto de certificação.
Comparação	Os requisitos versam sobre a necessidade de autoavaliar-se e certificar-se regularmente e, caso já certificado, o repositório tem o dever de informar à organização certificadora sobre qualquer mudança em seus procedimentos de preservação. O RDC-Arq apresenta o critério A.3.9 subdividido em dois requisitos, o que propicia a análise e ações de verificação em auditoria e autoavaliações/ certificações.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - demonstração da capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;	A4.1 O Repositório dispõe de processos de planejamento empresarial de curto e longo prazo para sustentar o repositório ao longo do tempo.
Agente da ação de preservação	O Repositório	O Repositório
Ação de preservação	Demonstrar;	Dispor;
Objeto da ação de preservação	capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;	de processos de planejamento empresarial de curto e longo prazo para sustentar o repositório ao longo do tempo.
Comparação	Ambos os requisitos tratam da obrigatoriedade do repositório digital prever recursos para sustentar-se ao longo do tempo.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - revisão e ajustes anuais;	A4.2 O repositório possui processos para revisar e ajustar os planos de negócios pelo menos anualmente.
Agente da ação de preservação	Um Repositório	O Repositório
Ação de preservação	- Revisar - Ajustar	- Revisar - Ajustar
Objeto da ação de preservação	Sustentabilidade financeira	Planos de negócios
Comparação	Os requisitos versam sobre a necessidade de revisar e ajustar, anualmente, os planos de negócio dos repositórios digitais, com o intuito de garantir sua sustentabilidade financeira.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - Transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere;	A4.3 As práticas e procedimentos financeiros dos repositórios são transparentes, em conformidade com normas e práticas contabilísticas relevantes, e auditadas por terceiros de acordo com requisitos legais territoriais.
Agente da ação de preservação	Um Repositório	O Repositório
Ação de preservação	Dever;	Ser
Objeto da ação de preservação	Transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere;	transparentes, em conformidade com normas e práticas contabilísticas relevantes, e auditadas por terceiros de acordo com requisitos legais territoriais.
Comparação	Os requisitos em análise apreciam sobre a indispensabilidade da transparência em práticas e procedimentos financeiros, no intuito de demosntrar a sustentabilidade dos repositórios no longo prazo	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos.	A4.4 O Repositório tem um compromisso contínuo de analisar e relatar os riscos e benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).
Agente da ação de preservação	Um Repositório	O Repositório
Ação de preservação	Dever;	Ter;
Objeto da ação de preservação	sustentabilidade financeira por meio do compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos	um compromisso contínuo de analisar e relatar os riscos e benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).
Comparação	Os requisitos tratam da necessidade de demosntrar sustentabilidade financeira através da análise e divulgação dos riscos e benefícios, investimentos e despesas.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise		A4.5 O Repositório compromete-se a acompanhar e a fazer pontes entre as lacunas de financiamento.
Agente da ação de preservação		O Repositório
Ação de preservação		Comprometer;
Objeto da ação de preservação		a acompanhar e a fazer pontes entre as lacunas de financiamento.
Comparação	O RDC-Arq não apresentou requisito semelhante a este critério do Manual TRAC.	
Resultado	Sem correspondências similares.	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**e. Contratos, licenças e passivos**	**A5. Contratos, licenças e responsabilidades**
Requisitos em análise	- 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.	A5.1 Se o repositório gerir, preservar e/ou fornecer acesso a materiais digitais em nome de outra organização, tem e mantém contratos ou acordos de depósito adequados.
		A5.2 Os contratos de repositório ou acordos de depósito devem especificar e transferir todos os elementos necessários direitos de conservação, devendo esses direitos transferidos ser documentados.
		A5.3 O Repositório especificou todos os aspectos adequados da aquisição, manutenção e acesso, e a retirada em acordos escritos com os depositantes e outras partes relevantes.
		A5.4 Pistas de repositório e gestão dos direitos de propriedade intelectual e restrições à utilização de conteúdo do repositório são conforme exigido pelo acordo de depósito, contrato ou licença.
		A5.5 Se os repositórios de conteúdos digitais com propriedade/direitos são pouco claros, as políticas estão alocadas para enfrentar a responsabilidade e os desafios a esses direitos.
Agente da ação de preservação	Os contratos, licenças e passivos firmados pelo repositório;	-O repositório; -Os contratos ou acordos de depósito do repositório; -O repositório; -Pistas de repositório e gestão dos direitos de propriedade intelectual e restrições à utilização de conteúdo do repositório; -as políticas;
Ação de preservação	Dever; Delinear; Ser; Poder;	Gerir, preservar e/ou fornecer; Dever; Especificar; Estar, Ser;
Objeto da ação de preservação	-ser claros e mensuráveis; -papéis, responsabilidades, prazos e condições;-facilmente acessíveis ou disponíveis aos interessados. -envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e	-acesso a materiais digitais em nome de outra organização, tem e mantém contratos ou acordos de depósito adequados. -os elementos necessários direitos de conservação, devendo esses direitos transferidos ser documentados;

	fornecedores de serviços.-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.	- todos os aspectos adequados da aquisição, manutenção e acesso, e a retirada em acordos escritos com os depositantes e outras partes relevantes. -conforme exigido pelo acordo de depósito, contrato ou licença. - alocadas para enfrentar a responsabilidade e os desafios a esses direitos.
Comparação	Enquanto o RDC-Arq utiliza um único requisito para versar sobre contratos licenças e passivos, o TRAC utiliza cinco requisitos para tratar do mesmo obeto de preservação. Ainda assim, considera-se que sejam conceitualmente similares.	
Resultado	Parcialmente Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.);	B1.1 O Repositório identifica propriedades que irá preservar para objetos digitais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Identificar;	Identificar;
Objeto da ação de preservação	as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.);	propriedades que irá preservar para objetos digitais.
Comparação	Ambos os requisitos observam a importância de identificar propriedades que deverão ser preservadas.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;	B1.2 O Repositório especifica claramente as informações que devem ser associadas ao material no momento do seu depósito (isto é, SIP).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Especificar;	Especificar;
Objeto da ação de preservação	a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;	as informações que devem ser associadas ao material no momento do seu depósito (isto é, SIP).
Comparação	Os requisitos alvo de comparação tratam do mesmo objeto da ação de preservação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;	B1.3 O Repositório tem mecanismos para autenticar a origem de todos os materiais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ter;	Ter;
Objeto da ação de preservação	mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;	mecanismos para autenticar a origem de todos os materiais.
Comparação	Os requisitos alvo de comparação tratam do mesmo objeto da ação de preservação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter procedimentos para verificar a integridade do *SIP*, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;	B1.4 O processo de ingestão do Repositório verifica a exaustividade de cada objeto apresentado (ou seja, o SIP) e exatidão, tal como especificado no ponto B1.2.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O processo de ingestão do Repositório
Ação de preservação	Ter;	Verificar;
Objeto da ação de preservação	procedimentos para verificar a integridade do *SIP*, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;	a exaustividade de cada objeto apresentado (ou seja, o SIP) e exatidão, tal como especificado no ponto B1.2.
Comparação	Os requisitos alvo de comparação tratam do mesmo objeto da ação de preservação:verificação de intergidade do Pacote SIP	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter o controle físico (controle completo dos *bits*) dos documentos transmitidos com cada *SIP*, a fim de preservá-los;	B1.5 O Repositório obtém controle físico suficiente sobre os objetos digitais para preservá-los.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O processo de ingestão do Repositório
Ação de preservação	Ter;	Obter;
Objeto da ação de preservação	o controle físico (controle completo dos *bits*) dos documentos transmitidos com cada *SIP*, a fim de preservá-los;	controle físico suficiente sobre os objetos digitais para preservá-los.
Comparação	Os requisitos alvo de comparação tratam do mesmo objeto da ação de preservação: O controle físico os objetos digitais com o objetivo de preservá-los.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo o processo de admissão;	B1.6 O Repositório fornece ao produtor/depositário respostas apropriadas em pontos durante os processos de ingestão.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O processo de ingestão do Repositório
Ação de preservação	Fornecer;	Fornecer;
Objeto da ação de preservação	ao produtor/depositante relatórios do andamento dos procedimentos durante todo o processo de admissão;	ao produtor/depositário respostas apropriadas em pontos durante os processos de ingestão.
Comparação	Os requisitos alvo de comparação tratam do mesmo objeto da ação de preservação: respostas apropriadas em pontos durante os processos de ingestão.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- demonstrar em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório; e	B1.7 O Repositório pode demonstrar quando a responsabilidade pela preservação é formalmente aceita para o conteúdo dos objetos de dados submetidos (ou seja, SIPs).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O processo de ingestão do Repositório
Ação de preservação	Demonstrar;	Demonstrar;
Objeto da ação de preservação	em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório;	quando a responsabilidade pela preservação é formalmente aceita para o conteúdo dos objetos de dados submetidos (ou seja, SIPs).
Comparação	Os requisitos alvo de comparação tratam do mesmo objeto da ação de preservação: O momento em que a responsabilidade pela preservação é formalmente aceita para o conteúdo dos objetos de dados submetidos	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação.	B1.8 O Repositório possui registros contemporâneos de ações e processos administrativos que são relevantes para a preservação (Ingestão: aquisição de conteúdo).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ter;	Possuir;
Objeto da ação de preservação	registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação	registros contemporâneos de ações e processos administrativos que são relevantes para a preservação (Ingestão: aquisição de conteúdo).
Comparação	Ambos os requisitos apresentam agentes da ação de preservação, ações de preservação e objetos da ação de preservação similares.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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 os componentes-chave do *AIP*: o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixidade, proveniência e contexto), e ainda como esses componentes se relacionam;	B2.1 O Repositório tem uma definição escrita e identificável para cada AIP ou classe de informação preservado pelo repositório.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Descrever;	Ter;
Objeto da ação de preservação	cada classe de informação a ser preservada pelo repositório, e como ela está implementada - essa descrição deve apontar os componentes-chave do *AIP*: o documento arquivístico, sua informação de representação e as várias categorias de informação descritiva de preservação, e ainda como esses componentes se relacionam;	uma definição escrita e identificável para cada AIP ou classe de informação preservado pelo repositório.
Comparação	Ambos os requisitos tratam do processo de ingestão do SIP no ambiente OAIS. A grande diferença do Pacote SIP arquivístico são os metados específicos relacionados às qualidades dos documentos arquivísticos, que vão além daquelas previstas para um objeto digital originalmente alvo das ações de preservação do TRAC. Isso porque o TRAC trata e objetos digitais oriundos de Museus, bibliotecas, bancos de dados e arquivos. O RDC-Arq trata, especificamente de objetos digitais produzidos, recebidos e acumulados em função de atividades de pessoas físicas, pessoas jurídicas.	
Resultado	Parcialmente similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- descrever minuciosamente as diferentes classes de informação e como os *AIPs* são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes (por exemplo, a imagem *TIFF* que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessárias à imagem *TIFF* que é apresentada para o olho humano);	B2.2 O Repositório tem uma definição de cada AIP (ou classe) que é adequada para caber a longo prazo necessidades de preservação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Descrever;	Ter.
Objeto da ação de preservação	minuciosamente as diferentes classes de informação e como os *AIPs* são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes.	tem uma definição de cada AIP (ou classe) que é adequada para caber a longo prazo necessidades de preservação.
Comparação	Ambos os requisitos analisados tratam da necessidade de determinar, detalhadamente, cada Pacote AIP, ou classe de AIPs, especificando suas necessidades de preservação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- descrever como os *AIPs* são construídos a partir dos *SIPs*, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do *AIP*;	B2.3 Repositório tem uma descrição de como os AIPs são construídos a partir de SIPs.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Descrever;	Ter;
Objeto da ação de preservação	como os *AIPs* são construídos a partir dos *SIPs*, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do *AIP*;	uma descrição de como os AIPs são construídos a partir de SIPs.
Comparação	Ambos os requisitos analisados observam sobre a forma com que os AIPs serão construídos a partir dos SIPs.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- ser capaz de demonstrar se os *SIPs* foram aceitos e transformados em um *AIP*s integralmente ou em parte, ou ainda se foram recusados;	B2.4 O Repositório pode demonstrar que todos os objetos submetidos (ou seja, SIPs) são aceitos como um todo ou parte de um eventual objeto de arquivo (isto é, AIP), ou dispostos de outra forma em um modelo registrado.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ser capaz de demosntrar;	Poder demonstrar;
Objeto da ação de preservação	se os *SIPs* foram aceitos e transformados em um *AIP*s integralmente ou em parte, ou ainda se foram recusados;	os SIPs são aceitos como um todo ou parte de um eventual objeto de arquivo (isto é, AIP), ou dispostos de outra forma em um modelo registrado.
Comparação	Ambos os requisitos analisados tratam da capacidade do repositório demonstrar se os SIPs submetidos foram aceitos totalmente ou em parte, ou se foram recusado, por meio de um registro.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- atribuir aos *AIPs*, identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por exemplo: Handle System, DOI, URN, PURL);	B2.5 O Repositório tem e utiliza uma convenção de nomenclatura que gera identificadores para todos os objetos arquivados (i.e., AIPs).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Atribuir;	Te Utilizar;
Objeto da ação de preservação	aos *AIPs*, identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos	utiliza uma convenção de nomenclatura que gera identificadores para todos os objetos arquivados.
Comparação	Os requisitos em análise tratam da necessidade de identificadores únicos persistentes para os objetos digitais arquivados.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- no caso de o documento já possuir um identificador único, a ele atribuído no *SIP*, o repositório deverá mantê-lo no *AIP*, ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao do *SIP*;	B2.6 Se identificadores únicos forem associados a SIPs antes de ingeridos, o repositório preserva os identificadores de forma que mantenha uma associação persistente com o resultante arquivado objeto (por exemplo, AIP).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Possuir;	Preserva;
Objeto da ação de preservação	o repositório deverá mantê-lo no *AIP(o identificador único)*, ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao do *SIP*;	o repositório preserva os identificadores de forma que mantenha uma associação persistente com o resultante arquivado objeto (por exemplo, AIP).
Comparação	Os requisitos em análise tratam da necessidade de manter o identificador único persistente atribuído ao SIP, ao AIP.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos (ex.: *PRONOM* - base de dados com registro de formatos mantida pelo arquivo nacional do Reino Unido) e registros de outras informações de representação;	B2.7 O Repositório demonstra que tem acesso às ferramentas e recursos necessários para estabelecer um contexto semântico ou técnico autoritário dos objetos digitais que contém (ou seja, acesso às Informações de Representação Internacionais apropriadas e registros de formato).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ter;	Demonstrar que tem;
Objeto da ação de preservação	- acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos e registros de outras informações de representação;	acesso às ferramentas e recursos necessários para estabelecer um contexto semântico ou técnico autoritário dos objetos digitais que contém.
Comparação	Ambos os requisitos tratam da necessidade de utilizar ferramentas adequadas para monitorar o formato dos arquivos armazenados no repositório.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior;	B2.8 O Repositório de Arquivos/Registros registra Informações de Representação (incluindo formatos) ingeridas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Registrar;	Registrar;
Objeto da ação de preservação	a informação, em um banco de dados local, de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior;	informações de representação (incluindo formatos) ingeridas.
Comparação	Ambos os requisitos analisados versam a respeito do registro das informações de representação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- registrar metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;	B2.9 O Repositório adquire metadados de preservação (ou seja, DIP) para suas Informações de Conteúdo associadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Registrar;	Adquirir;
Objeto da ação de preservação	-metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;	metadados de preservação (ou seja, DIP) para suas Informações de Conteúdo associadas.
Comparação	Os requisitos são analisam a aquisição de metados de preservação associados aos objetos digitais. O RDC-Arq é enfático ao citar os conjuntos de metados imprescindíveis aos documentos arquivísticos.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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);	B2.10 O Repositório tem um processo documentado para testar a compreensibilidade do conteúdo informativo e elevando o conteúdo informativo até o nível acordado de compreensibilidade.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ter;	Ter;
Objeto da ação de preservação	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);	um processo documentado para testar a compreensibilidade do conteúdo informativo e elevando o conteúdo informativo até o nível acordado de compreensibilidade.
Comparação	Os requisitos analisados tratam dos procedimentos para testar a a compreensão da comunidade designada sobre o conteúdo dos documentos digitais. Ambos mostram a necessidade de adequar a compreensão da comunidade à informação dos objetos digitais.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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*;	B2.11 O Repositório verifica cada AIP quanto à completude e exatidão no ponto em que ele é gerado.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Verificar;	Verificar;
Objeto da ação de preservação	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*;	cada AIP quanto à completude e exatidão no ponto em que ele é gerado.
Comparação	Ambos os requisitos tratamda necessidade de verificação de cada pacote AIP quanto à completude e exatidão durante a conversão do SIP em AIP.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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;	B2.12 O Repositório fornece um mecanismo independente para auditoria da integridade da coleta/conteúdo do repositório.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ter;	Fornecer;
Objeto da ação de preservação	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;	um mecanismo independente para auditoria da integridade da coleta/conteúdo do repositório.
Comparação	Os requisitos em análise observam que um mecanismo independente de auditoria da integridade dos objetos digitais coletados.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- documentar todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do *AIP*.	B2.13 O Repositório possui registros contemporâneos de ações e processos de administração que são relevantes para a preservação (criação da AIP).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Documentar;	Possuir;
Objeto da ação de preservação	todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do *AIP*.	registros contemporâneos de ações e processos de administração que são relevantes para a preservação (criação da AIP).
Comparação	Os requisitos em análise tratam dos registros de ações relativas à preservação, que se mostram indispensáveis.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	- estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;	B3.1 O Repositório tem estratégias de preservação documentadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Ser;	Ter;
Objeto da ação de preservação	estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;	estratégias de preservação documentadas.
Comparação	Os requisitos em análise tratam da necessidade de documentar as estratégias de preservação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	- 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);	B3.2 O Repositório dispõe de mecanismos de monitoramento e notificação quando Informações de Representação (incluindo formatos) aproximam-se da obsolescência ou não são mais viáveis.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Verbo não expresso(Especula-se que seja ter, dispor, possuir e sinônimos).	Dispor;
Objeto da ação de preservação	mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável.	mecanismos de monitoramento e notificação quando Informações de Representação (incluindo formatos) aproximam-se da obsolescência ou não são mais viáveis.
Comparação	Apesar do RDC-Arq não apresentar, literalmente, o verbo que indica a ação de preservação, os objetos da ação de preservação são congruentes.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	- mecanismos de mudanças do plano de preservação como resultado do monitoramento;	B3.3 O Repositório possui mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Verbo não expresso (Especula-se que seja ter, dispor, possuir e sinônimos).	Possuir;
Objeto da ação de preservação	mecanismos de mudanças do plano de preservação como resultado do monitoramento;	mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.
Comparação	Apesar do RDC-Arq não apresentar, literalmente, o verbo que indica a ação de preservação, os objetos da ação de preservação são congruentes.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;	B4.1 O Repositório emprega estratégias de preservação documentadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Verbo não expresso (Especula-se que seja, utilizar, ter, dispor, possuir e sinônimos).	Emprega
Objeto da ação de preservação	utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;	estratégias de preservação documentadas.
Comparação	Apesar do RDC-Arq não apresentar, literalmente, o verbo que indica a ação de preservação, os objetos da ação de preservação são congruentes.Interessante ressaltar que o RDC-Arq é assertivo ao mencionar que os metadados de preservação devem fazer parte das estratégias de preservação previstas.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- 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);	B4.2 Repositório implementa/responde a estratégias de armazenamento de objetos de arquivo (i.e., AIP) e migração.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Atender;	Implementar; Responder;
Objeto da ação de preservação	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);	estratégias de armazenamento de objetos de arquivo (i.e., AIP) e migração.
Comparação	Ambos os modelos de requisitos, apesar de serem textualmente distintos, apresentam-se semelhantes conceitualmente. O RDC-Arq apresentar um maior detalhamento quanto aos aspectos da preservação digital. o	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- preservação do documento digital (informação de conteúdo do *AIP*) originalmente admitido no repositório e daquele resultante da última migração;	B4.3 Repositório preserva as Informações de Conteúdo dos objetos de arquivo (ou seja, AIPs).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de preservar e sinônimos afins.	Preservar;
Objeto da ação de preservação	preservação do documento digital (informação de conteúdo do *AIP*) originalmente admitido no repositório e daquele resultante da última migração;	preserva as Informações de Conteúdo dos objetos de arquivo (ou seja, AIPs).
Comparação	Ambos os modelos de requisitos, apesar de serem textualmente distintos, apresentam-se semelhantes conceitualmente. O RDC-Arq cita explicitamente o documento digital (em referência ao documento arquivístico codificado em *bits*).	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- monitoramento constante da integridade dos *AIPs*, por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*); e	B4.4 O Repositório monitora ativamente a integridade dos objetos de arquivo (ou seja, AIPs).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "monitorar".	Monitorar;
Objeto da ação de preservação	integridade dos *AIPs*, por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*);	ativamente a integridade dos objetos de arquivo (ou seja, AIPs).
Comparação	Ambos os modelos de requisitos apresentam-se textualmente muito próximos,e apresentam semelhantes conceituais. O RDC-Arq cita explicitamente os mecanismos para verificação de fixidade e integridade.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- registro de todas as ações de preservação realizadas nos *AIPs*.	B4.5 O Repositório possui registros contemporâneos de ações e processos administrativos que são relevantes para a preservação (Armazenamento de Arquivos).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "registrar".	Monitorar;
Objeto da ação de preservação	as ações de preservação realizadas nos *AIPs*.	registros contemporâneos de ações e processos administrativos que são relevantes para a preservação (Armazenamento de Arquivos).
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente, sendo que o TRAC é assertivo em dizer que os registros devem ser atualizados (contemporâneos).	
Resultado	Parcialmente Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- 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);	B5.1 O Repositório articula os requisitos mínimos de metadados para permitir que a(s) comunidade(s) descubram e identifiquem material de interesse.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "possuir, ter".	Articular;
Objeto da ação de preservação	metadados mínimos que permitam a busca e localização dos documentos - esses metadados devem ser identificadores conhecidos pela comunidade-alvo de usuários	os requisitos mínimos de metadados para permitir que a(s) comunidade(s) descubram e identifiquem material de interesse.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao *AIP* correspondente;	B5.2 O repositório captura ou cria metadados descritivos mínimos e garante que eles sejam associados ao objeto arquivado (i.e., AIP).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "capturar; criar;".	Capturar; Criar;
Objeto da ação de preservação	metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao *AIP* correspondente;	metadados descritivos mínimos e garante que eles sejam associados ao objeto arquivado (i.e., AIP).
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- 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*;	B5.3 O Repositório pode demonstrar que a integridade referencial é criada entre todos os objetos arquivados (ou seja, AIPs) e informações descritivas associadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	Poder; Demosntrar;
Objeto da ação de preservação	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*;	a integridade referencial é criada entre todos os objetos arquivados (ou seja, AIPs) e informações descritivas associadas.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o *AIP* e seus metadados descritivos - nesse caso, o repositório deve ser capaz de restaurar a relação rompida.	B5.4 O Repositório pode demonstrar que a integridade referencial é mantida entre todos objetos arquivados (ou seja, AIPs) e informações descritivas associadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "manter".	Poder; Demosntrar;
Objeto da ação de preservação	permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o *AIP* e seus metadados descritivos - nesse caso, o repositório deve ser capaz de restaurar a relação rompida.	que a integridade referencial é mantida entre todos objetos arquivados (ou seja, AIPs) e informações descritivas associadas.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente. O RDC-Arq adverte sobre a necessidade do RDC-Arq restaurar uma quebra temporária da relação do AIP e seus metadados descritivos.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- divulgação, para a comunidade de usuários, das opções disponíveis de acesso aos documentos e de entrega dos mesmos;	B6.1 O Repositório documenta e comunica à(s) sua(s) comunidade(s) designada(s) que opções de acesso e entrega estão disponíveis.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "divulgar".	Documentar; Comunicar;
Objeto da ação de preservação	opções disponíveis de acesso aos documentos e de entrega dos mesmos para a comunidade de usuários	opções de acesso e entrega estão disponíveis à(s) sua(s) comunidade(s) designada(s)
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- 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;	B6.2 O Repositório implementou uma política de registro de todas as ações de acesso (inclui pedidos, ordens, etc.) que atendam aos requisitos do repositório e informações produtores/depositários.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "implementar".	Implementar;
Objeto da ação de preservação	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;	uma política de registro de todas as ações de acesso (inclui pedidos, ordens, etc.) que atendam aos requisitos do repositório e informações produtores/depositários.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente. O RDC-Arq é assertivo falar sobre a necessidade de controle de acessos.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- concessão de 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;	B6.3 O Repositório assegura que os acordos aplicáveis às condições de acesso são cumpridos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "conceder".	Assegurar;
Objeto da ação de preservação	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;	os acordos aplicáveis às condições de acesso são cumpridos.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- 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;	B6.4 O Repositório tem políticas de acesso documentadas e implementadas (regras de autorização, requisitos de autenticação) consistentes com os contratos de depósito para objetos armazenados. B6.5 Sistema de gerenciamento de acesso ao repositório implementa integralmente a política de acesso.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "conceder".	Ter;
Objeto da ação de preservação	-documentação e implementação de políticas de acesso 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;	- políticas de acesso documentadas e implementadas (regras de autorização, requisitos de autenticação) consistentes com os contratos de depósito para objetos armazenados. - Sistema de gerenciamento de acesso ao repositório implementa integralmente a política de acesso
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente. Importante ressaltar que o RDC-Arq mesclou os dois requisitos abordados no TRAC em um único requisito.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- 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;	B6.6 O Repositório registra todas as falhas de gerenciamento de acesso, e a equipe revisa as falhas inadequadas de incidentes de "negação de acesso".
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do “Repositório”.	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de “registrar”.	Registrar;
Objeto da ação de preservação	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;	todas as falhas de gerenciamento de acesso, e a equipe revisa as falhas inadequadas de incidentes de "negação de acesso".
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente. Importante ressaltar que o RDC-Arq mesclou os dois requisitos abordados no TRAC em um único requisito.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- demonstração de que o processo que gera o *DIP* 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);	B6.7 O Repositório pode demonstrar que o processo que gera a solicitação de objeto(s) digitais (ou seja, DIP) é completado em relação à solicitação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do “Repositório”.	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de “demonstrar”.	Demonstrar; Poder;
Objeto da ação de preservação	o processo que gera o *DIP* atende completamente à requisição do usuário;	que o processo que gera a solicitação de objeto(s) digitais (ou seja, DIP) é completado em relação à solicitação.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente e textualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- demonstração de que o processo que gera o *DIP* 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);	B6.8 O Repositório pode demonstrar que o processo que gera os objetos digitais solicitados (ou seja, DIP) está correto em relação ao pedido.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	Demonstrar; Poder;
Objeto da ação de preservação	o processo que gera o *DIP* está correto em relação ao pedido do usuário;	o processo que gera os objetos digitais solicitados (ou seja, DIP) está correto em relação ao pedido.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente e textualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- demonstração de que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição;	B6.9 Repositório demonstra que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	Demonstrar;
Objeto da ação de preservação	todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição;	todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente e textualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- garantia da autenticidade dos *DIPs*, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original - para isso, um repositório deve ser capaz de demonstrar o processo de construção do *DIP* a partir de um *AIP*.	B6.10 Repositório permite a divulgação de cópias autênticas do original ou objetos rastreáveis até os originais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "garantir; demonstrar".	Permitir;
Objeto da ação de preservação	garantia da autenticidade dos *DIPs*, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original	a divulgação de cópias autênticas do original ou objetos rastreáveis até os originais.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente. O RDC-Arq destaca-se pelo detalhamento, onde especifica o que um repositório digital arquivístico digital deve demonstrar.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- funcionamento do repositório com base num sistema operacional e outros *softwares* de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;	C1.1 Funções de repositório em sistemas operativos bem suportados e outros núcleos *software* infraestrutural.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	Funções de Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "ter".	Embora não expresso, pode-se inferir que a ação de preservação se trata de "ter".
Objeto da ação de preservação	com base num sistema operacional e outros *softwares* de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;	em sistemas operativos bem suportados e outros núcleos *software* infraestrutural.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente. O RDC-Arq é enfático ao dizer que o sistema operacional deve dar suporte à comunidade de usuários.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- adequação dos processos, do *hardware* e do *software* do sistema de *backup* às necessidades do repositório;	C1.2 Repositório garante que possui suporte adequado de hardware e software para backup funcionalmente suficiente para os serviços do repositório e para os dados detidos, por exemplo, metadados associados aos controles de acesso, repositório de conteúdos principais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "adequar".	Garantir; Possuir;
Objeto da ação de preservação	adequação dos processos, do *hardware* e do *software* do sistema de *backup* às necessidades do repositório;	suporte adequado de hardware e software para backup funcionalmente suficiente para os serviços do repositório e para os dados detidos
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas;	C1.3 O Repositório gere o número e a localização das cópias de todos os objetos digitais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "gerenciar".	Gerir;
Objeto da ação de preservação	gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas;	o número e a localização das cópias de todos os objetos digitais.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- 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;	C1.4 O Repositório dispõe de mecanismos para assegurar qualquer/várias cópias de objetos digitais são sincronizados.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Garantir;	Dispor;
Objeto da ação de preservação	o sincronismo entre as cópias de um mesmo documento,	mecanismos para assegurar qualquer/várias cópias de objetos digitais são sincronizados.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- mecanismos efetivos para a detecção de corrupção ou perda de *bits*;	C1.5 O Repositório possui mecanismos eficazes para detectar a corrupção ou perda de bits.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "ter".	Possuir;
Objeto da ação de preservação	mecanismos efetivos para a detecção de corrupção ou perda de *bits*;	mecanismos eficazes para detectar a corrupção ou perda de bits.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- relato dos incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados;	C1.6 Repositório reporta à sua administração todos os incidentes de corrupção ou perda de dados, e medidas tomadas para reparar/substituir dados corrompidos ou perdidos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "relatar".	Embora não expresso, pode-se inferir que a ação de preservação se trata de "reportar".
Objeto da ação de preservação	incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados;	todos os incidentes de corrupção ou perda de dados, e medidas tomadas para reparar/substituir dados corrompidos ou perdidos.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de *hardware*;	C1.7 O Repositório tem processos definidos para a mudança de suportes de armazenamento e/ou hardware (por exemplo *refreshing*, migração).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "prever".	Ter;
Objeto da ação de preservação	previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de *hardware*;	processos definidos para a mudança de suportes de armazenamento e/ou hardware.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;	C1.8 O Repositório tem um processo documentado de gestão de alterações que identifica as alterações a processos críticos que afetam potencialmente a capacidade do repositório para cumprir os seus responsabilidades obrigatórias.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Identificar;	Ter;
Objeto da ação de preservação	alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;	um processo documentado de gestão de alterações que identifica as alterações a processos críticos que afetam potencialmente a capacidade do repositório para cumprir os seus responsabilidades obrigatórias.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- previsão de procedimentos para testar o efeito de mudanças críticas no sistema; e ponderação entre os riscos e os benefícios nas decisões de atualização de *software* de segurança.	C1.9 O Repositório tem um processo para testar o efeito de alterações críticas no sistema.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Prever;	Ter;
Objeto da ação de preservação	o efeito de mudanças críticas no sistema; e ponderação entre os riscos e os benefícios nas decisões de atualização de *software* de segurança.	um processo para testar o efeito de alterações críticas no sistema.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente. O RDC-Arq lembra da importância de levar em conta os riscos e benefícios das decisões de atualização de software e segurança.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	O RDC-Arq não apresenta critério correspondente	C1.10 O Repositório tem um processo para reagir à disponibilidade de novas atualizações de segurança de software com base numa avaliação de risco-benefício.
Agente da ação de preservação		O Repositório
Ação de preservação		Ter;
Objeto da ação de preservação		um processo para reagir à disponibilidade de novas atualizações de segurança de software com base numa avaliação de risco-benefício.
Comparação	Não foi possível reaizar comparação por inexistência de requisito semelhante no RDC-Arq.	
Resultado	ISem correspondências similares Incongruentes	

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - TRAC**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**b. Tecnologias apropriadas**	**C2. Tecnologias adequadas**
Requisitos em análise	O repositório deve adotar uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.	C2.1 O Repositório dispõe de tecnologias de hardware adequadas aos serviços que presta às suas comunidade(s) designada(s) e dispõe de procedimentos para receber e acompanhar notificações e avaliar quando são necessárias alterações de tecnologia de hardware.
		C2.2 O Repositório dispõe de tecnologias de software adequadas aos serviços que presta à sua(s) comunidade(s) designada(s) e dispõe de procedimentos para receber e acompanhar notificações, e avaliar quando são necessárias alterações tecnológicas de software.
Agente da ação de preservação	O repositório	O repositório
		O repositório
Ação de preservação	Deve adotar;	Dispõe
Objeto da ação de preservação	uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.	tecnologias de hardware adequadas aos serviços que presta às suas comunidade(s) designada(s) e dispõe de procedimentos para receber e acompanhar notificações e avaliar quando são necessárias alterações de tecnologia de hardware.
		tecnologias de software adequadas aos serviços que presta à sua(s) comunidade(s) designada(s) e dispõe de procedimentos para receber e acompanhar notificações, e avaliar quando são necessárias alterações tecnológicas de software.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente. O RDC-Arq apresentou os dois requisitos do TRAC em um único requisito.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- análise sistemática de dados, sistemas, pessoas e instalação física;	C3.1 O Repositório mantém uma análise sistemática de fatores tais como dados, sistemas, pessoal, instalações físicas, e necessidades de segurança.
Agente da ação de preservação	O repositório	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "analisar".	Manter;
Objeto da ação de preservação	dados, sistemas, pessoas e instalação física;	uma análise sistemática de fatores tais como dados, sistemas, pessoal, instalações físicas, e necessidades de segurança.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- adoção de procedimentos de controle para tratar adequadamente as necessidades de segurança;	C3.2 O Repositório implementou controles para abordar adequadamente cada uma das necessidades de segurança.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "adotar".	Implementar;
Objeto da ação de preservação	procedimentos de controle para tratar adequadamente as necessidades de segurança;	controles para abordar adequadamente cada uma das necessidades de segurança.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- delineamento de papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema;	C3.3 O pessoal do Repositório tem funções, responsabilidades e autorizações delineadas em relação a implementar alterações no sistema.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O pessoal do repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "delinear".	Ter;
Objeto da ação de preservação	papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema;	funções, responsabilidades e autorizações delineadas em relação a implementar alterações no sistema.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes textualmente e conceitualmente.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Critérios de auditoria e certificação - TRAC
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- plano de prevenção de desastres e de reparação, que inclua, ao menos, um *backup*, *offsite*, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.	C3.4 O Repositório possui plano(s) escrito(s) adequado(s) de preparação para catástrofes e recuperação, incluindo pelo menos uma cópia de segurança externa de toda a informação preservada, juntamente com uma cópia externa do plano(s) de recuperação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O Repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "incluir".	Possuir;
Objeto da ação de preservação	um *backup*, *offsite*, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.	plano(s) escrito(s) adequado(s) de preparação para catástrofes e recuperação, incluindo pelo menos uma cópia de segurança externa de toda a informação preservada, juntamente com uma cópia externa do plano(s) de recuperação.
Comparação	Ambos os modelos de requisitos apresentam-se semelhantes conceitualmente. É importante observar que o RDC-Arq cita a necessidade de manter um *backup* de metadados, documentos e trilhas de auditorias.	
Resultado	Parcialmente similares	

APÊNDICE I - QUADRO COMPARATIVO ENTRE OS REQUISITOS DO RDC-ARQ E O ACTDR

Modelos de Requisitos	**RDC-Arq**	**Critérios de auditoria e certificação - ACTDR**
Seção	**II.2.1 - Infraestrutura organizacional**	**3 Infraestrutura Organizacional**
Grupo	**a. Governança e viabilidade organizacional**	**3.1. Governança e Viabilidade Organizacional**
Requisitos em análise	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.	3.1.1 O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, retenção no longo prazo, gerenciamento e acesso a informações digitais.
Agente da ação de preservação	O repositório	O repositório
Ação de preservação	- ter	Deve ter
Objeto da ação de preservação	como missão o compromisso com a preservação, o gerenciamento e o acesso de longo prazo dos documentos digitais.	uma declaração de missão que reflita um compromisso com a preservação, retenção no longo prazo, gerenciamento e acesso a informações digitais.
Comparação	O requisito do RDC-Arq.é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	3 Infraestrutura Organizacional
Grupo	**a. Governança e viabilidade organizacional**	3.1. Governança e Viabilidade Organizacional
Requisitos em análise	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.	3.1.2 O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório adotará no suporte no longo prazo de sua missão.
		3.1.2.1 O repositório deve ter um plano de sucessão, planos de contingência e / ou custódia adequados, caso o repositório deixe de operar ou a instituição governadora ou financiadora mude substancialmente seu escopo.
		3.1.2.2 O repositório deve monitorar seu ambiente organizacional para determinar quando executar seu plano de sucessão, planos de contingência e / ou acordos de custódia.
Agente da ação de preservação	O repositório	3.1.2 O repositório
		3.1.2.1 O repositório
		3.1.2.2 O repositório
Ação de preservação	ter	3.1.2 Deve ter
		3.1.2.1 Deve ter
		3.1.2.2 Deve monitorar
Objeto da ação de preservação	um plano de sucessão formal, planos de contingência e/ou acordos	3.1.2 um Plano Estratégico de Preservação que define a abordagem que o repositório adotará no suporte no longo prazo de sua missão.
		3.1.2.1 um plano de sucessão, planos de contingência e / ou custódia adequados, caso o repositório deixe de operar ou a instituição governadora ou financiadora mude substancialmente seu escopo.
		3.1.2.2 seu ambiente organizacional para determinar quando executar seu plano de sucessão, planos de contingência e / ou acordos de custódia.
Comparação	O requisito do RDC-Arq.é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**b. Estrutura organizacional e de pessoal**	**A2. Estrutura organizacional e pessoal**
Requisitos em análise	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 O repositório deve ter identificado e estabelecido o deveres que ele precisa executar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir esses deveres.
		3.2.1.1 O repositório deve ter identificado e estabelecido as tarefas que ele precisa executar.
		3.2.1.2 O repositório deve ter o número apropriado de funcionários para apoiar todas as funções e serviços.
		3.2.1.3 O repositório deve ter um programa ativo de desenvolvimento profissional que forneça aos funcionários habilidades e oportunidades de desenvolvimento de conhecimentos.
Agente da ação de preservação	O repositório	3.2.1 O repositório.
		3.2.1.1 O repositório
		3.2.1.2 O repositório
		3.2.1.3 O repositório
Ação de preservação	- Ter; - Manter;	3.2.1 deve ter
		3.2.1.1 deve ter
		3.2.1.2 deve ter
		3.2.1.3 deve ter
Alvo da ação de preservação	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 identificado e estabelecido o deveres que ele precisa executar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir esses deveres.
		3.2.1.1 identificado e estabelecido as tarefas que ele precisa executar.
		3.2.1.2 o número apropriado de funcionários para apoiar todas as funções e serviços
		3.2.1.3 um programa ativo de desenvolvimento profissional que forneça aos funcionários habilidades e oportunidades de desenvolvimento de conhecimentos.
Comparação	O requisito do RDC-Arq.é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Definir a comunidade alvo e sua base de conhecimento;	3.3.1 O repositório deve ter definido sua Comunidade Designada e a(s) base(s) de conhecimento associada(s) e deve ter essas definições adequadamente acessíveis.
Agente da ação de preservação	Embora não expresso, pode-se inferir que se trata do" repositório".	O repositório
Ação de preservação	- Definir	deve ter definido
Objeto da ação de preservação	a comunidade alvo e sua base de conhecimento	sua Comunidade Designada e a(s) base(s) de conhecimento associada(s) e deve ter essas definições adequadamente acessíveis.
Comparação	Os requisitos do RDC-Arq e os critérios do ACTDR são equivalentes.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Possuir políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;	3.3.2 O repositório deve ter Políticas de Preservação em vigor para garantir que seu Plano Estratégico de Preservação seja cumprido.
Agente da ação de preservação	Embora não expresso, pode-se inferir que se trata do "repositório".	O repositório
Ação de preservação	possuir	deve ter
Objeto da ação de preservação	políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;	Políticas de Preservação em vigor para garantir que seu Plano Estratégico de Preservação seja cumprido.
Comparação	O requisito do RDC-Arq.é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Possuir políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem;	3.3.2.1 O repositório deve ter mecanismos para revisão, atualização e desenvolvimento contínuo de suas Políticas de Preservação à medida que o repositório cresce e à medida que a tecnologia e a prática da comunidade evoluem.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Possuir	Deve ter
Objeto da ação de preservação	políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem;	mecanismos para revisão, atualização e desenvolvimento contínuo de suas Políticas de Preservação à medida que o repositório cresce e à medida que a tecnologia e a prática da comunidade evoluem.
Comparação	O requisito do RDC-Arq.é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Documentar permissões legais - por meio de acordos de custódia, normas de procedimentos e outros - que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;	Não apresenta critério similar.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	- Documentar;	
Objeto da ação de preservação	permissões legais que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Relacionar o registro histórico, acima referido, com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;	3.3.3. O repositório deve ter um histórico documentado das alterações em suas operações, procedimentos, software e hardware.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do “Repositório”.	O repositório
Ação de preservação	Relacionar;	Deve ter;
Objeto da ação de preservação	o registro histórico com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;	um histórico documentado das alterações em suas operações, procedimentos, software e hardware.
Comparação	O requisito do RDC-Arq.é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;	Não apresenta critério similar.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do “Repositório”.	
Ação de preservação	Demonstrar;	
Objeto da ação de preservação	a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;	
Comparação	O ACTDR não apresenta critério conceitualmente assemelhado ao requisito do RDC-Arq	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	fazer o registro histórico das mudanças de procedimentos, de *software* e *hardware*;	Não apresenta critério similar.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Fazer;	
Objeto da ação de preservação	o registro histórico das mudanças de procedimentos, de *software* e *hardware*;	
Comparação	O ACTDR não apresenta critério conceitualmente assemelhado ao requisito do RDC-Arq	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia;	3.3.5 O repositório deve definir, coletar, rastrear e fornecer adequadamente suas medidas de integridade da informação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Estar comprometido;	deve definir, coletar, rastrear e fornecer
Objeto da ação de preservação	definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia	adequadamente suas medidas de integridade da informação.
Comparação	Os requisitos do RDC-Arq e os critérios do ACTDR são equivalentes.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Estar comprometido em realizar regularmente uma autoavaliação de seu funcionamento e renovar sua certificação; afetarão seu *status* de certificação (no caso de repositórios já certificados).	3.3.6. O repositório deve se comprometer com um cronograma regular de autoavaliação e certificação externa.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Estar comprometido;	Deve se comprometer
Objeto da ação de preservação	- autoavaliação de seu funcionamento e renovar sua certificação;	com um cronograma regular de autoavaliação e certificação externa.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**C. Transparência de procedimentos e arcabouço político**	**A3. Responsabilidade processual e enquadramento político**
Requisitos em análise	Estar comprometido em notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu *status* de certificação (no caso de repositórios já certificados).	Não apresenta critério similar.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Estar comprometido;	
Objeto da ação de preservação	- notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu *status* de certificação	
Comparação	O ACTDR não apresenta critério conceitualmente assemelhado ao requisito do RDC-Arq.	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - demonstração da capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;	3.4.1 O repositório deve ter processos de planejamento de negócios de curto e longo prazo para manter o repositório ao longo do tempo.
Agente da ação de preservação	O Repositório	O repositório
Ação de preservação	Demonstrar;	Deve ter
Objeto da ação de preservação	capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;	processos de planejamento de negócios de curto e longo prazo para manter o repositório ao longo do tempo.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - revisão e ajustes anuais;	Não apresenta critério similar.
Agente da ação de preservação	Um Repositório	
Ação de preservação	- Revisar - Ajustar	
Objeto da ação de preservação	Sustentabilidade financeira	
Comparação	O ACTDR não apresenta critério conceitualmente assemelhado ao requisito do RDC-Arq.	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere;	3.4.2 O repositório deve ter práticas e procedimentos financeiros transparentes, compatíveis com as normas e práticas contábeis relevantes e auditados por terceiros de acordo com os requisitos legais territoriais.
Agente da ação de preservação	Um Repositório	O repositório
Ação de preservação	Deve ter	Deve ter
Objeto da ação de preservação	- transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere;	práticas e procedimentos financeiros transparentes, compatíveis com as normas e práticas contábeis relevantes e auditados por terceiros de acordo com os requisitos legais territoriais.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**d. Sustentabilidade financeira**	**A4. Sustentabilidade financeira**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos.	3.4.3 O repositório deve ter um compromisso contínuo de analisar e relatar riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).
Agente da ação de preservação	Um Repositório	O repositório
Ação de preservação	Dever	Deve ter
Objeto da ação de preservação	compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos	um compromisso contínuo de analisar e relatar riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Infraestrutura Organizacional**
Grupo	**e. Contratos, licenças e passivos**	**A5. Contratos, licenças e responsabilidades**
Requisitos em análise	- 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 O repositório deve ter e manter contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e / ou aos quais fornece acesso.
		3.5.1.1 O repositório deve ter contratos ou acordos de depósito que especifiquem e transfiram todos os direitos de preservação necessários, e esses direitos transferidos devem ser documentados.
		3.5.1.2 O repositório deve ter especificado todos os aspectos apropriados de aquisição, manutenção, acesso e retirada em acordos escritos com depositantes e outras partes relevantes.
		3.5.1.3 O repositório deve ter políticas escritas que indiquem quando ele aceita a responsabilidade de preservação pelo conteúdo de cada conjunto de objetos de dados enviados.
		3.5.1.4 O repositório deve ter políticas em vigor para lidar com responsabilidades e desafios à propriedade / direitos.
		3.5.2 O repositório deve rastrear e gerenciar os direitos de propriedade intelectual e as restrições ao uso do conteúdo do repositório, conforme exigido pelo contrato de depósito, contrato ou licença.
Agente da ação de preservação	Os contratos, licenças e passivos firmados pelo repositório;	O repositório
		O repositório
		O repositório
		O repositório
		O repositório
		O repositório
Ação de preservação	Dever; Delinear; Ser; Poder;	deve ter e manter
		deve ter
		deve ter
		deve ter
		deve ter
		deve rastrear e gerenciar

Objeto da ação de preservação	-ser claros e mensuráveis; -papéis, responsabilidades, prazos e condições; -facilmente acessíveis ou disponíveis aos interessados. -envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. -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.	contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e / ou aos quais fornece acesso.
		contratos ou acordos de depósito que especifiquem e transfiram todos os direitos de preservação necessários, e esses direitos transferidos devem ser documentados.
		especificado todos os aspectos apropriados de aquisição, manutenção, acesso e retirada em acordos escritos com depositantes e outras partes relevantes.
		políticas escritas que indiquem quando ele aceita a responsabilidade de preservação pelo conteúdo de cada conjunto de objetos de dados enviados.
		políticas em vigor para lidar com responsabilidades e desafios à propriedade / direitos.
		os direitos de propriedade intelectual e as restrições ao uso do conteúdo do repositório, conforme exigido pelo contrato de depósito, contrato ou licença.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**4 Gerenciamento Digital de Objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**4.1 Ingest: Aquisição de Conteúdo**
Requisitos em análise	- identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.);	4.1.1 O repositório deve identificar as informações do conteúdo e as propriedades das informações que o repositório preservará.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Identificar;	Deve identificar
Objeto da ação de preservação	as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.);	as informações do conteúdo e as propriedades das informações que o repositório preservará.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;	4.1.2 O repositório deve especificar claramente as informações que precisam ser associadas a informações específicas de conteúdo no momento de seu depósito.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Especificar;	Deve especificar
Objeto da ação de preservação	a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;	claramente as informações que precisam ser associadas a informações específicas de conteúdo no momento de seu depósito.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;	4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	Repositório
Ação de preservação	Ter;	Deve ter
Objeto da ação de preservação	mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;	mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	
Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter procedimentos para verificar a integridade do *SIP*, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;	4.1.5 O repositório deve ter um processo de ingestão que verifica cada SIP quanto à integridade e correção.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Ter;	Deve ter
Objeto da ação de preservação	procedimentos para verificar a integridade do *SIP*, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;	um processo de ingestão que verifica cada SIP quanto à integridade e correção.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter o controle físico (controle completo dos *bits*) dos documentos transmitidos com cada *SIP*, a fim de preservá-los;	4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Ter;	Deve obter
Objeto da ação de preservação	o controle físico (controle completo dos *bits*) dos documentos transmitidos com cada *SIP*, a fim de preservá-los;	controle suficiente sobre os Objetos Digitais para preservá-los.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo o processo de admissão;	4.1.7 O repositório deve fornecer ao produtor / depositante respostas adequadas nos pontos acordados durante os processos de ingestão.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Fornecer;	Deve fornecer
Objeto da ação de preservação	ao produtor/depositante relatórios do andamento dos procedimentos durante todo o processo de admissão;	ao produtor / depositante respostas adequadas nos pontos acordados durante os processos de ingestão.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- demonstrar em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório; e	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Demonstrar;	
Objeto da ação de preservação	em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório;	
Comparação	O ACTDR não apresenta critério similar ao requisito do RDC-Arq.	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**a. Admissão: captura de documentos digitais**	**B1. Ingestão: aquisição de conteúdos**
Requisitos em análise	- ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação.	4.1.8 O repositório deve ter registros contemporâneos de ações e processos de administração relevantes para a aquisição de conteúdo.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Ter;	Deve ter
Objeto da ação de preservação	registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação	registros contemporâneos de ações e processos de administração relevantes para a aquisição de conteúdo.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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 os componentes-chave do *AIP*: o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixidade, proveniência e contexto), e ainda como esses componentes se relacionam;	4.2.1 O repositório deve ter para cada AIP ou classe de AIPs preservados pelo repositório uma definição associada que seja adequada para analisar o AIP e adequada para as necessidades de preservação de longo prazo.
		4.2.1.1 O repositório deve ser capaz de identificar qual definição se aplica a qual AIP.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
Ação de preservação	Descrever;	deve ter
		deve ser
Objeto da ação de preservação	cada classe de informação a ser preservada pelo repositório, e como ela está implementada - essa descrição deve apontar os componentes-chave do *AIP*: o documento arquivístico, sua informação de representação e as várias categorias de informação descritiva de preservação, e ainda como esses componentes se relacionam;	para cada AIP ou classe de AIPs preservados pelo repositório uma definição associada que seja adequada para analisar o AIP e adequada para as necessidades de preservação de longo prazo.
		capaz de identificar qual definição se aplica a qual AIP.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- descrever minuciosamente as diferentes classes de informação e como os *AIPs* são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes (por exemplo, a imagem *TIFF* que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessárias à imagem *TIFF* que é apresentada para o olho humano);	4.2.1.2 O repositório deve ter uma definição de cada AIP que seja adequada para preservação no longo prazo, permitindo a identificação e análise de todos os componentes necessários nesse AIP.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Descrever;	Deve ter
Objeto da ação de preservação	minuciosamente as diferentes classes de informação e como os *AIPs* são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes.	uma definição de cada AIP que seja adequada para preservação no longo prazo, permitindo a identificação e análise de todos os componentes necessários nesse AIP.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- descrever como os *AIPs* são construídos a partir dos *SIPs*, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do *AIP*;	4.2.2 O repositório deve ter uma descrição de como os AIPs são construídos a partir dos SIPs.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Descrever;	Deve ter
Objeto da ação de preservação	como os *AIPs* são construídos a partir dos *SIPs*, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do *AIP*;	uma descrição de como os AIPs são construídos a partir dos SIPs.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- ser capaz de demonstrar se os *SIPs* foram aceitos e transformados em um *AIP*s integralmente ou em parte, ou ainda se foram recusados;	4.2.3 O repositório deve documentar a disposição final de todos os SIPs.
		4.2.3.1 O repositório deve seguir procedimentos documentados se um SIP não for incorporado a um AIP ou descartado e deve indicar por que o SIP não foi incorporado ou descartado.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
Ação de preservação	Ser capaz de demosntrar;	Deve documentar
		Deve seguir
Objeto da ação de preservação	se os *SIPs* foram aceitos e transformados em um *AIP*s integralmente ou em parte, ou ainda se foram recusados;	a disposição final de todos os SIPs.
		procedimentos documentados se um SIP não for incorporado a um AIP ou descartado e deve indicar por que o SIP não foi incorporado ou descartado.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- atribuir aos *AIPs*, identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por exemplo: Handle System, DOI, URN, PURL);	4.2.4.1 O repositório deve identificar exclusivamente cada AIP dentro do repositório.
		4.2.4.1.1 O repositório deve ter identificadores únicos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
Ação de preservação	Atribuir;	Deve identificar
		Deve ter
		Deve atribuir
Objeto da ação de preservação	aos *AIPs*, identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos	exclusivamente cada AIP dentro do repositório.
		identificadores únicos.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- no caso de o documento já possuir um identificador único, a ele atribuído no *SIP*, o repositório deverá mantê-lo no *AIP*, ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao do *SIP*;	4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do AIP e seus componentes, de modo a serem únicos no contexto do repositório.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Possuir;	Deve atribuir
Objeto da ação de preservação	o repositório deverá mantê-lo no *AIP(o identificador único)*, ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao do *SIP*;	identificadores persistentes do AIP e seus componentes, de modo a serem únicos no contexto do repositório.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos (ex.: *PRONOM* - base de dados com registro de formatos mantida pelo arquivo nacional do Reino Unido) e registros de outras informações de representação;	4.2.4.1.3 A documentação deve descrever qualquer processo usado para alterações em tais identificadores.
		4.2.4.1.4 O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais de duplicação.
		4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e previsíveis do repositório, como número de objetos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	A documentação
		O repositório
		O sistema de identificadores
Ação de preservação	Ter;	Deve descrever
		Deve ser capaz de fornecer
		Deve ser
Objeto da ação de preservação	- acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos e registros de outras informações de representação;	qualquer processo usado para alterações em tais identificadores.
		uma lista completa de todos esses identificadores e fazer verificações pontuais de duplicação.
		adequado para atender aos requisitos atuais e previsíveis do repositório, como número de objetos.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior;	4.2.5 O repositório deve ter acesso às ferramentas e recursos necessários para fornecer informações de representação autorizadas para todos os objetos digitais que ele contém.
		4.2.5.1 O repositório deve ter ferramentas ou métodos para identificar o tipo de arquivo de todos os Objetos de Dados enviados.
		4.2.5.2 O repositório deve ter ferramentas ou métodos para determinar quais informações de representação são necessárias para tornar cada objeto de dados compreensível para a comunidade designada.
		4.2.5.3 O repositório deve ter acesso às informações de representação necessárias.
		4.2.5.4 O repositório deve ter ferramentas ou métodos para garantir que as Informações de Representação necessárias sejam persistentemente associadas aos Objetos de Dados relevantes.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do “Repositório”.	O repositório
		O repositório
		O repositório
		O repositório
		O repositório
Ação de preservação	Registrar;	deve ter
		deve ter
		deve ter
		deve ter
		deve ter
Objeto da ação de preservação	a informação, em um banco de dados local, de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior;	acesso às ferramentas e recursos necessários para fornecer informações de representação autorizadas para todos os objetos digitais que ele contém.
		ferramentas ou métodos para identificar o tipo de arquivo de todos os Objetos de Dados enviados.
		ferramentas ou métodos para determinar quais informações de representação são necessárias para tornar cada objeto de dados compreensível para a comunidade designada.

		acesso às informações de representação necessárias. ferramentas ou métodos para garantir que as Informações de Representação necessárias sejam persistentemente associadas aos Objetos de Dados relevantes.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- registrar metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;	4.2.6 O repositório deve ter processos documentados para adquirir informações de descrição de preservação (PDI) para suas informações de conteúdo associadas e adquiri-las de acordo com os processos documentados.
		4.2.6.1 O repositório deve ter processos documentados para a aquisição da PDI.
		4.2.6.2 O repositório deve executar seus processos documentados para adquirir a PDI.
		4.2.6.3 O repositório deve garantir que o PDI esteja persistentemente associado às informações relevantes do conteúdo.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
		O repositório
		O repositório
Ação de preservação	Registrar;	Deve ter
		Deve ter
		Deve executar
		Garantir
Objeto da ação de preservação	- metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;	processos documentados para adquirir informações de descrição de preservação (PDI) para suas informações de conteúdo associadas e adquiri-las de acordo com os processos documentados.
		processos documentados para a aquisição da PDI.
		seus processos documentados para adquirir a PDI.
		que o PDI esteja persistentemente associado às informações relevantes do conteúdo.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares.	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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 O repositório deve garantir que as Informações de Conteúdo dos AIPs sejam compreensíveis para sua Comunidade Designada no momento da criação do AIP.
		4.2.7.1 O repositório deve ter um processo documentado para testar a compreensibilidade de suas Comunidades Designadas das Informações de Conteúdo dos AIPs em sua criação.
		4.2.7.2 O repositório deve executar o processo de teste para cada classe de informações de conteúdo dos AIPs.
		4.2.7.3 O repositório deve levar as Informações de Conteúdo do AIP até o nível de compreensão exigido, se falhar no teste de compreensão.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
		O repositório
		O repositório
Ação de preservação	Ter;	Deve garantir
		Deve ter
		Deve executar
		Deve levar
Objeto da ação de preservação	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);	que as Informações de Conteúdo dos AIPs sejam compreensíveis para sua Comunidade Designada no momento da criação do AIP.
		um processo documentado para testar a compreensibilidade de suas Comunidades Designadas das Informações de Conteúdo dos AIPs em sua criação.
		o processo de teste para cada classe de informações de conteúdo dos AIPs.
		as Informações de Conteúdo do AIP até o nível de compreensão exigido, se falhar no teste de compreensão.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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*;	4.2.8 O repositório deve verificar cada AIP quanto à integridade e correção no ponto em que é criado.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Verificar;	Deve verificar
Objeto da ação de preservação	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*;	cada AIP quanto à integridade e correção no ponto em que é criado.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- 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;	4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção / conteúdo do repositório.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Ter;	Deve fornecer
Objeto da ação de preservação	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;	um mecanismo independente para verificar a integridade da coleção / conteúdo do repositório.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**B2. Ingestão: criação do pacote de arquivamento**
Requisitos em análise	- documentar todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do *AIP*.	4.2.10 O repositório deve ter registros contemporâneos de ações e processos de administração relevantes para a criação do AIP.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Documentar;	Deve ter
Objeto da ação de preservação	todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do *AIP*.	registros contemporâneos de ações e processos de administração relevantes para a criação do AIP.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	Um repositório digital deve fazer o planejamento da preservação dos documentos sob sua custódia, a fim de enfrentar os problemas trazidos pela obsolescência tecnológica e fragilidade do suporte. Esse planejamento deve ser feito a partir de uma política de preservação digital, ser bem documentado e incluir: - estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;	4.3.1 O repositório deve ter estratégias de preservação documentadas relevantes para suas propriedades.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Ser;	Deve ter
Objeto da ação de preservação	estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;	estratégias de preservação documentadas relevantes para suas propriedades.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	- 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);	4.3.2 O repositório deve ter mecanismos para monitorar seu ambiente de preservação.
		4.3.2.1 O repositório deve ter mecanismos para monitoramento e notificação quando as Informações de Representação forem inadequadas para a Comunidade Designada entender os dados armazenados.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Verbo não expresso (Especula-se que seja ter, dispor, possuir e sinônimos).	Deve ter
Objeto da ação de preservação	mecanismos para monitoramento e notificação quando alguma informação de representação dos documentos no repositório estiver se tornando obsoleta ou inviável.	mecanismos para monitoramento e notificação quando as Informações de Representação forem inadequadas para a Comunidade Designada entender os dados armazenados.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	- mecanismos de mudanças do plano de preservação como resultado do monitoramento;	4.3.3 O repositório deve ter mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Verbo não expresso (Especula-se que seja ter, dispor, possuir e sinônimos).	Deve ter
Objeto da ação de preservação	mecanismos de mudanças do plano de preservação como resultado do monitoramento;	mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**c. Planejamento da preservação**	**B3. Planejamento de Preservação**
Requisitos em análise	- fornecimento de evidências sobre a eficácia do plano de preservação	4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Deve ter	Deve fornecer
Objeto da ação de preservação	fornecimento de evidências sobre a eficácia do plano de preservação	evidências da eficácia de suas atividades de preservação.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Verbo não expresso (Especula-se que seja, utilizar, ter, dispor, possuir e sinônimos).	
Objeto da ação de preservação	utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	ISem correspondências similares	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- 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);	4.4.1 O repositório deve ter especificações de como os AIPs são armazenados no nível de *bit.*
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Atender;	Deve ter
Objeto da ação de preservação	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);	especificações de como os AIPs são armazenados no nível de *bit.*
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR, porém, parcialmente.	
Resultado	Sem correspondências similares	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- preservação do documento digital (informação de conteúdo do *AIP*) originalmente admitido no repositório e daquele resultante da última migração;	4.4.1.1 O repositório deve preservar as informações de conteúdo dos AIPs.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de preservar e sinônimos afins.	Deve
Objeto da ação de preservação	preservação do documento digital (informação de conteúdo do *AIP*) originalmente admitido no repositório e daquele resultante da última migração;	preservar as informações de conteúdo dos AIPs.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- monitoramento constante da integridade dos *AIPs*, por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*);	4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "monitorar".	Deve monitorar
Objeto da ação de preservação	integridade dos *AIPs*, por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*);	ativamente a integridade dos AIPs.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**B4. Armazenamento e preservação/manutenção de AIPs**
Requisitos em análise	- registro de todas as ações de preservação realizadas nos *AIPs*.	4.4.2 O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIPs.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "registrar".	Deve ter
Objeto da ação de preservação	as ações de preservação realizadas nos *AIPs*.	registros contemporâneos de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIPs.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- 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);	4.5.1 O repositório deve especificar requisitos mínimos de informação para permitir que a Comunidade Designada descubra e identifique material de interesse.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "possuir, ter".	deve especificar
Objeto da ação de preservação	metadados mínimos que permitam a busca e localização dos documentos - esses metadados devem ser identificadores conhecidos pela comunidade-alvo de usuários	requisitos mínimos de informação para permitir que a Comunidade Designada descubra e identifique material de interesse.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao *AIP* correspondente;	4.5.2 O repositório deve capturar ou criar informações descritivas mínimas e garantir que elas estejam associadas ao AIP.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "capturar; criar;".	deve capturar ou criar
Objeto da ação de preservação	metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao *AIP* correspondente;	informações descritivas mínimas e garantir que elas estejam associadas ao AIP.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- 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*;	4.5.3 O repositório deve manter uma ligação bidirecional entre cada AIP e suas informações descritivas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	deve manter
Objeto da ação de preservação	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*;	uma ligação bidirecional entre cada AIP e suas informações descritivas.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**e. Gerenciamento de informação**	**B5. Gestão da informação**
Requisitos em análise	- permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o *AIP* e seus metadados descritivos - nesse caso, o repositório deve ser capaz de restaurar a relação rompida.	4.5.3.1 O repositório deve manter as associações entre seus AIPs e suas informações descritivas ao longo do tempo.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "manter".	deve manter
Objeto da ação de preservação	permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o *AIP* e seus metadados descritivos - nesse caso, o repositório deve ser capaz de restaurar a relação rompida.	as associações entre seus AIPs e suas informações descritivas ao longo do tempo.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- divulgação, para a comunidade de usuários, das opções disponíveis de acesso aos documentos e de entrega dos mesmos;	4.6.1 O repositório deve estar em conformidade com as Políticas de Acesso.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "divulgar".	Deve estar
Objeto da ação de preservação	opções disponíveis de acesso aos documentos e de entrega dos mesmos para a comunidade de usuários	em conformidade com as Políticas de Acesso.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- 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;	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "implementar".	
Objeto da ação de preservação	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;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- concessão de 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;	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "conceder".	
Objeto da ação de preservação	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;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- 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;	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "conceder".	
Objeto da ação de preservação	-documentação e implementação de políticas de acesso 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;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- 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;	4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias no gerenciamento de acesso.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "registrar".	Deve registrar e revisar
Objeto da ação de preservação	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;	todas as falhas e anomalias no gerenciamento de acesso.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- demonstração de que o processo que gera o *DIP* 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);	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	
Objeto da ação de preservação	o processo que gera o *DIP* atende completamente à requisição do usuário;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- demonstração de que o processo que gera o *DIP* 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);	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	
Objeto da ação de preservação	o processo que gera o *DIP* está correto em relação ao pedido do usuário;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	ISem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- demonstração de que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição;	4.6.2.1 O repositório deve registrar e agir de acordo com os relatórios de problemas sobre erros nos dados ou respostas dos usuários.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "demonstrar".	deve registrar e agir
Objeto da ação de preservação	todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição;	de acordo com os relatórios de problemas sobre erros nos dados ou respostas dos usuários.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gestão de Objetos Digitais**
Grupo	**f. Gerenciamento de acesso**	**B6. Gerenciamento de acesso**
Requisitos em análise	- garantia da autenticidade dos *DIPs*, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original - para isso, um repositório deve ser capaz de demonstrar o processo de construção do *DIP* a partir de um *AIP*.	4.6.2 O repositório deve seguir políticas e procedimentos que permitam a disseminação de objetos digitais rastreáveis aos originais, com evidências que comprovem sua autenticidade.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "garantir; demonstrar".	deve seguir
Objeto da ação de preservação	garantia da autenticidade dos *DIPs*, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original	políticas e procedimentos que permitam a disseminação de objetos digitais rastreáveis aos originais, com evidências que comprovem sua autenticidade.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- funcionamento do repositório com base num sistema operacional e outros *softwares* de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;	
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "ter".	
Objeto da ação de preservação	com base num sistema operacional e outros *softwares* de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;	
Comparação	O ACTDR não apresenta critério assemelhado ao requisito do RDC-Arq	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- adequação dos processos, do *hardware* e do *software* do sistema de *backup* às necessidades do repositório;	5.1.1.1 O repositório deve empregar vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia. 5.1.1.1.1 O repositório deve ter tecnologias de hardware adequadas aos serviços que fornece às comunidades designadas. 5.1.1.1.2 O repositório deve ter procedimentos para monitorar e receber notificações quando forem necessárias alterações na tecnologia de hardware. 5.1.1.1.3 O repositório deve ter procedimentos para avaliar quando são necessárias alterações no hardware atual. 5.1.1.1.4 O repositório deve ter procedimentos, comprometimento e financiamento para substituir o hardware quando a avaliação indicar a necessidade de fazê-lo. 5.1.1.1.5 O repositório deve ter tecnologias de software apropriadas aos serviços que fornece às comunidades designadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
		O repositório
		O repositório
		O repositório
		O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "adequar".	deve identificar e gerenciar
		deve empregar
		deve ter
		deve ter
		deve ter
		deve ter
Objeto da ação de preservação	adequação dos processos, do *hardware* e do *software* do sistema de *backup* às necessidades do repositório;	os riscos para suas operações e objetivos de preservação associados à infraestrutura do sistema.
		vigilância tecnológica ou outros sistemas de notificação de monitoramento de tecnologia.
		O repositório deve ter tecnologias de hardware adequadas aos serviços que fornece às comunidades designadas.

		procedimentos para monitorar e receber notificações quando forem necessárias alterações na tecnologia de hardware.
		procedimentos, comprometimento e financiamento para substituir o hardware quando a avaliação indicar a necessidade de fazê-lo.
		tecnologias de software apropriadas aos serviços que fornece às comunidades designadas.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas;	5.1.2 O repositório deve gerenciar o número e o local das cópias de todos os objetos digitais.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "gerenciar".	Deve gerenciar
Objeto da ação de preservação	gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas;	o número e o local das cópias de todos os objetos digitais.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- 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;	5.1.2.1 O repositório deve ter mecanismos para garantir que qualquer / várias cópias de objetos digitais sejam sincronizadas.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Garantir;	deve ter
Objeto da ação de preservação	o sincronismo entre as cópias de um mesmo documento,	mecanismos para garantir que qualquer / várias cópias de objetos digitais sejam sincronizadas.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- mecanismos efetivos para a detecção de corrupção ou perda de *bits*;	5.1.1.3 O repositório deve ter mecanismos eficazes para detectar corrupção ou perda de bits.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "ter".	deve ter
Objeto da ação de preservação	mecanismos efetivos para a detecção de corrupção ou perda de *bits*;	mecanismos eficazes para detectar corrupção ou perda de bits.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- relato dos incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados;	5.1.1.3.1 O repositório deve registrar e relatar à sua administração todos os incidentes de corrupção ou perda de dados e devem ser tomadas medidas para reparar / substituir dados corrompidos ou perdidos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "relatar".	Deve registrar e relatar
Objeto da ação de preservação	incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados;	à sua administração todos os incidentes de corrupção ou perda de dados e devem ser tomadas medidas para reparar / substituir dados corrompidos ou perdidos.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de *hardware*;	5.1.1.5 O repositório deve ter processos definidos para a mídia de armazenamento e / ou alteração de hardware (por exemplo, atualização, migração).
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "prever".	deve ter
Objeto da ação de preservação	previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de *hardware*;	processos definidos para a mídia de armazenamento e / ou alteração de hardware (por exemplo, atualização, migração).
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;	5.1.1.6 O repositório deve ter identificado e documentado processos críticos que afetam sua capacidade de cumprir com suas responsabilidades obrigatórias.
		5.1.1.6.1 O repositório deve ter um processo documentado de gerenciamento de mudanças que identifique alterações nos processos críticos que potencialmente afetam a capacidade do repositório de cumprir suas responsabilidades obrigatórias.
		5.1.1.6.2 O repositório deve ter um processo para testar e avaliar o efeito das alterações nos processos críticos do repositório.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
		O repositório
Ação de preservação	Identificar;	deve ter
		deve ter
Objeto da ação de preservação	alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;	identificado e documentado processos críticos que afetam sua capacidade de cumprir com suas responsabilidades obrigatórias.
		um processo documentado de gerenciamento de mudanças que identifique alterações nos processos críticos que potencialmente afetam a capacidade do repositório de cumprir suas responsabilidades obrigatórias.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**a. Infraestrutura de sistema**	**C1. Infraestrutura do sistema**
Requisitos em análise	- previsão de procedimentos para testar o efeito de mudanças críticas no sistema; e ponderação entre os riscos e os benefícios nas decisões de atualização de *software* de segurança.	5.1.1.4 O repositório deve ter um processo para registrar e reagir à disponibilidade de novas atualizações de segurança com base em uma avaliação de risco-benefício.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Prever;	deve ter
Objeto da ação de preservação	o efeito de mudanças críticas no sistema; e ponderação entre os riscos e os benefícios nas decisões de atualização de *software* de segurança.	para registrar e reagir à disponibilidade de novas atualizações de segurança com base em uma avaliação de risco-benefício.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**ACTDR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**b. Tecnologias apropriadas**	**C2. Tecnologias adequadas**
Requisitos em análise	O repositório deve adotar uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.	5.1.1.1.6 O repositório deve ter procedimentos para monitorar e receber notificações quando forem necessárias alterações de software.
		5.1.1.1.7 O repositório deve ter procedimentos para avaliar quando são necessárias alterações no software atual.
		5.1.1.1.8 O repositório deve ter procedimentos, comprometimento e financiamento para substituir o software quando a avaliação indicar a necessidade de fazê-lo.
Agente da ação de preservação	O repositório	O repositório
		O repositório
		O repositório
Ação de preservação	Deve adotar;	deve ter
		deve ter
		deve ter
Objeto da ação de preservação	uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.	ter procedimentos para monitorar e receber notificações quando forem necessárias alterações de software.
		procedimentos para avaliar quando são necessárias alterações no software atual.
		ter procedimentos, comprometimento e financiamento para substituir o software quando a avaliação indicar a necessidade de fazê-lo.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- análise sistemática de dados, sistemas, pessoas e instalação física;	5.2.1 O repositório deve manter uma análise sistemática dos fatores de risco à segurança associados aos dados, sistemas, pessoal e instalações físicas.
Agente da ação de preservação	O repositório	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "analisar".	Deve manter
Objeto da ação de preservação	dados, sistemas, pessoas e instalação física;	uma análise sistemática dos fatores de risco à segurança associados aos dados, sistemas, pessoal e instalações físicas.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- adoção de procedimentos de controle para tratar adequadamente as necessidades de segurança;	5.2.2 O repositório deve ter implementado controles para abordar adequadamente cada um dos riscos de segurança definidos.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "adotar".	Deve ter
Objeto da ação de preservação	procedimentos de controle para tratar adequadamente as necessidades de segurança;	implementado controles para abordar adequadamente cada um dos riscos de segurança definidos.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- delineamento de papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema;	5.2.3 A equipe do repositório deve ter funções, responsabilidades e autorizações delineadas relacionadas à implementação de mudanças no sistema.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	A equipe do repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "delinear".	deve ter
Objeto da ação de preservação	papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema;	funções, responsabilidades e autorizações delineadas relacionadas à implementação de mudanças no sistema.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	ACTDR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Tecnologias, Infraestruturas Técnicas, & Segurança**
Grupo	**c. Segurança**	**C3. Segurança**
Requisitos em análise	- plano de prevenção de desastres e de reparação, que inclua, ao menos, um *backup*, *offsite*, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.	5.2.4 O repositório deve ter planos adequados de preparação e recuperação de desastres por escrito, incluindo pelo menos um backup externo de todas as informações preservadas, juntamente com uma cópia externa do(s) plano(s) de recuperação.
Agente da ação de preservação	Embora não expresso, pode-se inferir que o sujeito se trata do "Repositório".	O repositório
Ação de preservação	Embora não expresso, pode-se inferir que a ação de preservação se trata de "incluir".	deve ter
Objeto da ação de preservação	um *backup*, *offsite*, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.	planos adequados de preparação e recuperação de desastres por escrito, incluindo pelo menos um backup externo de todas as informações preservadas, juntamente com uma cópia externa do(s) plano(s) de recuperação.
Comparação	O requisito do RDC-Arq é conceitualmente assemelhado ao critério do ACTDR.	
Resultado	Similares	

APÊNDICE J - QUADRO COMPARATIVO ENTRE O RDC-ARQ E O CATÁLOGO DE CRITÉRIOS NESTOR

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**a. Governança e viabilidade organizacional**	**Não tem Grupos**
Requisitos em análise	- 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. 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.	1.2 O Repositório Digital assume a responsabilidade pela preservação no longo prazo da informação representada pelos objetos digitais.
		4.6 Continuação das tarefas de preservação é assegurada mesmo para além da existência do Repositório Digital.
Agente da ação de preservação	O repositório	1.2 O repositório
	O repositório	4.6 O repositório
Ação de preservação	Ter;	1.2 Assumir;
	Ter;	4.6 Ser;
Objeto da ação de preservação	- 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. - 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.	1.2 a responsabilidade pela preservação no longo prazo da informação representada pelos objetos digitais.
		4.6 continuação das tarefas de preservação é assegurada mesmo para além da existência do Repositório Digital.
Comparação	O requisito elencado pelo RDC-Arq pode ser observado entre os requisitos do NESTOR quando se compara, a Missão com a responsabilidade do Repositório no longo prazo. Destaca-se que o RDC-Arq é mais assertivo e detalhado se comparado ao critério NESTOR. Quanto à forma que a continuidade dos serviços do repositório pelo RDC-Arq são abordados pelo NESTOR em 4.6 sem todo o detalhamento dedicado no RDC-Arq.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**b. Estrutura organizacional e de pessoal**	**Não tem Grupos**
Requisitos em análise	- 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.	4.3 existem estruturas organizativas adequadas para o Repositório Digital.
		5.1 Todos os processos e responsabilidades foram definidos.
		4.2 Número suficiente de pessoal devidamente qualificado estão disponíveis.
Agente da ação de preservação	O repositório;	4.3 Agente oculto
		5.1 Todos os processos e responsabilidades
		4.2 Subentende-se que seja “o repositório”
Ação de preservação	Ter; Deve manter;	4.3 Existir;
		5.1 Ser;
		4.2 Estar;
Objeto da ação de preservação	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.	4.3 o Repositório digital
		5.1 os processos e responsabilidades
		4.2 Número suficiente de pessoal devidamente qualificado
Comparação	Podemos observar que o requisito do RDC-Arq encontra-se parcialmente descritas nos critérios 4.3, 5.1 e 4.2 do NESTOR, com conceitos próximos.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**c. Transparência de procedimentos e arcabouço político**	**Não tem Grupos**
Requisitos em análise	O repositório deve demonstrar explicitamente seus requisitos, decisões, desenvolvimento e ações que garantem a preservação de longo prazo e o acesso a conteúdos digitais sob seus cuidados. Dessa forma, assegura aos usuários, gestores, produtores e certificadores que está cumprindo plenamente seu papel enquanto um repositório digital confiável. Para tanto, o repositório deve: - definir a comunidade alvo e sua base de conhecimento;	1.3 O Repositório Digital definiu suas comunidade(s) designada(s).
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Definir;	Definir;
Objeto da ação de preservação	a comunidade alvo e sua base de conhecimento	suas comunidade(s) designada(s).
Comparação	O RDC-Arq faz referência em seu requisito, além da comunidade alvo, à sua base de conhecimento. O critério NESTOR não faz essa distinção.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**c. Transparência de procedimentos e arcabouço político**	**Não tem Grupos**
Requisitos em análise	- possuir políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**c. Transparência de procedimentos e arcabouço político**	**Não tem Grupos**
Requisitos em análise	- possuir políticas, procedimentos e mecanismos de atualização, na medida em que o repositório cresce e a tecnologia e práticas da comunidade evoluem;	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**c. Transparência de procedimentos e arcabouço político**	**Não tem Grupos**
Requisitos em análise	- documentar permissões legais - por meio de acordos de custódia, normas de procedimentos e outros - que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;	1.1 O Repositório Digital desenvolveu critérios para a seleção dos seus objetos digitais.
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Documentar;	Desenvolver;
Objeto da ação de preservação	permissões legais - por meio de acordos de custódia, normas de procedimentos e outros - que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;	critérios para a seleção dos seus objetos digitais.
Comparação	Apesar de serem textualmente muito diferentes, conceitualmente, os requisitos tratam do estabelecimento de normas e critérios para a entrada dos objetos digitais no repositório. No Entender deste pesquisador, o Nestor deixou em aberto as formas de entrada. O RDC-Arq foi mais assertivo, neste sentido.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**c. Transparência de procedimentos e arcabouço político**	**Não tem Grupos**
Requisitos em análise	- relacionar o registro histórico, acima referido, com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;	
Requisitos em análise	- demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;	
Requisitos em análise	- fazer o registro histórico das mudanças de procedimentos, de *software* e *hardware*;	
Requisitos em análise	- estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia;	
Requisitos em análise	- estar comprometido em realizar regularmente uma autoavaliação de seu funcionamento e renovar sua certificação; e	
Requisitos em análise	estar comprometido em notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu *status* de certificação (no caso de repositórios já certificados).	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**d. Sustentabilidade financeira**	**Não tem Grupos**
Requisitos em análise	Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos: - demonstração da capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;	4.1 O financiamento adequado do repositório digital é garantido.
Agente da ação de preservação	repositório digital	O financiamento adequado do repositório digital.
Ação de preservação	Deve demonstrar; Obter;	Ser;
Objeto da ação de preservação	recursos financeiros estáveis e contínuos para sustentá-lo, seja por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;	garantia
Comparação	Apesar de textualmente muito diferentes, conceitualmente, ambos os modelos de requisitos visam a estabilidade de recursos financeiros contínuos e sustentáveis.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**d. Sustentabilidade financeira**	**Não tem Grupos**
Requisitos em análise	- revisão e ajustes anuais;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere; e	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos.	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.1 - Infraestrutura organizacional**	**A. Estrutura organizacional**
Grupo	**e. Contratos, licenças e passivos**	**Não tem Grupos**
Requisitos em análise	- 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.	3.1 Existem contratos legais entre os produtores e o repositório digital.
		3.2 No desempenho das suas tarefas de arquivamento, o Repositório Digital age com base em acordos legais.
		12.6 O Repositório Digital adquire metadados adequados para gravar os direitos e condições uso correspondentes.
Agente da ação de preservação	Os contratos, licenças e passivos firmados pelo repositório	3.1 contratos legais
		3.2 o Repositório Digital
		12.6 o Repositório Digital
Ação de preservação	Ser; Delinear; Podem envolver; Devem especificar;	3.1 Existir;
		3.2 Agir;
		12.6 Adquirir;
Objeto da ação de preservação	- papéis, responsabilidades, prazos e condições; - a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. - 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.	3.1 entre os produtores e o repositório digital.
		3.2 com base em acordos legais no desempenho das suas tarefas de arquivamento
		12.6 metadados adequados para gravar os direitos e condições uso correspondentes.
Comparação	Os requisitos e critérios em comparação, mesmo textualmente diferentes entre si, apresentam semelhanças quanto aos objetos de preservação tutelados, especialmente, nestes casos, relativos a papéis , responsabilidades entre produtores e o repositório, bem como a necessidade de especificar acordos legais .	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- identificar as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.);	9.2 O Repositório Digital identifica quais as características dos objetos digitais são importantes para a preservação da informação.
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Identificar;	Identificar;
Objeto da ação de preservação	as propriedades do documento que serão preservadas (ex.: o conteúdo, *layout*, tabela de cor, resolução da imagem, canais de som etc.);	quais as características dos objetos digitais são importantes para a preservação da informação.
Comparação	O requisito do RDC-Arq é muito semelhante conceitualmente ao critério NESTOR, uma vez que ambos identificam as propriedades/ características dos objetos digitais a serem preservados.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- especificar claramente a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;	9.1 O Repositório Digital especifica seus pacotes de informação de submissão (SIP).
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Especificar; Deve estar;	Especificar;
Objeto da ação de preservação	a informação que deve estar associada ao documento (metadados associados) no momento da sua submissão;	seus pacotes de informação de submissão (SIP).
Comparação	O requisito do RDC-Arq é muito semelhante conceitualmente ao critério NESTOR. O objeto de preservação em ambos é o SIP.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- ter mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;	7.1 Ingest: o Repositório Digital garante a autenticidade dos objetos digitais.
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Ter; Autenticar; Garantir;	Garantir;
Objeto da ação de preservação	mecanismos para autenticar a origem dos documentos que estão sendo admitidos no repositório, de forma a garantir sua proveniência;	a autenticidade dos objetos digitais.
Comparação	Os requisitos em análise tratam a respeito de mecanismos de garantia de autenticidade de objetos digitais.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- ter procedimentos para verificar a integridade do *SIP*, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;	6.1 Ingest: o Repositório Digital garante a integridade dos objetos digitais.
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Ter; Verificar; Pode ser;	Garantir;
Objeto da ação de preservação	procedimentos para verificar a integridade do *SIP*, o que pode ser feito por meio de procedimentos automatizados e/ou checagem humana;	a integridade dos objetos digitais.
Comparação	Os requisitos em análise tratam a respeito de mecanismos de garantia de integridade dos objetos digitais.O RDC-Arq cita alguns meios de procedimentos para tal.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- ter o controle físico (controle completo dos *bits*) dos documentos transmitidos com cada *SIP*, a fim de preservá-los;	9.3 O Repositório Digital tem controle técnico dos objetos digitais, a fim de levar a cabo medidas de preservação no longo prazo.
Agente da ação de preservação	O repositório;	O Repositório Digital;
Ação de preservação	Ter;	Ter;
Objeto da ação de preservação	o controle físico (controle completo dos *bits*) dos documentos transmitidos com cada *SIP*, a fim de preservá-los;	controle técnico dos objetos digitais, a fim de levar a cabo medidas de preservação no longo prazo.
Comparação	Ambos os requisitos tratam de controle. Embora eles não sejam textualmente idênticos, o controle físico citado pelo RDC-Arq, pode ser interpretado como controle técnico dos objetos digitais, com o intuito de preservá-los.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- fornecer ao produtor/depositante relatórios do andamento dos procedimentos durante todo o processo de admissão;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- demonstrar em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório; e	1.1 O repositório digital desenvolveu critérios para a seleção dos seus objetos digitais.
Agente da ação de preservação	O repositório;	O Repositório Digital;
Ação de preservação	Demonstrar; Ser;	Desenvolveu;
Objeto da ação de preservação	em que momento a responsabilidade pela preservação do documento submetido (*SIP*) é formalmente aceita pelo repositório;	critérios para a seleção dos seus objetos digitais.
Comparação	Os requisitos analisados tratam de critérios formais para demonstrar a responsabilidade da admissão de pacotes de submissão de informação aceitos pelo repositório.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**a. Admissão: captura de documentos digitais**	**Não tem Grupos**
Requisitos em análise	- ter registros de todas as ações e processos administrativos que ocorrem durante o processo de admissão e são relevantes para a preservação.	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- 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 os componentes-chave do *AIP*: o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixidade, proveniência e contexto), e ainda como esses componentes se relacionam;	10.1 O Repositório Digital define seus pacotes de informação de arquivamento (AIPs).
Agente da ação de preservação	O repositório;	O Repositório Digital;
Ação de preservação	Descrever; Dever; Ser;	Definir;
Objeto da ação de preservação	cada classe de informação a ser preservada pelo repositório, e como ela está implementada - essa descrição deve apontar os componentes-chave do *AIP*: o documento arquivístico, sua informação de representação (informação estrutural e semântica) e as várias categorias de informação descritiva de preservação (fixidade, proveniência e contexto), e ainda como esses componentes se relacionam;	seus pacotes de informação de arquivamento (AIPs).
Comparação	Embora ambos os requisitos tratem da criação do Pacote AIP, o RDC-Arq é bastante detalhista quanto aos metadados necessários às especificidades do documento arquivístico.	
Resultado	Parcialmente similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- descrever minuciosamente as diferentes classes de informação e como os *AIPs* são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes (por exemplo, a imagem *TIFF* que é processada por um sistema pode necessitar de ações de preservação diferentes das ações necessárias à imagem *TIFF* que é apresentada para o olho humano);	10.1 O Repositório Digital define seus pacotes de informação de arquivamento (AIPs).
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Descreve; Ser; Pode necessitar;	Definir;
Objeto da ação de preservação	as diferentes classes de informação e como os *AIPs* são implementados, nos casos em que a especificidade daquelas classes exigir ações de preservação diferentes;	seus pacotes de informação de arquivamento (AIPS).
Comparação	Apesar de ambos os requisitos tratarem sobre as definições necessárias aos Pacotes de Arquivamento de Informação, o RDC-Arq fala sobre as necessidades de especificidades exigidas por diferentes casos de preservação.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- descrever como os *AIPs* são construídos a partir dos *SIPs*, ou seja, apontar todas as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do *AIP*;	10.2 O Repositório Digital cuida de transformar os pacotes de informação de submissão (SIPs) em pacotes de informação de arquivamento (AIPs).
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Descrever; Apontar; Passar; Serem;	Cuidar de transformar;
Objeto da ação de preservação	as transformações pelas quais passarão os documentos e os metadados submetidos, e os metadados a serem adicionados no momento da formação do *AIP*;	os pacotes de informação de submissão (SIPs) em pacotes de informação de arquivamento (AIPs).
Comparação	Apesar de serem conceitualmente similares, conforme podemos observar na comparação acima, o RDC-Arq é mais específico quanto a necessidade de descrição da maneira como os AIPs são transformados em SIPs, bem como os metadados a serem adicionados neste momento.	
Resultado	Parcialmente similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- ser capaz de demonstrar se os *SIPs* foram aceitos e transformados em um *AIP*s integralmente ou em parte, ou ainda se foram recusados;	.
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- atribuir aos *AIPs*, identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos (por exemplo: Handle System, DOI, URN, PURL);	12.1 O repositório digital única e persistentemente identifica seus objetos e seus relacionamentos.
Agente da ação de preservação	O repositório	O Repositório Digital
Ação de preservação	Atribuir;	Identificar;
Objeto da ação de preservação	identificadores que sejam únicos, persistentes e visíveis aos gestores e auditores, de acordo com padrões reconhecidos	seus objetos e seus relacionamentos única e persistentemente.
Comparação	Os requisitos analisados versam sobre identificação única persistente de objetos digitais. O RDC-Arq exemplifica e dá exemplos de padrões conhecidos, e os utiliza em seus AIPs.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- no caso de o documento já possuir um identificador único, a ele atribuído no *SIP*, o repositório deverá mantê-lo no *AIP*, ou criar um outro identificador, que deverá ser associado, de maneira persistente, ao do *SIP*;	
Requisitos em análise	- ter acesso a ferramentas amplamente reconhecidas para apoiar o monitoramento dos componentes digitais dos documentos, tais como diretórios de formatos de arquivos (ex.: *PRONOM* - base de dados com registro de formatos mantida pelo arquivo nacional do Reino Unido) e registros de outras informações de representação;	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- registrar, em um banco de dados local, a informação de representação dos documentos admitidos, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior;	12.3 O repositório digital registra metadados adequados para a descrição estrutural dos objetos digitais.
		12.5 O Repositório Digital adquire metadados adequados para a descrição técnica dos objetos digitais.
Agente da ação de preservação	O repositório	12.3 O Repositório Digital
		12.5 O Repositório Digital
Ação de preservação	Registrar;	12.3 Registrar;
		12.5 Adquirir;
Objeto da ação de preservação	a informação de representação dos documentos admitidos em um banco de dados local, quando essa informação não estiver disponível nas ferramentas mencionadas no ponto anterior	12.3 metadados adequados para a descrição estrutural dos objetos digitais.
		12.5 metadados adequados para a descrição técnica dos objetos digitais.
Comparação	Os requisitos analisados tratam do registro e aquisição de objetos digitais, através de metadados.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- registrar metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;	12.4 O repositório digital registra metadados adequados para documentar todas as alterações feitas pelo repositório digital aos objetos digitais.
		12.6 O repositório digital adquire metadados adequados para gravar os direitos e condições de uso correspondentes.
Agente da ação de preservação	O repositório	12.4 O repositório digital
		12.6 O repositório digital
Ação de preservação	Registrar; Apoiar;	12.4 Registrar;
		12.6 Adquirir;
Objeto da ação de preservação	metadados de preservação associados aos documentos admitidos, de maneira a apoiar sua integridade, localização, legibilidade e proveniência, dentre outros;	12.4 metadados adequados para documentar todas as alterações feitas pelo repositório digital aos objetos digitais.
		12.6 metadados adequados para gravar os direitos e condições de uso correspondentes.
Comparação	Os requisitos analisados observam a necessidade de registrar alterações que os objetos digitais sofrem, através de metadados. Além disso, mostram que é imprescindível gravar direitos e condições de acesso. O RDC-Arq destaca-se por ser mais específico quanto à necessidade dos metadados de preservação.	
Resultado	Parcialmente Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- 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);	2.2 O repositório digital garante que a(s) comunidade(s) designada(s) podem interpretar os objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter; Testar;	Garantir;
Objeto da ação de preservação	os documentos são compreensíveis pela comunidade-alvo e, em caso negativo, adequá-los às necessidades dessa comunidade (ex.: documentos voltados para deficientes visuais);	a(s) comunidade(s) designada(s) podem interpretar os objetos digitais.
Comparação	Ambos os requisitos tratam de observar formas e procedimentos para que a comunidade designada interprete os objetos digitais preservados.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- 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*;	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- 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;	6.1 Ingest: o repositório digital garante a integridade dos objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter; Verificar;	Garantir;
Objeto da ação de preservação	a integridade do conjunto do seu acervo.	a integridade dos objetos digitais.
Comparação	Os requisitos analisados versam sobre mecanismos para verificação de integridade dos objetos digitais no fase de Ingestão (admissão).	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**b. Admissão: criação do pacote de arquivamento**	**Não tem Grupos**
Requisitos em análise	- documentar todas as ações relevantes à preservação dos documentos e que estão relacionadas à criação do *AIP*.	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**c. Planejamento da preservação**	**Não tem Grupos**
Requisitos em análise	- estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;	8 O repositório digital tem um plano estratégico para as suas medidas técnicas de preservação (planejamento de preservação).
		4.4 O repositório digital envolve em planejamento de longo prazo.
Agente da ação de preservação	O repositório	O repositório digital
		O repositório digital
Ação de preservação	Ter; (subentendido)	Ter;
		Envolver;
Objeto da ação de preservação	- estratégias de preservação bem definidas e periodicamente atualizadas, apontando e detalhando cada procedimento a ser adotado, como, por exemplo, a normalização de formatos;	um plano estratégico para as suas medidas técnicas de preservação (planejamento de preservação).
		em planejamento de longo prazo.
Comparação	Ambos os requisitos em análise tratam sobre medidas de preservação no longo prazo, com planejamento adequado.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**c. Planejamento da preservação**	**Não tem Grupos**
Requisitos em análise	- 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);	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**c. Planejamento da preservação**	**Não tem Grupos**
Requisitos em análise	- mecanismos de mudanças do plano de preservação como resultado do monitoramento;	4.5 O repositório digital reage a mudanças substanciais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter;	Reagir;
Objeto da ação de preservação	mecanismos de mudanças do plano de preservação como resultado do monitoramento; e	a mudanças substanciais.
Comparação	Os requisitos analisados versam sobre mecanismos para verificação de integridade dos objetos digitais no fase de Ingestão (admissão).	
Resultado	Compatíveis	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**c. Planejamento da preservação**	**Não tem Grupos**
Requisitos em análise	- 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);	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**c. Planejamento da preservação**	**Não tem Grupos**
Requisitos em análise	- mecanismos de mudanças do plano de preservação como resultado do monitoramento;	4.5 O repositório digital reage a mudanças substanciais.
Agente da ação de preservação	O Repositório	O repositório digital
Ação de preservação	Ter;	Reagir;
Objeto da ação de preservação	mecanismos de mudanças do plano de preservação como resultado do monitoramento; e	a mudanças substanciais.
Comparação	Os requisitos analisados versam sobre mecanismos para verificação de integridade dos objetos digitais no fase de Ingestão (admissão).	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**c. Planejamento da preservação**	**Não tem Grupos**
Requisitos em análise	- fornecimento de evidências sobre a eficácia do plano de preservação.	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**Não tem Grupos**
Requisitos em análise	- utilização das estratégias previstas no planejamento da preservação, que podem ser várias e devem ser registradas nos metadados de preservação;	
Resultado	Sem correspondências similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**Não tem Grupos**
Requisitos em análise	- 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);	10.4 O repositório digital implementa estratégias para a preservação a longo prazo dos pacotes de informação de arquivamento (AIPs).
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Atender;	Implementar;
Objeto da ação de preservação	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);	estratégias para a preservação a longo prazo dos pacotes de informação de arquivamento (AIPs).
Comparação	Os requisitos analisados tratam de estratégias de preservação dos AIPs. Ressalta-se que o RDC-Arq cita, explicitamente, sobre a necessidade de cuidados relativos à migração dos objetos digitais.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**Não tem Grupos**
Requisitos em análise	- preservação do documento digital (informação de conteúdo do *AIP*) originalmente admitido no repositório e daquele resultante da última migração;	
Resultado	Sem correspondências similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**Não tem Grupos**
Requisitos em análise	- monitoramento constante da integridade dos *AIPs*, por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*);	6.2 Armazenamento de arquivo: o repositório digital garante a integridade dos objetos digitais.
		7.2 Armazenamento de arquivo: o repositório digital garante a autenticidade dos objetos digitais.
Agente da ação de preservação	O Repositório	6.2 o repositório digital
		7.2 o repositório digital
Ação de preservação	Monitorar;	6.2 Garantir
		7.2 Garantir
Objeto da ação de preservação	constante da integridade dos *AIPs*, por meio do registro de metadados de fixidade e de *logs* de checagem dessa integridade (por exemplo, *checksum*);	6.2 a integridade dos objetos digitais.
		7.2 a autenticidade dos objetos digitais.
Comparação	Ambos os requisitos analisados tratam do monitoramento da integridade dos objetos digitais. O RDC-Ar trata com maior detalhamento, ao citar textualmente os meios de verificação de fixidade e de integridade.	
Resultado	Parcialmente similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**d. Armazenamento e preservação / manutenção do *AIP***	**Não tem Grupos**
Requisitos em análise	- registro de todas as ações de preservação realizadas nos *AIPs*.	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**e. Gerenciamento de informação**	**Não tem Grupos**
Requisitos em análise	- 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);	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**e. Gerenciamento de informação**	**Não tem Grupos**
Requisitos em análise	- captura ou criação dos metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao *AIP* correspondente;	12.2 O repositório digital grava metadados adequados para o formato formal e descrição de conteúdo-base, descrição e identificação dos objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Capturar; Criar;	Gravar;
Objeto da ação de preservação	metadados mínimos pelo repositório, durante o processo de admissão, e associação desses metadados ao *AIP* correspondente;	metadados adequados para o formato formal e descrição de conteúdo-base, descrição e identificação dos objetos digitais.
Comparação	Os requisitos em análise prescrevem que os repositórios devem capturar / gravar e criar metadados adequados durante o processo de admissão, com a devida descrição e identificação.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**e. Gerenciamento de informação**	**Não tem Grupos**
Requisitos em análise	- 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*;	12.7 A estrutura de embalagem é conservada em todos os momentos.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter;	Ser;
Objeto da ação de preservação	integridade referencial entre os *AIPs* e sua informação descritiva (metadados)	conservada em todos os momentos.
Comparação	Os requisitos em análise tratam da conservação da estrutura da embalagem do pacote, bem como os metadados descritivos.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**e. Gerenciamento de informação**	**Não tem Grupos**
Requisitos em análise	- permanência da integridade referencial, mesmo no caso de quebra temporária da relação entre o *AIP* e seus metadados descritivos - nesse caso, o repositório deve ser capaz de restaurar a relação rompida.	12.7 A estrutura de embalagem é conservada em todos os momentos.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Permanecer;	Ser;
Objeto da ação de preservação	integridade referencial, mesmo no caso de quebra temporária da relação entre o *AIP* e seus metadados descritivos - nesse caso, o repositório deve ser capaz de restaurar a relação rompida.	conservada em todos os momentos.
Comparação	Os requisitos em análise tratam da conservação da estrutura da embalagem do pacote, bem como métodos para recuperar a relação entre o pacote AIP e seus metadados, caso a relação seja temporariamente quebrada.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**f. Gerenciamento de acesso**	**Não tem Grupos**
Requisitos em análise	- divulgação, para a comunidade de usuários, das opções disponíveis de acesso aos documentos e de entrega dos mesmos;	6.3 Acesso: o repositório digital garante a integridade dos objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Divulgar;	Garantir;
Objeto da ação de preservação	opções disponíveis de acesso aos documentos e de entrega dos mesmos;	a integridade dos objetos digitais.
Comparação	Os requisitos em análise tratam do acesso da comunidade designada ao repositório digital. O NESTOR foca na garantia de acesso a objetos digitais íntegros. O RDC-Arq cita, literalmente, a necessidade de se divulgar as opções disponíveis de acesso aos objetos digitais.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**f. Gerenciamento de acesso**	**Não tem Grupos**
Requisitos em análise	- 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;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**f. Gerenciamento de acesso**	**Não tem Grupos**
Requisitos em análise	- concessão de 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;	3.3 Com relação ao uso, o repositório digital age com base em acordos legais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Conceder;	Agir;
Objeto da ação de preservação	- concessão de 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;	com base em acordos legais.
Comparação	Os requisitos em análise tratam do uso / acesso dos objetos digitais disponibilizados à comunidade designada sob condições previamente definidas e a usuários autorizados, tendo como base acordos legais formalizados entre Produtores e o Repositório.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**f. Gerenciamento de acesso**	**Não tem Grupos**
Requisitos em análise	- 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;	6.3 Acesso: o repositório digital garante a integridade dos objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Documentar; Implementar;	Garantir;
Objeto da ação de preservação	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;	a integridade dos objetos digitais.
Comparação	Os requisitos em análise tratam do uso / acesso dos objetos digitais disponibilizados pelos repositórios. O NESTOR é mais abrangente e menos detalhista ao abordar o assunto, pois apenas resume que o acesso deve garantir a integridade dos objetos digitais. O RDC-Arq é mais específico, ao orientar que é primordial que se documente e implemente politicas de acesso que identifiquem e autentifiquem os usuários, como forma de controle de acesso.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**f. Gerenciamento de acesso**	**Não tem Grupos**
Requisitos em análise	- 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;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- demonstração de que o processo que gera o *DIP* 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);	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- demonstração de que o processo que gera o *DIP* 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);	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- demonstração de que todos os pedidos de acesso resultam em uma resposta de aceitação ou rejeição;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.2 – Gerenciamento do documento digital**	**B. Gerenciamento de objetos**
Grupo	**f. Gerenciamento de acesso**	**Não tem Grupos**
Requisitos em análise	- garantia da autenticidade dos *DIPs*, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original - para isso, um repositório deve ser capaz de demonstrar o processo de construção do *DIP* a partir de um *AIP*.	7.3 Acesso: o repositório digital garante a autenticidade dos objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Garantir;	Garantir;
Objeto da ação de preservação	autenticidade dos *DIPs*, por meio da entrega de cópias autênticas dos originais ou da viabilidade de rastreamento auditável da relação entre o *DIP* e o objeto original - para isso, um repositório deve ser capaz de demonstrar o processo de construção do *DIP* a partir de um *AIP*.	a autenticidade dos objetos digitais.
Comparação	Ambos os requisitos analisados tratam da autenticidade de objetos digitais. O RDC-Arq observa , explicitamente, os DIPs, e recomenda que o repositório deve demonstrar o processo de criação do DIP partir do AIP. O NESTOR é mais abrangente, não citando o pacote DIP.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**a. Infraestrutura de sistema**	**Não tem Grupos**
Requisitos em análise	- funcionamento do repositório com base num sistema operacional e outros *softwares* de infraestrutura que tenham um bom suporte do mercado e da comunidade de usuários;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- adequação dos processos, do *hardware* e do *software* do sistema de *backup* às necessidades do repositório;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- gerenciamento do número de cópias de todos os documentos mantidos no repositório, e a localização de cada uma delas;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- 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;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**a. Infraestrutura de sistema**	**Não tem Grupos**
Requisitos em análise	- mecanismos efetivos para a detecção de corrupção ou perda de *bits*;	6.2 Armazenamento de arquivo: o repositório digital garante a integridade dos objetos digitais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter; (Subentendido)	Garantir;
Objeto da ação de preservação	- mecanismos efetivos para a detecção de corrupção ou perda de *bits*;	a integridade dos objetos digitais.
Comparação	Apesar dos modelos de requisitos analisados abordarem de forma diferente o armazenamento de objetos digitais, Apenas o RDC-Arq especifica que deve haver procedimentos para detecção de corrupção ou perda de bits. O NESTOR é mais abrangente, orientando apenas que deve ser garantida a integridade dos objetos digitais, sem comentar/especificar métodos.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**a. Infraestrutura de sistema**	**Não tem Grupos**
Requisitos em análise	- relato dos incidentes de corrupção ou perda de dados eventualmente ocorridos e adoção de medidas para reparação ou substituição desses mesmos dados;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- previsão de procedimentos de atualização de suporte (*refreshing*) e de migração decorrentes do cumprimento do prazo de vida do suporte ou da obsolescência dos componentes de *hardware*;	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**a. Infraestrutura de sistema**	**Não tem Grupos**
Requisitos em análise	- documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;	4.5 O repositório digital reage a mudanças substanciais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter; (Subentendido)	Reagir;
Objeto da ação de preservação	documentação da gestão de mudanças capaz de identificar alterações em processos críticos que afetem a capacidade de o repositório cumprir com suas responsabilidades obrigatórias;	a mudanças substanciais.
Comparação	Os requisitos analisados tratam ambos da capacidade do repositório identificar alterações em seu processo de funcionamento. O RDC-Arq é mais detalhado que o NESTOR, ao recomendar que a sejam documentadas mudanças em seus processos.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**a. Infraestrutura de sistema**	**Não tem Grupos**
Requisitos em análise	- previsão de procedimentos para testar o efeito de mudanças críticas no sistema; e ponderação entre os riscos e os benefícios nas decisões de atualização de *software* de segurança.	4.5 O repositório digital reage a mudanças substanciais.
Agente da ação de preservação	O repositório	O repositório digital
Ação de preservação	Ter; (Subentendido)	Reagir;
Objeto da ação de preservação	- previsão de procedimentos para testar o efeito de mudanças críticas no sistema; e ponderação entre os riscos e os benefícios nas decisões de atualização de *software* de segurança.	a mudanças substanciais.
Comparação	Os requisitos analisados tratam ambos da necessidade do repositório identificar alterações em seu processo de funcionamento. O RDC-Arq é mais detalhado que o NESTOR, ao recomendar que a sejam realizados testes dos efeitos das mudanças realizadas no cinema, bem como que se realize ponderações sobre riscos e benefícios na atualização softwares.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**b. Tecnologias apropriadas**	**Não tem Grupos**
Requisitos em análise	O repositório deve adotar uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.	4.5 O repositório digital reage a mudanças substanciais
Agente da ação de preservação	O Repositório	O repositório digital
Ação de preservação	Adotar;	Reagir;
Objeto da ação de preservação	uma tecnologia de *hardware* e *software* apropriada para os serviços que presta, procedimentos para o recebimento e monitoramento de notificações e para a avaliação da necessidade de mudanças na tecnologia utilizada.	a mudanças substanciais.
Comparação	Os requisitos analisados são compatíveis, uma vez que tratam do mesmo objeto de ação de preservação, que são as mudanças em seus sistemas. O RDC-Arq apresenta-se mais detalhado, ao prescrever procedimentos que a tecnologia de hardware e software devem realizar para monitorar e avaliar a necessidade de atualizações, através de notificações.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**c. Segurança**	**Não tem Grupos**
Requisitos em análise	- análise sistemática de dados, sistemas, pessoas e instalação física;	14 A infraestrutura protege o repositório digital e seus objetos digitais.
Agente da ação de preservação	O Repositório	A infraestrutura
Ação de preservação	Analisar;	Proteger;
Objeto da ação de preservação	análise sistemática de dados, sistemas, pessoas e instalação física;	o repositório digital e seus objetos digitais.
Comparação	Apesar de serem textualmente muito diferentes, os requisitos tratam da proteção do repositório e dos objetos digitais. O RDC-Arq é mais específico, ao citar a necessidade de analisar, sistematicamente, dados, sistemas, pessoas e instalações físicas.	
Resultado	Similares	

Modelos de Requisitos	RDC-Arq	Catalogue of criteria for trusted digital repositories NESTOR
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**c. Segurança**	**Não tem Grupos**
Requisitos em análise	- adoção de procedimentos de controle para tratar adequadamente as necessidades de segurança;	13.2 A infraestrutura de TI implementa os requisitos do sistema de segurança de TI de segurança.
Agente da ação de preservação	O Repositório	A infraestrutura de TI
Ação de preservação	Adotar;	Implementar;
Objeto da ação de preservação	procedimentos de controle para tratar adequadamente as necessidades de segurança;	os requisitos do sistema de segurança de TI de segurança.
Comparação	Os requisitos tratam, ambos, de procedimentos de controle, visando a segurança do repositório. O NESTOR é assertivo ao citar que trata-se de segurança de TI. O RDC-Arq, neste caso, é mais genérico, ao citar apenas segurança, sem detalhamento.	
Resultado	Similares	

Modelos de Requisitos	**RDC-Arq**	**Catalogue of criteria for trusted digital repositories NESTOR**
Seção	**II.2.3 – Tecnologia, infraestrutura técnica e segurança**	**C. Infraestrutura e Segurança**
Grupo	**c. Segurança**	**Não tem Grupos**
Requisitos em análise	- delineamento de papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema; e plano de prevenção de desastres e de reparação, que	Não foi relacionado critério semelhante no Catálogo NESTOR.
Requisitos em análise	- inclua, ao menos, um *backup*, *offsite*, de tudo o que é mantido no repositório (documentos, metadados, trilhas de auditoria etc.), inclusive do próprio plano de reparação.	Não foi relacionado critério semelhante no Catálogo NESTOR.
Resultado	Incongruentes	