UNIVERSIDADE DE BRASÍLIA (UNB)
FACULDADE DE CIÊNCIA DA INFORMAÇÃO (FCI)
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO
(PPGCINF)

REQUISITOS DE SOFTWARES PARA REPOSITÓRIOS DIGITAIS: Uma análise à luz da ISO 16363

Discente: Marcos Sigismundo da Silva
Orientador: Professor Dr. Dalton Lopes Martins

Brasília
Dezembro de 2023

UNIVERSIDADE DE BRASÍLIA (UNB)
FACULDADE DE CIÊNCIA DA INFORMAÇÃO (FCI)
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO
(PPGCINF)

Dissertação de mestrado apresentada à Faculdade de Ciência da Informação da Universidade de Brasília como requisito parcial para a obtenção do título de Mestre em Ciência da Informação. Área de concentração: Gestão, Organização e Comunicação da Informação e do Conhecimento. Linha de pesquisa: Gestão, tecnologias e organização da informação e do conhecimento.

Discente: Marcos Sigismundo da Silva

Orientador: Professor Dr. Dalton Lopes Martins

Brasília
Dezembro de 2023

Dados Internacionais de Catalogação na Publicação (CIP)

S586r

Silva, Marcos Sigismundo da.
Requisitos de softwares para repositórios digitais: uma análise à luz da iso 16363; orientador: Dalton Lopes Martins. – Brasília, 2022.
Dissertação (Mestrado em Ciência da Informação) – Universidade de Brasília, 2022.

1. Repositórios digitais. 2. Certificação 3. Tainacan. I. Dalton Lopes Martins, orient. II Título.

CDU 06.35(100)ISO:004.42

Ficha catalográfica elaborada pelo bibliotecário Marcos Sigismundo da Silva CRB 1/1769

FOLHA DE APROVAÇÃO

AGRADECIMENTOS

RESUMO

Esse trabalho aborda o tema da preservação digital que ganhou relevância crítica na era da informação digital, exigindo uma atualização nas práticas e conceitos tradicionais de manutenção de registros. A obsolescência tecnológica representa um desafio particular, colocando em risco a integridade e autenticidade de objetos digitais. Diante da necessidade de se padronizar as atividades dos Repositórios Digitais Confiáveis, a norma ISO 16363 emerge como um importante mecanismo de certificação, estabelecendo padrões rigorosos para auditorias. A implementação desta norma em software de repositório digital tem o potencial de elevar significativamente os padrões de segurança e conformidade, influenciando positivamente a confiança dos usuários e incentivando a adoção mais ampla dos sistemas. Essa pesquisa teve o objetivo de analisar e propor requisitos de gestão de objetos digitais, para estudos e construção de software de gestão de objetos digitais em ambientes confiáveis de preservação digital com base na norma ISO 16363. O resultado dessa análise foi aplicado ao sistema Tainacan, software livre brasileiro para criação de repositórios digitais, que demonstrou carências nos critérios selecionados, enfatizando a necessidade de aprimoramentos em sua estrutura tecnológica e informacional para garantir a integridade do acervo ao longo do tempo. A eventual conformidade do Tainacan com essas diretrizes poderá revolucionar as práticas de preservação e acesso digital. Além de expandir sua aplicabilidade, isso poderá beneficiar várias partes interessadas, incluindo acadêmicos e instituições, focados na preservação eficiente e no acesso duradouro a dados e objetos digitais.

Palavras-chave: Repositórios Digitais; Certificação Digital; ISO 16363, Preservação Digital; Tainacan; Objetos digitais.

ABSTRACT

This work addresses the critically relevant theme of digital preservation in the digital information era, necessitating an update to traditional practices and concepts of record maintenance. Technological obsolescence poses a particular challenge, jeopardizing the integrity and authenticity of digital objects. In light of the need to standardize the activities of Trustworthy Digital Repositories, the ISO 16363 standard emerges as a significant certification mechanism, establishing stringent standards for audits. The implementation of this standard in digital repository software has the potential to significantly raise security and compliance standards, positively influencing user trust and encouraging broader adoption of systems. This research aimed to analyze and propose requirements for the management of digital objects, for studies and the construction of digital object management software in reliable digital preservation environments based on the ISO 16363 standard. The outcome of this analysis was applied to the Tainacan system, a Brazilian open-source software for creating digital repositories, which revealed deficiencies in the selected criteria, emphasizing the need for improvements in its technological and informational structure to ensure the integrity of the collection over time. The eventual compliance of Tainacan with these guidelines has the potential to revolutionize digital preservation and access practices. In addition to expanding its applicability, this could benefit various stakeholders, including academics and institutions, focused on efficient preservation and enduring access to digital data and objects..

Keywords: Digital Repositories; Digital Certification; ISO 16363, Digital Preservation; Tainacan; Digital Objects.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AIP	Pacote de armazenamento de informação
API	Application Programming Interface
CCSDS	Consultative Committee for Space Data System
CONARQ	Conselho Nacional de Arquivos
CPA	*Commission on Preservation & Access*
CRL	Centro de Bibliotecas de Pesquisa
DIP	Pacote de Informação para Disseminação
DPC	Digital Preservation Coalition
DRAMBORA	*Digital Repository Audit Method Based on Risk Assessment*
EPUB	*Electronic Publication*
FUNARTE	Fundação Nacional das Artes
IBICT	Instituto Brasileiro de Informação em Ciência e Tecnologia
IBRAM	Instituto Brasileiro de Museus
IPHAN	Instituto do Patrimônio Histórico e Artístico Nacional
ISO	*International Organization for Standardization*
MPEG	*Moving Picture Experts Group*
NARA	*National Archives and Records Administration*
NDSA	*National Digital Stewardship Alliance*
NESTOR	*“network” and “storage”*
OAI-PMH	*Open Archives Initiative Protocol for Metadata Harvesting*
OAIS	*Open Archive Information System*
OCLC	*Online Computer Library Center*
PDI	Preservation Description Information
RIs	Repositórios Instictucionais
RLG	*Research Library Group*
SAAI	Sistema Aberto de Arquivamento de Informação
SIP	Pacote de submissão de informação

SIRF	*Self-contained Information Retention Format*
TRAC	Trusted Repository Audit Checklist
UNAM	Universidade Nacional Autónoma de México

SUMÁRIO

1 INTRODUÇÃO

No advento da era digital, a preservação digital assume papel central na proteção do patrimônio intelectual e cultural das instituições. A preservação digital se estabelece como esforço essencial para assegurar a disponibilidade contínua de recursos digitais, enfatizando sua relevância no contexto contemporâneo, onde a obsolescência tecnológica e os riscos de degradação digital ameaçam a integridade e o acesso a longo prazo a dados e documentos importantes.

A preservação digital tornou-se assunto cada vez mais importante na era da informação digital e preocupação constante por parte dos profissionais da informação (Márdero Arellano, 2008). Inicialmente a preservação centrava-se na manutenção de documentos em formatos físicos, mas o advento das tecnologias de informação e comunicação tem requerido uma reformulação conceitual e prática da preservação. Especificamente, a obsolescência tecnológica representa um desafio significativo, ameaçando a fidedignidade e autenticidade de objetos digitais. Verifica-se a necessidade de garantir que os objetos digitais sejam gerenciados e mantidos adequadamente preservando sua integridade e acessibilidade a longo prazo, por meio de normas e procedimentos adequados (Corda; Viñas; Vallefín, 2020).

Os documentos eletrônicos, sejam eles fotografias, vídeos, áudios, dados de pesquisa precisam ter sua preservação adequada. Esse processo visa garantir que os objetos digitais não se percam ou sejam alterados inadvertidamente, tornando-se indisponíveis para as gerações futuras e dificultando os esforços para a preservação do patrimônio cultural, científico, histórico e social.

Um dos aspectos da preservação digital é o desenvolvimento e uso de repositórios de digitais. Para Camargo e Vidotti (2008) esses sistemas se apresentam como um meio seguro para o armazenamento, gerenciamento, tratamento, recuperação, uso, preservação e compartilhamento de produções acadêmicas e científicas. Qualquer repositório pode se enquadrar nessas características, entretanto, é necessário aplicar determinados procedimentos para garantir a confiabilidade de todo o ambiente ao longo do tempo.

Os repositórios de preservação digital desempenham um papel crítico na garantia da disponibilidade e acessibilidade de longo prazo dos objetos digitais.

Também garantem que o conteúdo digital seja mantido adequadamente ao longo do tempo, com medidas para preservar sua autenticidade, integridade e para garantir sua usabilidade e acessibilidade contínuas. Dado o reconhecimento da importância dos repositórios de preservação digital, ao longo dos últimos anos diversos padrões e diretrizes foram desenvolvidos com objetivo de viabilizar que os repositórios de preservação digital sejam projetados e operados adequadamente.

Um desses padrões propostos é a ISO 16363. Essa norma internacional estabelece critérios e procedimentos para auditoria e certificação de repositórios digitais confiáveis, enfatizando a preservação a longo prazo e o acesso contínuo a conteúdos digitais. Ela define as melhores práticas para garantir a integridade, a autenticidade e a segurança da informação armazenada. Além disso, a norma serve como um guia para a implementação e avaliação de processos de gestão de repositórios digitais. A adoção dessa norma ajuda a garantir que os repositórios de preservação digital sejam projetados e operados adequadamente e que o conteúdo digital seja gerenciado e preservado adequadamente a longo prazo (Lehmkuhl; Macedo; Silva, 2018).

O gerenciamento dos objetos digitais é um dos itens críticos da preservação digital. A ISO 16363 fornece diretrizes para a identificação, organização e gestão adequados, incluindo recomendações para a criação de objetos digitais, gestão dos seus metadados e gerenciamento de seu ciclo de vida, desde a criação até a preservação e o acesso.

O acesso ao conteúdo preservado é outra instância importante da preservação digital. A norma aborda diretrizes para gerenciamento de acesso do usuário e a proteção do conteúdo digital contra uso não autorizado. Ao aderir a essas diretrizes, os repositórios de preservação digital podem garantir que o conteúdo digital seja adequadamente gerenciado, preservado e disponibilizado, garantindo que permaneça acessível e utilizável.

Para a gestão de repositórios digitais, podem ser usados softwares de código aberto ou software livre específicos para esse fim. Embora frequentemente utilizados de forma intercambiável, esses termos têm conceitos distintos com implicações significativas para o desenvolvimento, distribuição e utilização. O software de código aberto refere-se a programas cujo código-fonte é disponibilizado publicamente,

permitindo a revisão, alteração e redistribuição por terceiros. No entanto, essa categoria não abrange, necessariamente, a liberdade implícita no conceito de software livre, que não só garante o acesso ao código-fonte, mas também defende quatro liberdades fundamentais: a liberdade de usar, estudar, modificar e redistribuir o software. Enquanto o software de código aberto pode ser guiado por uma variedade de licenças, algumas das quais podem impor restrições ao uso ou redistribuição, o software livre adere rigorosamente a princípios que visam promover a autonomia do usuário (Stallman, 2002; Perens, 1999).

O uso do software livre tornou-se cada vez mais popular no campo da preservação digital. Ao fornecer uma solução econômica e flexível para o desenvolvimento e operação de repositórios de preservação digital. Além disso, o uso de software de código aberto pode permitir maior colaboração e compartilhamento de recursos entre as instituições, levando a um ecossistema de preservação digital mais sustentável e interoperável (Camargo; Vidotti, 2008).

Diante da necessidade de sistemas mais flexíveis, viáveis economicamente e sustentáveis, o Tainacan surge como uma alternativa de software livre que se enquadra nos aspectos descritos acima para criação de repositórios digitais. O Tainacan, um sistema *open-source* dedicado à administração de repositórios digitais, foi concebido para otimizar a gestão e a apresentação de conteúdos digitais em páginas eletrônicas que utilizam a estrutura do sistema gestor de conteúdos *Web* chamado *Wordpress*. O Tainacan disponibiliza uma gama diversificada de funcionalidades, incluindo a criação de acervos digitais, a inserção de metadados detalhados e a personalização de modos de exibição. Sua integração com páginas que operam sob o *Wordpress* ocorre de forma simplificada, mediante a inserção de plugin compatível com a plataforma.

Para a realização da pesquisa, foi analisada a ISO 16363 com vistas a identificar requisitos de software para tratamento dos objetos digitais em diferentes momentos do fluxo de preservação no repositório digital. Após a análise, foram propostos parâmetros e recomendações de uso para aplicação dos requisitos. Os resultados dessa análise foram aplicados ao software Tainacan para verificar até que ponto esse sistema atende a norma, indicando, quando possível, os pontos para desenvolvimento de novas funcionalidades ou melhorias.

Pretende-se com os resultados desta pesquisa, fornecer uma contribuição para o campo da preservação digital, demonstrando como melhor adequar as tecnologias referentes aos repositórios digitais confiáveis a ISO 16363, oferecendo orientação para instituições e organizações que buscam soluções tecnológicas para suas necessidades.

1.1 PROBLEMA

Considerar os requisitos apresentados pela ISO 16363 na gestão de repositórios de preservação digital pode trazer benefícios importantes, porém há alguns desafios e questões que devem ser consideradas. Um exemplo é a necessidade de padronizar nos softwares os requisitos estabelecidos pela norma, para entrarem conforme as diretrizes de tratamento dos objetos digitais e transparência dos processos.

A ISO 16363 requer um alto nível de conhecimento técnico para ser implementada e mantida. Encontrar e reter o conhecimento necessário, pode ser difícil, para as instituições que precisam certificar seus ambientes e seus softwares de repositório digital, principalmente em face da rápida evolução das tecnologias de preservação digital. Apesar da norma possuir uma sessão sobre a segurança do sistema informatizado, na totalidade não ficam muito claro quais são os itens que especificam requisitos para os softwares de repositório digital e como adequar os sistemas a esses requisitos

Diante da falta de clareza em se saber, especificamente, os requisitos de software na norma, surge a questão: É possível, no atual contexto da preservação digital de longo prazo, a formulação de critérios, recomendações e parâmetros de uso na construção de sistemas de gestão de objetos digitais a partir da ISO 16363?

1.2 OBJETIVO GERAL

Sob a égide da norma ISO 16363, propor requisitos de avaliação para estudos e construção de software de gestão de objetos digitais em ambientes confiáveis de preservação digital.

1.2.1 Objetivos específicos

- Delimitar os critérios da norma ISO 16363 que devem ser atendidos especificamente pelo software de repositórios digitais em suas rotinas automatizadas.
- Propor requisitos básicos de gestão de objetos digitais (com critérios, recomendações e parâmetros de uso), a partir do estudo dos itens da norma para construção de sistemas de gestão de objetos digitais.
- Provar a aplicabilidade dos requisitos levantados com a análise do software Tainacan em relação aos itens da norma ISO 16363.

1.2.2 Pressupostos

- A norma ISO 16363 possui critérios específicos para determinar como o software de repositório digital deve automatizar rotinas no ambiente de preservação.
- É possível estabelecer requisitos de gestão de objetos digitais, a partir da ISO 16363, destacando o papel do software no processo.

2 JUSTIFICATIVA

A preservação digital emerge como um campo de vital importância na salvaguarda da memória coletiva e do conhecimento humano na era digital. Com a transição acelerada para formatos digitais, a manutenção do acesso a longo prazo de documentos, imagens, dados e demais conteúdos digitais torna-se tarefa prioritária. Tal preservação assegura que gerações futuras possam ter acesso a um legado de informações com valor cultural, histórico, científico e educacional. A preservação pode proteger contra a obsolescência tecnológica, os riscos de perda por deterioração de mídias digitais e as ameaças cibernéticas. No contexto acadêmico e de pesquisa, a preservação digital é fundamental para garantir a continuidade das investigações e para assegurar que dados de pesquisa permaneçam íntegros, autênticos e acessíveis em repositórios digitais confiáveis.

A ISO 16363 é uma norma internacional que estabelece requisitos para a confiabilidade e sustentabilidade de repositórios digitais, visando assegurar a preservação de longo prazo de conteúdos digitais. Ela define critérios e práticas recomendadas para a avaliação da capacidade desses repositórios em proteger e manter o acesso aos dados que armazenam. Esta norma é parte importante para orientar organizações na implementação e manutenção de sistemas de preservação digital eficazes. Para Santos e Flores (2020) a norma contém diretrizes que dão base, em diversas dimensões, para avaliar a confiabilidade de um repositório digital e certificá-lo por órgão ou entidade competente para tal.

A utilização da ISO 16363 em softwares para repositórios de preservação digital pode fornecer um nível de garantia aos usuários e partes interessadas de que o repositório de preservação digital atende a um conjunto de padrões mínimos para o gerenciamento e preservação de conteúdo digital. A aplicação da norma pode aumentar a confiança dos usuários no repositório e no conteúdo digital armazenado nele, levando a uma maior confiança e adoção do repositório.

Bodero Poveda, Giusti e Morales Alarcón (2021) consideram que a norma permite classificar as informações relacionadas à preservação digital todos os aspectos envolvidos nos critérios para infraestrutura organizacional, gestão do objeto digital e gestão da infraestrutura de segurança, possibilitando dar perspectivas gerais de análise estratégica do ambiente de preservação para a instituição.

Além dessas perspectivas, o uso de padrões, como a ISO 16363 ou a ISO 14721 *Open Archival Information System* (OAIS), pode promover a interoperabilidade de repositórios de preservação digital. Para Santos e Flores (2020), ao aderir a um conjunto comum de especificações, os repositórios digitais podem intercambiar objetos digitais e metadados, promovendo, em última análise, maior colaboração e compartilhamento de recursos, podendo levar ao desenvolvimento de uma infraestrutura de preservação digital mais forte e segura, garantindo a preservação de longo prazo do conteúdo digital.

Com a implementação da ISO 16363 é possível planejar uma estrutura para melhoria contínua dos repositórios de preservação digital, pois a norma fornece um conjunto de melhores práticas para o gerenciamento e preservação de conteúdo digital e, ao aderir a essas diretrizes, os repositórios podem avaliar e melhorar continuamente seus processos e sistemas, tanto de forma autônoma quanto de certificadores externos, conforme apontam Santos e Flores (2020).

A publicação da resolução 43, lançada pelo Conselho Nacional de Arquivos (CONARQ), também contribuiu com a visibilidade da ISO 16363 em nível nacional, ao usá-la como base para sua elaboração. Essa resolução, apresenta requisitos que um repositório digital deve seguir para poder ser considerado confiável, independentemente do tipo de material digital (arquivístico ou não). Braga, Holanda e Pignataro (2022) falam sobre como a Resolução 43 ganhou importância no cenário nacional devido a sua adesão por grande quantidade de instituições.

Diante do exposto, entende-se a ISO 16363 como norma relevante para nortear a implantação de repositórios digitais confiáveis. Entretanto, devida a sua complexidade e abrangência do seu conteúdo, faz-se necessária análise dos requisitos para determinar como os softwares de repositório digital podem se adequar à gestão dos objetos digitais no fluxo da preservação.

Para validar os requisitos propostos, após a análise da norma, foi necessário selecionar um software livre para repositórios digitais. Tendo em vista o histórico do investimento brasileiro na construção e promoção do software livre, bem como os avanços nacionais na promoção desse tipo de sistema, optou-se por utilizar o software Tainacan durante a fase aplicada da pesquisa. O Tainacan é resultado de uma pesquisa nacional bem-sucedida, que tem promovido uma revolução na forma como

as instituições de cultura têm gerido seus acervos. Sua flexibilidade permite adaptar a entrada de dados para qualquer tipo de acervo, desde os mais genéricos e simples, como relatórios de projetos até conjuntos complexos de metadados. Tem sido amplamente implementado em museus, por incentivo do Instituto Brasileiro de Museus (IBRAM), em instituições de ensino, instituições privadas e terceiro setor.

Ao propor a análise da norma, fazer a proposição dos requisitos necessários para o software tratar os objetos digitais e aplicar essa análise no software Tainacan, essa dissertação se encaixa na linha de pesquisa: Gestão, tecnologias e organização da informação e do conhecimento da Faculdade de Ciência da Informação da Universidade de Brasília, por fornecer uma contribuição para o campo da preservação digital, oferecendo orientação para instituições e organizações que buscam soluções tecnológicas para suas necessidades diante da norma ISO 16363.

3 CONCEITOS GERAIS E REVISÃO DE LITERATURA

Para se entender melhor a preservação digital no contexto da ciência da informação, é indispensável realizar um levantamento dos fundamentos teóricos e metodológicos que norteiam algumas das ações implementadas nesta área. Especialistas em ciência da informação têm se dedicado a estabelecer e refinar práticas e normas que garantam a manutenção e o acesso contínuo a conjuntos de dados e documentos digitais ao longo do tempo. A revisão da literatura em questão fornece um panorama descritivo dos principais apontamentos estabelecidos desde a última década do século XX relacionados à preservação digital e à manutenção do acesso à informação científica em formatos digitais de maneira duradoura. Estas análises são fruto do trabalho de investigadores do campo da ciência da informação e áreas correlatas, que consideram diferentes preceitos capazes de esclarecer o processo de preservação digital como elemento intrínseco ao ciclo de vida da informação.

3.1 O REPOSITÓRIO DIGITAL PARA A CIÊNCIA DA INFORMAÇÃO

Os repositórios digitais, ambiente digital para gestão informacional, tendem a assumir uma posição de destaque no campo da Ciência da Informação, funcionando como pilares para a preservação e disseminação do conhecimento. São ferramentas importantes para garantir o acesso contínuo e a autenticidade de registros científicos, culturais e educacionais em um mundo cada vez mais digitalizado. O gerenciamento eficiente desses repositórios implica não apenas na salvaguarda do legado digital para gerações futuras, mas também na promoção de uma infraestrutura sustentável para pesquisa, inovação e educação.

Em 1934, o belga Paul Otlet, publicou sua obra intitulada "*Traité de documentation*" (Otlet, 2004) que contribuiu com as bases do que seria a ciência da informação. Aqui se entendia o termo “documentação” como as atividades de coleta, conservação, pesquisa e divulgação dos documentos. Entre suas características mais importantes estavam a capacidade de refletir rapidamente sobre novas informações e agrupar o que estava disperso para facilitar o acesso (Pedroso Izquierdo, 2004).

A maioria dos estudiosos do assunto enquadra o surgimento da ciência da informação na década de 1950, após o fim da guerra, quando houve uma explosão de informações que demandava um grande esforço para controlar e organizar com as ferramentas, de organização da informação, até então utilizadas (Araújo, 2014).

Saracevic (1995), apontou as três características principais que fazem parte da existência da ciência da informação: a interdisciplinaridade, a tecnologia da informação e sua participação na evolução da sociedade da informação. Estas características tendem a colocar a ciência da informação no centro da organização e preservação do patrimônio cultural das instituições, que carecem dessas ações.

No campo da ciência da informação, os repositórios digitais são importantes por fornecerem um local central para a gestão das informações digitais, tornando mais fácil aos pesquisadores encontrar e acessar o que precisam. Ademais, tonaram-se meios de garantir também a preservação a longo prazo e a acessibilidade da informação digital (Shintaku; Meirelles, 2010).

Ao falar em sistemas de gestão de objetos digitais, os repositórios digitais aparecem como ferramentas para o armazenamento, organização e preservação das informações que dão suporte à pesquisa. Os pesquisadores têm nessas ferramentas a expectativa de um local seguro para acessar conteúdos autênticos. Assim, os repositórios digitais assumem o papel do ambiente gestor do patrimônio informacional de arquivos, bibliotecas e museus.

Os repositórios digitais podem ajudar a mitigar os riscos de perda ou degradação devido à obsolescência tecnológica, falhas de hardware ou software, fornecendo um ambiente seguro e estável para armazenar informações digitais e usando as melhores práticas e tecnologias para preservar as informações ao longo do tempo. Guardar essas informações é especialmente importante para informações que precisam ficar disponíveis para uso futuro, tais como as informações que suportam o processo científico.

Percebe-se que os autores que abordam os repositórios digitais como tema de estudo, concordam que essas ferramentas podem tornar mais fácil para os pesquisadores compartilharem seu trabalho com outros estudiosos, tanto dentro de suas instituições quanto fora delas, podendo acelerar o ritmo das pesquisas, facilitando a colaboração e o compartilhamento de conhecimento.

Os repositórios digitais assumem grande importância para a ciência da informação, pois ajudam a preservar informações digitais, fornecendo um ambiente seguro e estável para armazenar informações digitais, usando as melhores práticas e tecnologias para preservá-las ao longo do tempo.

3.2 REPOSITÓRIO DIGITAL: análise dos conceitos

O primeiro repositório digital surgiu no início da década de 1991 (Shintaku, Seabra Junior, 2019) nos Estados Unidos e intitulado *ArXiv5* com abrangência nas áreas da Ciência da Computação, Física, Matemática e Ciências Não Lineares. O Repositório ArXiv foi criado com um experimento para testar modelos diferentes de publicação no processo de comunicação científica.

Os repositórios digitais são uma alternativa ao acesso, disseminação e preservação da produção científica a partir do final do século XX. A Iniciativa dos Arquivos Abertos ou *Open Archives Initiative* (OAI) propiciou novas possibilidades para o processo de comunicação científica por meio da inserção dos repositórios institucionais de acesso aberto para organizar, disseminar e prover o acesso às informações científicas (Shintaku; Meirelles, 2010).

Para Vechiato *et al. (*2017), repositórios digitais são sistemas disponíveis na internet que fornecem recursos tecnológicos abertos e interoperáveis, promovendo a facilidade de depósito e acesso a documentos digitais, para divulgar e dar acesso à produção intelectual, ampliando a visibilidade da produção e comunicação científica.

Trata-se de coleções de objetos digitais armazenados em ambiente tecnológico (servidor) e geridos por um software destinado para esse fim. É uma ideia genérica do conceito, ou seja, bibliotecas digitais (ou repositórios digitais) são plataformas para armazenamento e gestão de objetos digitais (Santos Junior, 2010).

O repositório digital pode assumir diferentes papéis conforme as instituições que o estão implementando. Para as bibliotecas ele representa o local onde as diversas coleções, que disponibilizam vários tipos de mídias, são organizadas para todo o tipo de usuário da comunidade alvo. A biblioteca pode ter ou não total controle sobre a criação dos objetos digitais ali depositados, mas também tem o papel de manter esse material disponível e íntegro por tempo indeterminado.

Os repositórios representam o chamado Movimento Verde ou Via Verde do Acesso Aberto, facilitando o acesso à informação e a gestão dos conteúdos científicos das instituições culturais e de pesquisa (Ochoa-Gutiérrez; Giraldo; Tamayo, 2021). O termo “Acesso Aberto” começou a ser usado quando os periódicos eletrônicos cresceram e surgiram os primeiros títulos com acesso gratuito. O movimento veio para eliminar barreiras de naturezas econômicas e de direitos de exploração que limitam diversos aspectos para o uso dos conteúdos de pesquisa e culturais, permitindo o salvamento, cópia e distribuição dos textos na íntegra (Márdero Arellano, 2008).

Shintaku e Vidotti (2016) veem como fundamental a presença dos repositórios institucionais acadêmicos nos processos atuais de disseminação da informação, principalmente vinculados ao movimento do acesso aberto. Entretanto, essa presença tem atuação mais ampla e atuante, como apresentado pelo projeto *ArXiv1*, que desde 1991 oferece um local para publicação de pesquisas científicas voltadas às ciências, na forma de um repositório temático, recebendo contribuições, incluindo pré-prints.

Para Giesecke (2011), ao se discutir o papel dos repositórios institucionais, percebe-se que este deve assumir um papel inovador, publicando trabalhos e não apenas criando coleções de trabalhos publicados. A gestão do repositório requer estrutura diferenciada, com bases para os processos, requerendo entendimento maior sobre o fluxo editorial, incluindo direitos autorais e como transformar um manuscrito em trabalho final, criando serviços robustos de publicação para a instituição.

Segundo Andrew (2004), para as teses, o repositório é fonte primária, impondo serviços como: preservação, controle de acesso e direitos autorais. O repositório oferece infraestrutura tecnológica à publicação de originais, requerendo processos de curadoria e editoração.

As instituições têm colocado esforços para oferecer ambientes de publicação da produção das pesquisas. Esses repositórios institucionais promovem a organização, preservação e acesso desse material por meio de diversos recursos de busca e interoperabilidade (Giusti, 2014). Os padrões utilizados nesses repositórios dão à comunidade de autores e usuários a possibilidade de fazer o desenvolvimento do acervo e manter o conteúdo íntegro, acessível e relevante no contexto em que ele se apresenta.

A importância dos repositórios em todo o mundo evidencia a relevância do cuidado necessário com a preservação dos objetos digitais que, pela sua própria natureza, não existem sem representação e facilmente se tornam obsoletos. Dessa maneira, manter esse ambiente acessível temporalmente para que a comunidade possa ter acesso a ele, demanda um grande esforço financeiro e de pesquisas que integram um conjunto de ações para a preservação dos objetos digitais.

Giusti (2014) afirma que essas ações foram propostas com o objetivo principal de encontrar a melhor metodologia para a avaliação de um repositório institucional e propor, a partir dela, uma série de tarefas e padrões a serem atendidos por esses ambientes. Assim, têm surgido nos últimos anos importantes pesquisas dedicadas à preservação digital em face da urgência de se ter políticas institucionais a respeito do assunto. Diversos autores têm realizado trabalhos e projetos que norteiam os estudiosos do assunto, de modo a dar embasamento ao planejamento específico para a preservação digital em diferentes tipos documentais.

O documento "*Trusted Digital Repositories Attributes and Responsibilites", Online Computer Library Center* (OCLC) (OCLC, 2002), traz orientações e recomendações que se destinam principalmente a instituições culturais, como bibliotecas, arquivos, museus e editoras acadêmicas, direcionadas àqueles com responsabilidades pela preservação do patrimônio cultural.

A implementação de diretrizes e práticas recomendadas, como as estabelecidas pelo "*Trusted Digital Repositories Attributes and Responsibilities*" é ponto importante para assegurar a integridade, autenticidade e acessibilidade do patrimônio cultural e acadêmico. Esses padrões vão além da mera armazenagem de dados, enfocando também aspectos como metadados adequados, infraestrutura segura e processos de auditoria, vitais para a preservação a longo prazo.

Institucionalmente, os Repositórios Institucionais (RIs) servem como veículos fundamentais não apenas para armazenar as coleções, mas também garantem que esse conteúdo seja facilmente acessível e interpretável para futuras gerações de pesquisadores. A relevância dos RIs se amplia ainda mais quando consideramos seu papel no suporte ao movimento de Acesso Aberto e democratização do conhecimento.

A função dos RIs na preservação do legado intelectual de uma instituição é imensurável. Os artigos, teses e demais trabalhos acadêmicos abrigados nesses

repositórios são mais do que simples documentos; eles representam o desenvolvimento contínuo da ciência, tecnologia e humanidades. Garantir que esses materiais estejam seguros, acessíveis e livres de corrupção ou obsolescência é, portanto, uma tarefa de enorme responsabilidade.

A OCLC é uma organização fundada em 1967 pelo *Ohio College Library Center*. Sediada em Dublin, no estado americano de Ohio, foi criada pelo educador e bibliotecário norte-americano Fred Kilgour, visando estabelecer, manter e operar uma rede digital de bibliotecas para disponibilizar produtos e serviços que possibilitem o fácil acesso às informações científicas, literárias e educacionais.

Naquela publicação, de 2001, houve o desenho de conceitos para repositórios digitais em diferentes aspectos. Para os museus, o repositório digital representa a possibilidade de expor virtualmente suas obras através de substitutos digitais. A grande comunidade alvo tem a oportunidade de visitar o acervo com obras dos mais variados autores. O museu deve criar e gerenciar as obras virtuais, cabendo a ele a preservação digital deste material.

Para Martins e Martins (2020) o uso das ferramentas digitais transforma a gestão das coleções nos museus ao impactarem fortemente na maneira como essas instituições se relacionam com a sociedade. As tecnologias da informação e comunicação trouxeram a possibilidade de disponibilizar os conteúdos das coleções para um número muito maior de pessoas por meio do ambiente virtual, trazendo inúmeras vantagens em vários aspectos da sociedade em geral.

Nos arquivos, o repositório digital assume o papel de guarda e acesso dos objetos digitais. Flores, Rocco e Santos (2019), entendem que nesse contexto, a guarda dos objetos arquivísticos demanda uma alteração na responsabilidade pela custódia. Assim, o repositório deverá reter determinados dados, solicitados ao produtor, que possibilitem a preservação a longo prazo, de modo que continuem acessíveis à comunidade. O repositório tem então a necessidade de, em parceria com o produtor da informação, definir quais os dados e propriedades são relevantes para se manter a autenticidade dos objetos a serem preservados.

Os cenários apresentados pela OCLC demonstram a importância dos repositórios digitais em diferentes abordagens da gestão informacional na ciência da informação. Percebe-se o conceito de repositório digital confiável como um sistema

cuja missão é fornecer acesso confiável e de longo prazo a recursos digitais gerenciados para sua comunidade interessada, hoje e no futuro.

De acordo com Rocha (2016), um repositório precisa ter mais que a função de armazenar artigos, livros, teses ou outros objetos digitais, ele, fundamentalmente, tem que ser confiável em toda sua amplitude. Nesse contexto, o conceito de repositório digital confiável, apontado pela OCLC, remonta a necessidade do compromisso institucional com a manutenção a longo prazo do seu ambiente informacional, sua sustentabilidade estrutural e financeira com sistemas tecnológicos sob políticas, práticas e desempenho que possam ser auditados e medidos oferecendo acesso confiável e de longo prazo aos recursos digitais por ele gerenciados, ao longo dos anos (OCLC, 2002).

Entendendo o repositório digital como um conceito em âmbito institucional, a infraestrutura tecnológica da instituição é um fator determinante na natureza do software de repositório digital. Como guardiões tradicionais do patrimônio cultural, bibliotecas, arquivos e museus estão abordando ativamente métodos e estratégias para preservar os materiais digitais. À medida que a criação desse material cresce, aumenta também a responsabilidade em manter a confiança nesse conteúdo a longo prazo.

Esses repositórios desempenham papéis multifacetados, desde a salvaguarda do patrimônio intelectual e cultural até o cumprimento de obrigações éticas relativas à disseminação e preservação do conhecimento. Desse modo, bibliotecas, museus e arquivos institucionais evoluem no sentido de adotar estratégias para garantir a integridade e a longevidade dos ativos digitais, dada a crescente produção e a subsequente responsabilidade informacional.

Em 1996 o relatório RLG/CPA (WATERS; GARRETT, 1996) distribuiu uma declaração sobre a confiança nos repositórios digitais:

> Para garantir a longevidade da informação, talvez o papel mais importante na operação de um repositório digital seja gerenciar a identidade, integridade e qualidade dos próprios arquivos como um repositório confiável. Os usuários de informações armazenadas em formato eletrônico e de serviços de arquivamento relacionados a essas informações precisam ter a garantia de que um acervo digital é o que diz ser e as informações armazenadas nele são seguras a longo prazo (Waters; Garrett, 1996, tradução nossa).

Instituições como bibliotecas, arquivos e museus, por natureza, são confiáveis para coletar, armazenar e disponibilizar os itens ali guardados. Elas são confiáveis para promover o crescimento do conhecimento e para preservar esse acervo da melhor maneira possível para as gerações futuras. Entretanto, a informação digital pode ser transitória e difícil de preservar, demandando novos métodos de gerenciamento e preservação para o cenário de gerenciamento digital. Faz-se necessário pensar na adoção de padrões que garantam a integridade desse conteúdo.

Barros, Ferrere Maia (2018) percebem a preservação digital como peça fundamental para garantir o acesso a longo prazo aos documentos digitais, enfrentando-se, entretanto, os desafios que surgiram ao se evitar o comprometimento de sua autenticidade. Para Innarelli (2011), as Tecnologias da Informação e Comunicação devem ser utilizadas como meio e não como fim, de modo a automatizar grande parte dos processos envolvidos na gestão da informação, mas não devem excluir os profissionais da Ciência da Informação que são os responsáveis por garantir a integridade da documentação digital.

Neste sentido Innarelli (2011) ainda afirma que:

> O entendimento da complexidade e fragilidade dos documentos digitais deixa claro que a preservação digital não é resolvida pela própria tecnologia e nunca será, é resolvida com o estabelecimento de políticas e agendas de trabalho que, quando levadas a sério e incorporadas no dia a dia, permitirão a perpetuação dos acervos digitais, mesmo que estes deixem de ser digitais para serem atômicos, biológicos, futurológicos, etc.

Desse modo, entende-se que a preservação digital não está baseada apenas na tecnologia, mas que o repositório digital compreende a implantação de políticas de preservação, estratégias institucionais, normas bem aplicadas, e todo um planejamento dos processos que constituem a gestão dos documentos digitais.

Essas ações permitem a prevenção em relação a obsolescência tecnológica, dando a comunidade a confiança de que os objetos digitais continuarão autênticos e acessíveis a longo prazo. Essa confiança é fornecida por atributos que devem expor a diferentes situações e responsabilidades institucionais.

Além da implementação de estratégias, para as atividades de preservação digital em longo prazo é fundamental que se considerem os requisitos abordados no modelo de referência OAIS. O modelo especifica um conjunto de requisitos para um

repositório digital, que tenha a responsabilidade de preservar documentos digitais, garantir o acesso a longo prazo para uma comunidade alvo (Flores; Rocco; Santos, 2019).

O OAIS, ou Sistema Aberto de Arquivamento de Informação (SAAI) em português, acomoda os atributos da responsabilidade administrativa, a viabilidade organizacional, sustentabilidade financeira, adequação tecnológica e dos processos tecnológicos, segurança do sistema, prestação de contas e transparência. Ao abranger todas essas dimensões o OAIS se constitui como um padrão para garantir os requisitos necessários para que o repositório digital seja confiável.

3.3 O MODELO OAIS

O modelo OAIS é um *framework* conceitual padrão, estabelecido pela ISO 14721, para entender e formalizar as operações e responsabilidades de um sistema de arquivamento digital. Ele define as melhores práticas e requisitos para a *ingest*ão, arquivamento, preservação e disseminação de objetos de informação digital, delineando componentes como Pacotes de Informação[1] para Ingestão (SIPs), Pacotes de Informação Arquivística (AIPs) e Pacotes de Informação para Disseminação (DIPs). O modelo OAIS também se concentra no papel das "Comunidades Alvo", que são os grupos específicos de usuários que o sistema de arquivamento visa servir, garantindo que a informação seja acessível, compreensível e utilizável a longo prazo.

Em 2003, foi publicado sua versão, onde determinava a necessidade de padronizar não só a organização e recuperação dos objetos digitais, mas também, a interoperabilidade e a preservação digital (Cruz Mundet; Carrera, 2016).

O modelo OAIS, foi criado para garantir a arquitetura necessária de preservação dos arquivos digitais, “sua implementação em repositórios institucionais representa um desafio para não apenas facilitar o acesso à informação científica e acadêmica, mas também para garantir sua preservação temporalmente” (Ochoa-Gutiérrez; Giraldo; Tamayo, 2021).

[1] Do inglês: SIP – *Submission Information Package*; AIP – *Archival Information Package*; DIP – *Dissemination Information Package.*

A preservação digital é um dos desafios fundamentais na gestão de repositórios institucionais, pois a documentação disponível neles representa a memória institucional que deve permanecer acessível ao longo do tempo. Modelos de referência como o OAIS buscam definir os processos necessários para a preservação e acesso à informação efetivamente e a longo prazo. No entanto, este modelo tem sido utilizado principalmente em repositórios de arquivos associados a sistemas de gestão documental, e sua implementação em repositórios institucionais representa um desafio não apenas para facilitar o acesso à informação científica e acadêmica, mas também para garantir sua preservação ao longo do tempo (Ochoa-Gutiérrez; Giraldo; Tamayo, 2021).

O termo “Arquivo”, usado no modelo, refere-se a uma ampla variedade de funções e sistemas de armazenamento e preservação. Os chamados “Arquivos Tradicionais” são entendidos como instalações ou organizações que preservam documentos, de uma organização, instituição ou corporação, para acesso de comunidades públicas ou privadas. O Arquivo em si cumpre a tarefa de preservar, sejam livros, papéis, mapas, fotografias ou filmes, o principal foco é garantir que elas estejam em um suporte que a disponibilize a longo prazo e que o acesso a essa mídia seja cuidadosamente controlado (CCSDS, 2012).

Cruz Mundet; Carrera (2016) afirmam que, por ser um modelo criado por agências espaciais preocupadas com a preservação e acesso dos seus dados de pesquisa, ele pode ser aplicado a qualquer repositório, principalmente de instituições que possuem a obrigação de manter seus objetos digitais preservados e acessíveis a longo prazo. Para Ochoa-Gutiérrez; Giraldo; Tamayo (2021), diante do rápido desenvolvimento tecnológico, a autenticidade da informação em meios digitais está exposta a falhas. Faz-se necessário garantir o acesso aos recursos informacionais a longo prazo, disponibilizando sistemas que possam permitir processos, tecnologias e ações de preservação digital em repositórios institucionais.

Mesmo sendo aplicado nas estruturas arquivísticas, percebe-se que pode ser usado em outros tipos de recursos de informação que requerem orientação e tecnologias padronizadas para garantir a preservação dos documentos digitais ao longo do tempo. Assim, os repositórios digitais, como estratégia de organização e

disseminação da informação, podem integrar suas práticas, protocolos e tecnologias que facilitem a preservação digital da memória institucional.

A necessidade de conceitualização do modelo OAIS se faz importante para se entender a estrutura para preservar e acessar a informação de longo prazo. Desse modo, segundo Márdero Arellano (2008), instituições não arquivísticas podem implementar um processo de preservação.

Márdero Arellano (2008) afirma ainda que, com a adoção do modelo OAIS, o repositório deve cumprir determinadas ações para atender a comunidade alvo, por exemplo:

1. Negociar e aceitar a informação dos produtores de informação;
2. Manter o controle da informação a fim de garantir a preservação por longo prazo;
3. Determinar por si mesmo ou em conjunto com os parceiros, que comunidades devem tornar-se comunidade alvo e devem conseguir entender a informação fornecida;
4. Garantir que a informação seja compreensível para a comunidade alvo sem o auxílio dos produtores de informação;
5. Seguir políticas e procedimentos documentados, garantindo que a informação seja preservada e disseminada como cópias autênticas do original ou rastreável até o original;
6. Tornar a informação disponível para a comunidade alvo.

É importante ressaltar que a administração de um sistema de preservação pode servir para garantir também a interoperabilidade entre sistemas de informação, sejam eles bibliotecas, arquivos e/ou repositórios digitais. Suas funções principais de Recepção, Geração de Pacotes de Arquivamento e Acesso são fundamentais na determinação da existência, descrição, localização e disponibilidade da informação armazenada.

3.4 A ESTRUTURA DO MODELO OAIS

O modelo OAIS é resultado de mais de 10 anos de trabalho do *Consultative Committee for Space Data System* (CCSDS), ligado à NASA, que concebeu o modelo

com base em políticas arquivísticas em sua estrutura (CCSDS, 2012). Esse modelo é considerado o mais usado para repositórios de preservação. Ele define parâmetros de troca de informações por meio de pacotes que devem ser considerados para a implementação de um projeto de preservação digital ou analógico (Márdero Arellano, 2008).

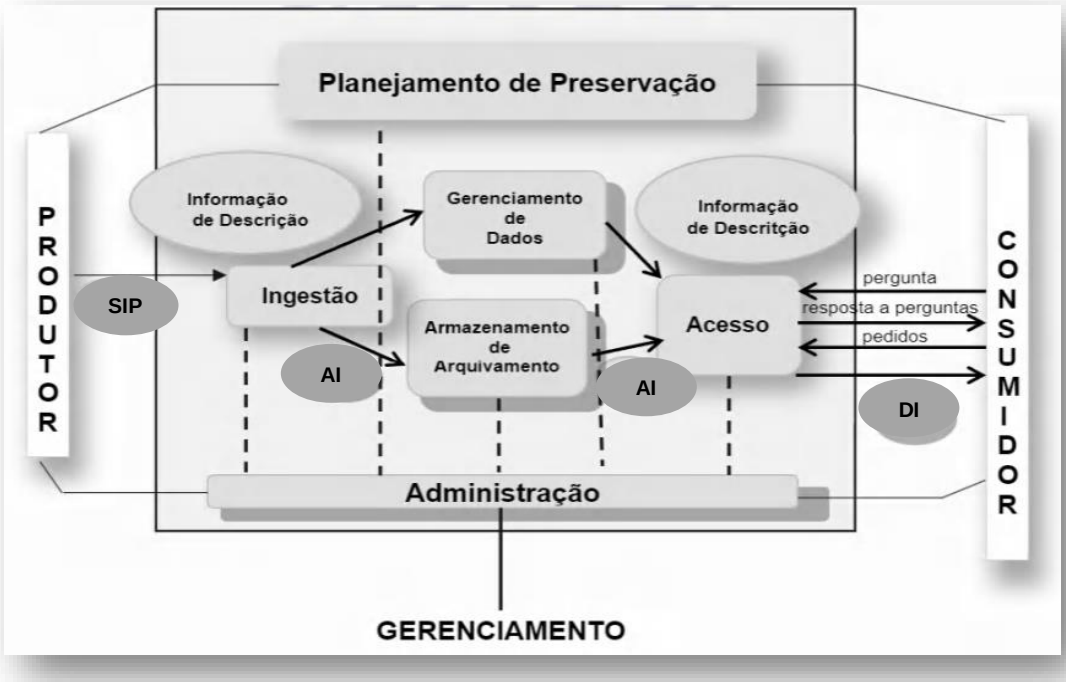
Por não se referir a um tipo específico de implementação, o modelo se adapta a toda comunidade que necessite disponibilizar informação a longo prazo. Para os repositórios digitais, destaca-se não só a gestão dos fluxos de informação com vista à otimização da recuperação da informação para o livre acesso, mas também a necessidade de definir estratégias adequadas para otimizar a coleta, organização e preservação da informação.

Basicamente, sem uma boa estratégia e um bom plano de preservação, o acesso não pode ser garantido ao longo do tempo. Por isso, o modelo de referência OAIS se estabelece como padrão necessário para garantir a guarda da memória institucional (Ochoa-Gutiérrez; Giraldo; Tamayo, 2021).

Na estrutura do OAIS atuam quatro entidades de informação: produtores, usuários, administração e o arquivo propriamente dito, e existem seis entidades funcionais: recepção, armazenamento, gerenciamento de dados, administração do sistema, planejamento de preservação e acesso (Figura 1) (CCSDS, 2012).

A Entidade Funcional *Ingest* (rotulada como “Ingestão” na figura) fornece os serviços e funções para aceitar Pacotes de Informações de Envio (SIPs - pacotes de submissão de informação) de Produtores (ou de elementos internos sob controle da Administração) e preparar o conteúdo para armazenamento e gerenciamento no Arquivo (CCSDS, 2012).

Figura 1 - Modelo OAIS



Fonte: CCSDS, 2012.

A Entidade Funcional de Armazenamento fornece serviços e funções para o armazenamento, manutenção e recuperação de AIPs (pacote de armazenamento de informação). As funções do armazenamento de arquivamento incluem: receber AIPs da “Recepção” e adicioná-los ao armazenamento permanente, gerenciar a hierarquia de armazenamento, atualizar a mídia na qual os acervos do arquivo são armazenados, realizar verificações de erros especiais e de rotina, fornece recursos de recuperação de desastres e fornecer AIPs para acesso (CCSDS, 2012).

A Entidade Funcional de Gerenciamento de Dados fornece os serviços e funções para preencher, manter e acessar as Informações Descritivas que identificam e documentam os acervos do Arquivo e os dados administrativos usados para gerenciar o Arquivo (CCSDS, 2012).

A Entidade Funcional de Administração do sistema, fornece os serviços e funções para a operação geral do sistema de Arquivo. As funções de administração incluem solicitar e negociar acordos de envio com produtores, auditar envios para garantir que eles atendam aos padrões de arquivo e manter o gerenciamento de configuração do hardware e software do sistema (CCSDS, 2012).

A Entidade Funcional de Planejamento de Preservação fornece os serviços e funções para monitorar o ambiente OAIS, fornecendo recomendações e planos de preservação para garantir que as informações armazenadas permaneçam acessíveis e compreensível pela comunidade interessada a longo prazo, mesmo que o ambiente de computação original se torne obsoleto (CCSDS, 2012).

A Entidade Funcional de Acesso fornece os serviços e funções que auxiliam os usuários na determinação da existência, descrição, localização e disponibilidade de informações armazenadas no OAIS e permite que recebam produtos de informação (CCSDS, 2012).

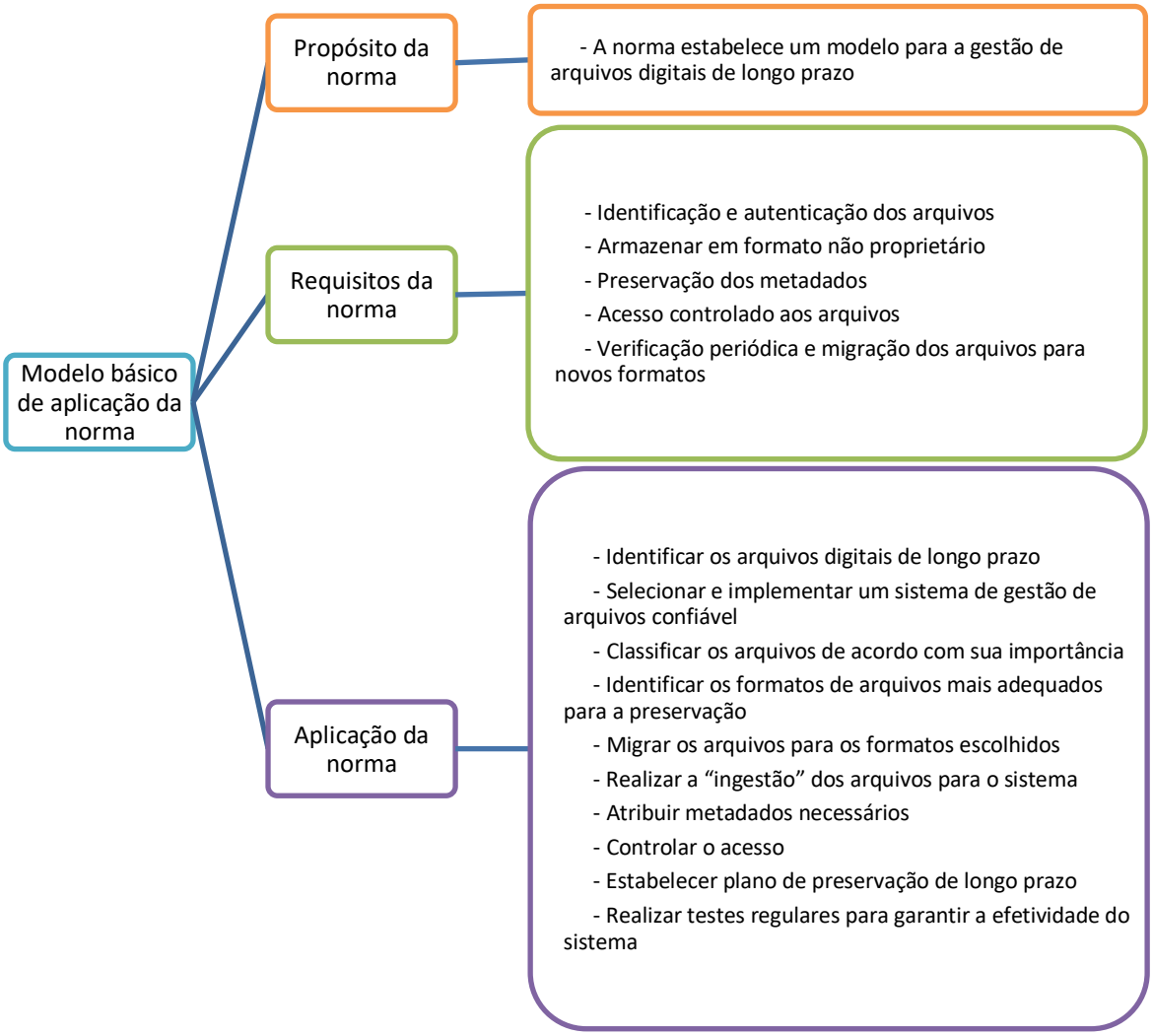
O modelo OAIS permite às instituições configurarem sistemas de preservação a longo prazo para a comunidade interessada, permitindo disponibilizar serviços de submissão, organização, gerenciamento e acesso contínuo aos objetos digitais preservados.

A aplicação deste modelo tem ocorrido principalmente no âmbito arquivístico, entretanto, outros recursos informacionais demandam orientações e tecnologias para garantir a preservação digital ao longo do tempo. Assim, é necessário aos softwares para implantação de repositórios digitais, integrar processos e protocolos que permitam a preservação digital da memória institucional, devido à importância destas ferramentas para a organização da informação de uma maneira geral (Ochoa-Gutiérrez; Giraldo; Tamayo, 2021).

Muitos autores constatam que a conformidade com o modelo OAIS é uma forma de atribuir confiança nos processos de preservação. Sendo ele um modelo conceitual, permite a implementação em uma variedade de repositórios e metadados. Permite ainda definir os softwares responsáveis pelas estratégias de preservação nas ações de depósito, migração, conversão e emulação.

O acesso a longo prazo dependerá da eficácia de execução destas estratégias, por isto é de extrema importância que exista uma avaliação criteriosa e uma verificação constante das ferramentas (SANTOS, 2018). A aplicação do modelo segue preceitos conforme a figura 2.

Figura 2 - Modelo de aplicação do modelo OAIS



Fonte: Elaboração própria, 2023.

3.5 O PROCESSO DE INGESTÃO (*INGEST*)

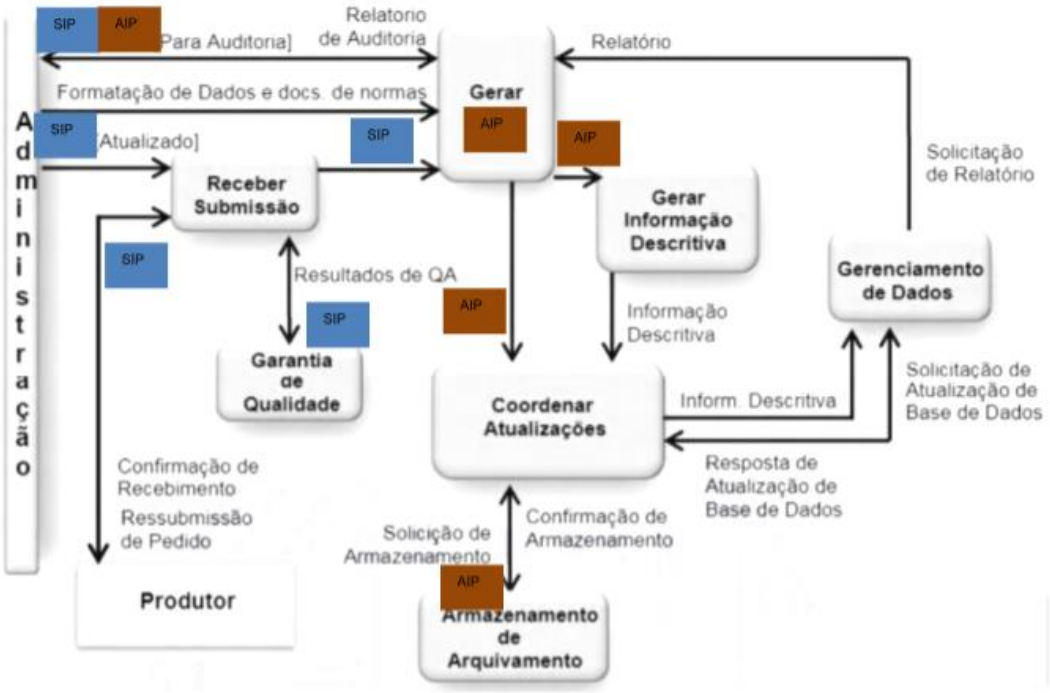
O processo de "*Ingest*" no modelo OAIS constitui das atividades de criação do pacote de submissão (SIPs) e preparação para o armazenamento e gerenciamento de longo prazo na forma de Pacotes de Informação Arquivística (AIPs), essas atividades são pontos de análise desta pesquisa. O sistema verifica a integridade daqueles pacotes e faz uma primeira avaliação de dados e metadados em relação aos critérios de aceitação previamente definidos.

Após a recepção e validação inicial, tem-se a fase seguinte para a transformação do SIP em um AIP. Faz-se uma análise pormenorizada dos metadados e do conteúdo, visando aprimorar a preservação de longo prazo e a acessibilidade. Os metadados de preservação são adicionados ou atualizados, e os dados podem ser normalizados para um formato que seja mais adequado para o arquivamento de longo prazo. Tarefas como a geração de *checksums* também são comuns nesta etapa para garantir a integridade dos dados ao longo do tempo (*Consultative* Committee *for Space Data Systems*, 2012).

No modelo, existe um processo de coordenação com as atividades de "*Data Management*", onde é garantido que todos os metadados necessários para recuperação e compreensão dos AIPs sejam coletados e armazenados de forma eficaz. Adicionalmente, verifica-se a conformidade com políticas e normas do repositório, bem como a adequação dos AIPs para as necessidades das Comunidades Alvo.

Concluída a transformação e o enriquecimento do SIP em um AIP, ocorre a transferência deste último para o armazenamento arquivístico, onde estará sujeito às operações de gestão e preservação de longo prazo. Neste ponto, é crucial que haja um registro meticuloso das ações realizadas, não apenas para fins de rastreabilidade, mas também para garantir a capacidade de reproduzir ou entender o processo de *ingest*ão no futuro. As funções da entidade funcional de ingestão são mostradas na figura 3.

Figura 3 - Entidade funcional de ingestão



Fonte: CCSD, 2012.

O processo de "*ingest*" no modelo de referência OAIS representa uma fase crítica para a garantia de confiabilidade, autenticidade e integridade de um repositório digital. A implementação rigorosa de políticas e procedimentos de "*ingest*" conforme as diretrizes de normas como a ISO 16363 é fundamental para assegurar que os objetos digitais sejam não apenas tecnicamente aceitáveis, mas também contextualmente significativos. A falha em adotar um processo de "*ingest*" da maneira correta, pode comprometer a integridade do repositório digital, tornando-o susceptível a perdas, corrupção ou obsolescência.

3.6 A PRESERVAÇÃO DIGITAL

A preservação digital é o processo de garantir que as informações digitais, como documentos eletrônicos, arquivos de áudio e vídeo e softwares, possam ser acessadas e utilizadas no futuro. Envolve armazenar as informações para evitar que sejam perdidas ou danificadas e manter sua acessibilidade ao longo do tempo. A preservação digital é importante porque a informação digital costuma ser mais frágil e

suscetível à perda do que a informação física, e é essencial para preservar o patrimônio cultural e histórico.

A preocupação em preservar informações digitais não é nova e tem sido explorada em vários níveis nos últimos tempos. Tem-se dificuldade em garantir a longevidade, integridade e acesso aos formatos dos arquivos armazenados. A obsolescência tecnológica representa uma ameaça inerente à informação (Waters; Garrett, 1996).

A preservação digital destina-se garantir o acesso a longo prazo a conteúdos digitais e o bibliotecário tem nessa prática um objeto de estudo que engloba todas as tarefas envolvidas no fluxo informacional. Os sistemas para armazenamento e recuperação da informação são demandados a acompanhar o avanço na produção científica ocorrendo a necessidade de se pensar na preservação desse conteúdo no contexto de novas tecnologias que garantam a integridade dos pacotes armazenados.

Para Giusti; Villarreal (2018), as organizações devem promover uma estrutura interna que abordem diferentes atividades que garantam preservar digitalmente sua memória institucional. Essa estrutura compreende: adaptações de processos, sejam eles tecnológicos ou informacionais, ao longo do ciclo de vida dos objetos digitais. Giusti também vê a necessidade das instituições de ensino e pesquisa para modernizar os serviços de informação que elas prestam. A gestão do acervo digital e sua preservação é um dos pontos que devem ser observados.

A essência da preservação é a manutenção do contexto dos documentos. É necessário manter a capacidade de recriar a forma original e função do documento quando acessado, para estabelecer a autenticidade, validade e valor, permitindo ao leitor assegurar sua visão e valor.

Na preservação digital os objetos digitais devem manter seus atributos de modo que possam ser copiados, acessados, distribuídos, tornando-se então pesquisáveis e lidos por sistemas em todas suas fases de criação e distribuição. As características do documento digital devem ser mantidas em todas as funcionalidades.

Para Márdero Arellano (2008) a condição básica à preservação digital seria, então, a adoção desses métodos e tecnologias que integrariam a preservação física (quando se tratar de mídias magnéticas), lógica e intelectual dos objetos digitais. Sendo o foco da preservação lógica, a manutenção dos formatos para inserção dos

dados e a busca por novos softwares e *hardwares* que mantenham vigentes seus conteúdos, para conservar sua capacidade de acesso.

Desta maneira, na preservação digital, são necessários procedimentos de manutenção e recuperação de dados bem como estratégias e procedimentos para manter sua acessibilidade e autenticidade ao longo do tempo. Podendo requerer colaboração da comunidade interessada e boas práticas de licenciamento, metadados e documentação, antes de aplicar ações mais técnicas.

Em um passado recente, a preservação era entendida como uma série de métodos a serem adotados para prevenir os documentos de deterioração física. Entretanto, com o avanço tecnológico dos últimos anos e a quantidade de documentos sendo gerados, exclusivamente, em meio digital. A preservação digital ganhou importância no ciclo da gestão da informação (geração, tratamento, preservação/conservação e difusão da informação) (Márdero Arellano, 2008).

Devida às várias características dos objetos digitais, dentre elas facilidade de criação e gestão, tem-se neles a crescente produção e disseminação da informação no mundo atual. Na era da informação digital, o foco está na geração e/ou aquisição de material digital, mas a preservação digital está ganhando espaço na lista de prioridades para se manter a confiabilidade a longo prazo dos acervos eletrônicos.

3.7 O REPOSITÓRIO DIGITAL CONFIÁVEL

As instituições culturais têm, em sua natureza, a confiabilidade para armazenar e preservar o patrimônio cultural para as futuras gerações. Elas têm se destacado na preservação dos objetos físicos e digitais ao longo do tempo, entretanto, com a informação digital, devido a sua característica transitória, os métodos tradicionais de preservação são menos aplicáveis (OCLC, 2002).

O modelo OAIS descreve as várias etapas para a implantação de um Repositório Digital Confiável. Ele passa, em suas descrições, pela estruturação dos conceitos para o arquivamento digital, preservação e o acesso em longo prazo (Ribeiro, 2019). *O Research Library Group* (RLG) e *Online Computer Library Center* (OCLC), indica a importância do desenvolvimento de repositórios digitais confiáveis para a preservação e o acesso a longo prazo (RLG/NARA, 2007).

No relatório da OCLC, a missão do repositório digital confiável é disponibilizar acesso confiável de longo prazo para a comunidade interessada. Entende-se aqui que o repositório é considerado confiável à medida que segue uma série de requisitos definidos por normas específicas (OCLC, 2002).

Tanto a infraestrutura da instituição, seja ela uma grande universidade, biblioteca, arquivo ou museu, quanto a comunidade que irá consumir as informações, são fatores determinantes na natureza do Repositório Digital Confiável. São esses fatores que determinarão: o que é depositado, como a informação digital é gerenciada e preservada, e como ela é acessada. Apesar de seus diferentes modelos organizacionais, todos os repositórios digitais precisarão abordar as mesmas questões não apenas de funcionalidade, mas também de confiabilidade.

O relatório da OCLC (2002), afirma, entretanto, que seja qual for a infraestrutura geral, para atender às expectativas dos atores envolvidos, todos os repositórios digitais confiáveis devem cumprir determinados atributos e responsabilidades como:

- Aceitar a responsabilidade pela manutenção de longo prazo dos recursos digitais em nome de seus depositantes e em benefício dos usuários atuais e futuros;
- Ter um sistema organizacional que apoie não só a viabilidade a longo prazo do repositório, mas também a informação digital pela qual é responsável;
- Demonstrar responsabilidade financeira e sustentabilidade;
- Projetar seu(s) sistema(s) de acordo com convenções e padrões comumente aceitos para garantir o gerenciamento, acesso e segurança contínuos dos materiais nele depositados;
- Estabelecer metodologias de avaliação de sistemas que atendam às expectativas de confiabilidade da comunidade;
- Ser confiável para cumprir suas responsabilidades de longo prazo com os depositantes e usuários de forma aberta e explícita;
- Ter políticas, práticas e desempenho que possam ser auditados e medidos.

Estas questões envolvem conceitos e termos que estabelecem uma base para definir as características dos repositórios digitais confiáveis. Expressões como: “confiável”, “responsável”, “autêntico”, ajudam a definir a natureza do repositório e

suas relações com aqueles que criam, gerenciam e usam os objetos digitais. A Tecnologia da Informação trabalha com o estabelecimento de “confiança” em sistemas militares e de controle de voos (por exemplo) para trazer confiabilidade à manutenção da informação que circula nesses ambientes. Ainda no contexto da autenticidade, especialistas em bibliotecas digitais contribuíram com suas experiências para a construção de sistemas seguros que acomodam abundância de recursos digitais.

Instituições responsáveis pela preservação de material não digital podem ter um nível razoável de confiança. Bibliotecas, e outros centros de cultura, preservaram de forma confiável uma grande quantidade de registros humanos ao longo do tempo. Embora os desafios apresentados na preservação de informações digitais sejam muito diferentes e requerem novas soluções, a comunidade já tem o sentido de confiabilidade devido ao histórico das instituições.

Os processos de preservação da informação digital variam conforme os tipos de objetos - textuais, numéricos, imagens, vídeos, sons, multimídias. Independentemente do método de preservação aplicado, entretanto, o objetivo central deve ser preservar a integridade da informação; definindo e preservando as características de um objeto de informação que o distinguem na totalidade ou como uma obra única, em seu conteúdo, referência, proveniência e contexto (Waters; Garrett, 1996).

Com a facilidade de se produzir conteúdo digital, trazida pelas tecnologias da informação e comunicação, é necessária a constante afirmação sobre a importância de se preservar para as futuras gerações. Os registros culturais devem estar sob o comprometimento organizacional, técnico, legal e econômico em todas as dimensões institucionais envolvidas nesse tema, por meio de processo e métodos que assegurem a preservação digital.

A implementação crescente do modelo OAIS em arquivos digitais estimula o desenvolvimento de ferramentas especializadas, particularmente para o planejamento da preservação. Este processo requer a gestão criteriosa da "informação de representação", envolvendo a normalização de formatos de arquivo e o monitoramento das suas relações com aplicações e versões subsequentes (Serra Serra, 2007).

É possível assegurar a confiabilidade de um repositório digital, implementando processos de auditoria interna. O processo de auditoria é essencial para avaliar a confiabilidade dos métodos de preservação empenhados pelos repositórios digitais. A conformidade com o modelo OAIS, permite a avaliação de requisitos de ordem informacional, tecnológica e organizacional pré-estabelecidos.

As atividades de certificação estão diretamente relacionadas às auditorias. São um complemento capaz de mensurar a confiabilidade dos repositórios digitais, seguindo determinados modelos, e fornecendo um conjunto de dados capaz de quantificar as potencialidades e as vulnerabilidades do repositório.

3.8 AS CERTIFICAÇÕES E PADRÕES INTERNACIONAIS PARA REPOSITÓRIOS DIGITAIS CONFIÁVEIS

A preservação digital refere-se à prática de garantir que a informação digital permaneça acessível e utilizável ao longo do tempo. Essa pode ser uma tarefa desafiadora, pois a mídia digital costuma ser mais propensa à deterioração e obsolescência do que a mídia física.

A adoção de políticas de preservação é ponto fundamental para a instituição prover segurança à integridade dos objetos digitais que estão sob sua guarda. Entretanto, proteger esses arquivos contra alterações não autorizadas ou a obsolescência tecnológica não depende apenas das tecnologias utilizadas, mas também, é importante aplicar estratégias e normas específicas.

Para assegurar essa integridade, é importante destacar que o repositório deve fornecer evidências que operam uma gestão de dados e metadados adequada para garantir integridade, autenticidade e acesso. A integridade, garantirá a rastreabilidade das alterações realizadas nos objetos digitais, provendo autenticidade e confiabilidade aos dados originais. Dessa maneira, sua proveniência, incluindo a relação entre os dados originais, os disponibilizados e as relações existentes entre conjuntos de dados e metadados estarão preservadas (Barros; Ferrer; Maia, 2018).

Os repositórios então devem estar em condições de funcionar em um ambiente confiável e estável, com possibilidade de análise das vulnerabilidades e riscos inerentes aos sistemas computacionais. É importante observar que nenhuma ferramenta de software sozinha pode enfrentar todos os desafios da preservação

digital. As organizações geralmente precisam usar uma combinação de ferramentas e estratégias para preservar efetivamente os materiais digitais a longo prazo.

Neste contexto, planos e políticas de preservação digital têm um papel importante para as organizações, pois possibilitam o gerenciamento dos riscos críticos, das atividades de pessoal responsável, baseado em diretrizes e requisitos adotados internacionalmente (Barros; Ferrer; Maia, 2018). Para enfrentar esse desafio, várias instituições desenvolveram programas de certificação que visam reconhecer que as organizações implementaram as melhores práticas de preservação digital na forma de um padrão.

Para Ribeiro (2019), as certificações são um conjunto de critérios reunidos que podem facilitar e organizar uma escala de avaliação, para a maturidade e execução dos processos de guarda da informação. O atendimento ao modelo OAIS, possibilita a aferição dos critérios de conformidade com as políticas de uso, compartilhamento, atendimento a normas, padrões, e aos aspectos de segurança tecnológica.

São vários os padrões disponíveis que permitem usuários de sistemas de informação promoverem a preservação digital. Os itens comuns a esses guias de boas práticas envolvem avaliações em relação à integridade, autenticidade, flexibilidade, normalização e acessibilidade dos objetos digitais e seus metadados. Os modelos de auditoria e maturidade permitem ainda atestar o nível em que se encontra a implementação das políticas de preservação digital na instituição (Bodero Poveda, De Giusti; Morales, 2022).

Dentre os diversos padrões existentes, são destaques aqueles que viabilizam a certificação de repositórios por meio de avaliações preliminares que dão suporte aos processos formais de certificação. Foram avaliados três padrões de certificação que usam o modelo OAIS como base. Esse modelo tem um carácter genérico de implementação se adaptando aos mais diversos tipos de repositórios e suas necessidades de preservação a longo prazo, dando liberdade para adaptar padrões de metadados e softwares que façam a gestão das etapas de organização da preservação (Santos, 2018).

3.9 METODOLOGIAS E PROGRAMAS DE AVALIAÇÃO DE REPOSITÓRIOS

As certificações de repositórios digitais confiáveis são mecanismos baseados em padrões pré-estabelecidos para atestar as ações da instituição em diversos aspectos da implantação, nos procedimentos que garantem a preservação digital. Elas são uma forma de as organizações demonstrarem que atenderam a determinados padrões de preservação digital. Esses programas geralmente envolvem uma avaliação das práticas de preservação digital de uma organização. A certificação fornece um nível de garantia para as partes interessadas de que uma organização está seguindo as melhores práticas de preservação digital. No quadro 1 são apresentadas algumas das certificações internacionais:

Quadro 1 – Certificações internacionais

CERTIFICAÇÃO	**DESCRIÇÃO**
Trusted Repository Audit Checklist (TRAC)	Esta certificação é emitida pelo Centro de Bibliotecas de Pesquisa (CRL) e é baseada em padrões internacionais para preservação digital.
Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)	Esta certificação é emitida pela *Digital Preservation Coalition* (DPC) e se concentra na avaliação das práticas de gerenciamento de risco de repositórios digitais.
CoreTrustSeal	Esta certificação é emitida pelo *CoreTrustSeal Board* sendo baseada nos padrões da ISO 16363, amplamente reconhecidos como os padrões mais abrangentes e rigorosos para repositórios digitais.
*National Digital Stewardship Alliance (*NDSA)	Esta certificação é emitida pela NDSA e baseada no nível de conformidade com o Modelo de Maturidade de Administração de Preservação Digital da NDSA.

Fonte: Elaboração própria, (2023).

3.10 PADRÕES INTERNACIONAIS PARA PRESERVAÇÃO

A ISO é uma organização internacional que desenvolve e publica normas para indústrias e tecnologias, visando estabelecer um entendimento comum de como produtos e serviços devem ser projetados, produzidos e testados. As normas ISO são desenvolvidas por comitês técnicos formados por especialistas de diferentes países e depois revisadas e aprovadas pelos países membros da ISO.

A instituição possui várias normas e padrões voltados para preservação fornecendo diretrizes e práticas recomendadas para preservação digital, ajudando as

organizações a entenderem as etapas necessárias para preservar informações digitais de forma adequada.

Abaixo, no quadro 2, são listadas as normas relacionadas a preservação disponíveis no site da instituição:

Quadro 2 - Normas relacionadas a preservação digital

NOME DA NORMA	DESCRIÇÃO
ISO/IEC 23000-6:2009 Tecnologia da informação — Formato de multimídia (MPEG-A) — Parte 6: Formato de arquivamento profissional [reformulada]	A ISO/IEC 23000-6:2009 especifica o formato de aplicação de arquivamento profissional (PA-AF). O objetivo do PA-AF é fornecer um formato de empacotamento padronizado para arquivos digitais. Esse formato também pode servir como uma implementação do pacote de informações especificado pelo modelo OAIS.
ISO/TR 13028:2010 Informação e documentação - Diretrizes de implementação para digitalização de registros.	ISO/TR 13028:2010: estabelece diretrizes para criar e manter registros apenas em formato digital; estabelece diretrizes de melhores práticas para digitalização para garantir a confiabilidade.
ISO 16175-3:2010 Informação e documentação — Princípios e requisitos funcionais para registros em ambientes de escritório eletrônico — Parte 3: Diretrizes e requisitos funcionais para registros em sistemas de negócios [reformulada]	A ISO 16175-3:2010 especifica requisitos gerais e diretrizes para gerenciamento de registros e para a identificação apropriados de registros de atividades de requisitos transacionadas em sistemas de negócios.
ISO/TS 21547:2010 Informática em saúde — Requisitos de segurança para arquivamento de registros eletrônicos de saúde	O objetivo da ISO/TS 21547:2010 é definir os princípios básicos necessários para preservar com segurança os registros de saúde em qualquer formato a longo prazo. Concentra-se em problemas de arquivamento específicos de saúde previamente documentados. Ele também fornece uma breve introdução aos princípios gerais de arquivamento.
ISO 16175-2:2011 Informação e documentação — Princípios e requisitos funcionais para registros em ambientes de escritório eletrônico — Parte 2: Diretrizes e requisitos funcionais para sistemas de gerenciamento de registros digitais (revisado pela ISO/TS 16175-2:2020)	A ISO 16175-2:2011 é aplicável a produtos frequentemente denominados "sistemas de gerenciamento de registros eletrônicos" ou "sistemas de gerenciamento de conteúdo empresarial". A ISO 16175-2:2011 usa o termo sistemas de gerenciamento de registros digitais para aqueles aplicativos de software cuja função principal é o gerenciamento de registros.
ISO 13008:2012 Informação e documentação — Processo de conversão e migração de registros digitais [reformulada]	Especifica as questões de planejamento, requisitos e procedimentos para a conversão e/ou migração de registros digitais (que inclui objetos digitais mais metadados) a fim de preservar a autenticidade, confiabilidade, integridade e usabilidade de tais registros

ISO/IEC 23000-6:2012 Tecnologia da informação — Formato de aplicativo multimídia (MPEG-A) — Parte 6: Formato de aplicativo de arquivamento profissional	O objetivo do formato de aplicativo de arquivo profissional ISO/IEC 23000-6 (PA-AF) é fornecer um formato de embalagem padronizado para arquivos digitais. Este formato pode servir como uma implementação do pacote de informações especificado pelo Modelo OAIS.
ISO 17090-4:2014 Informática em saúde — Infraestrutura de chave pública — Parte 4: Assinaturas digitais para documentos de saúde [reformulada]	A ISO 17090-4:2014 oferece suporte à intercambialidade de assinaturas digitais e à prevenção de assinaturas digitais incorretas ou ilegais, fornecendo requisitos e formatos mínimos para geração e verificação de assinaturas digitais e certificados relacionados.
ISO/TR 17797:2014 Arquivamento eletrônico — Seleção de mídia de armazenamento digital para preservação a longo prazo	A ISO/TR 17797:2014 fornece diretrizes sobre a seleção da mídia de armazenamento mais apropriada para uso em soluções de armazenamento eletrônico de longo prazo. Ele inclui uma discussão sobre armazenamento magnético, óptico e eletrônico.
ISO/TR 18160:2014 Gerenciamento de documentos — Preservação digital	A ISO/TR 18160:2014 recomenda métodos de teste para avaliar a consistência das imagens digitais gravadas em microfilme usando entrada de documentos gerados digitalmente, bem como documentos digitais criados a partir da digitalização de documentos.
ISO/TR 19814:2017 Informação e documentação — Gestão de coleções para arquivos e bibliotecas	A ISO/TR 19814:2017 fornece orientação e recomendações no planejamento, implementação, manutenção e melhoria da preservação de coleções de arquivos e bibliotecas.
ISO 14641:2018 Gestão de documentos eletrônicos — Projeto e operação de um sistema de informação para a preservação de documentos eletrônicos	Este documento especifica um conjunto de especificações técnicas e políticas organizacionais a serem implementadas para a captura, armazenamento e acesso de documentos eletrônicos. Isso garante legibilidade, integridade e rastreabilidade dos documentos durante a sua preservação.
ISO 19165-1:2018 Informações geográficas — Preservação de dados e metadados digitais — Parte 1: Fundamentos	A ISO 19165-1:2018 define um complemento de metadados de preservação da ISO 19115-1. A ISO 19165-1:2018 estabelece os requisitos para a manutenção a longo prazo de dados geoespaciais digitais.
ISO 14533-4:2019 Processos, elementos de dados e documentos no comércio, indústria e administração — Perfis de assinatura de longo prazo — Parte 4: Atributos apontando para objetos de prova de existência (externos) usados em formatos de assinatura de longo prazo	Este documento especifica os elementos definidos nos padrões internacionais da ISO/ITU-T, ETSI e IETF RFC que permitem, pelo menos, uma prova da existência de objetos de dados e assinaturas digitais e a preservação do status de validade das assinaturas digitais por um longo período usadas na validação.
ISO/IEC 23681:2019 Tecnologia da informação — Especificação de formato de retenção de informação independente (SIRF)	Este documento especifica o *Self-contained Information Retention Format* - SIRF (Formato de retenção de informações independentes, tradução literal). Propõe uma abordagem para a preservação de conteúdo digital que potencializa os processos da profissão arquivística.

ISO 16175-1:2020 Informação e documentação — Processos e requisitos funcionais para software para gerenciamento de registros — Parte 1: Requisitos funcionais e orientação associada para quaisquer aplicativos que gerenciam registros digitai	Este documento fornece modelo, requisitos funcionais de alto nível e orientação associada para aplicativos de software destinados a gerenciar registros digitais (incluindo cópias digitais de registros analógicos de origem).
ISO 17090-4:2020 Informática em saúde — Infraestrutura de chave pública — Parte 4: Assinaturas digitais para documentos de saúde	Este documento oferece suporte à intercambialidade de assinaturas digitais e à prevenção de assinaturas digitais incorretas ou ilegais, fornecendo requisitos e formatos mínimos para geração e verificação de assinaturas digitais e certificados relacionados.
ISO 19165-2:2020 Informações geográficas — Preservação de dados e metadados digitais — Parte 2: Especificações de conteúdo para dados de observação da Terra e produtos digitais derivados	Este documento visa estender a preservação de longo prazo de dados geoespaciais digitais para fornecer detalhes sobre o conteúdo que descreve a proveniência e o contexto específico dos dados de missões que observam a Terra usando instrumentos espaciais.
ISO/IEC TS 22424-1:2020 Publicação digital — Preservação EPUB3 — Parte 1: Princípios	A série ISO/IEC TS 22424 oferece suporte à preservação de longo prazo de publicações EPUB por meio de uma estratégia dupla. Este documento considera os recursos do EPUB do ponto de vista da preservação a longo prazo.
ISO/IEC TS 22424-2:2020 Publicação digital — Preservação EPUB3 — Parte 2: Requisitos de metadados	A série ISO/IEC TS 22424 oferece suporte à preservação de longo prazo de publicações EPUB por meio de uma estratégia dupla. Este documento torna o EPUB compatível com as práticas atuais de arquivos OAIS e requisitos técnicos de sistemas de repositório.
ISO 13008:2022 Informação e documentação — Processo de conversão e migração de registros digitais	Este documento especifica como converter e/ou migrar registros digitais para preservar sua autenticidade, confiabilidade, integridade e usabilidade. É necessário ressaltar que diferentes países podem ter outras certificações específicas para suas realidades ou ainda adaptando as normas internacionais para as especificações nacionais.

Fonte: Elaboração própria, 2023.

3.11 A ISO 16363:2012

Em dezembro de 1994, a Comissão de Preservação e Acesso e o Grupo de Bibliotecas de Pesquisa criaram a Força-Tarefa sobre Arquivamento Digital (CPA/RLG - TASK FORCE). O objetivo da Força-Tarefa era investigar formas de garantir acesso contínuo aos registros armazenados em formato digital (Waters; Garrett, 1996).

Em 1996, essa Força-Tarefa reconheceu a necessidade de as organizações atestarem a confiabilidade para armazenar, migrar e fornecer acesso a coleções digitais como um componente crítico da infraestrutura de arquivamento digital. Naquele ponto não era suficiente as instituições se identificarem como confiáveis e foi

necessário estabelecer um processo de certificação para arquivos digitais atestarem sua preservação da informação digital.

O desenvolvimento do OAIS avançou na responsabilidade do trabalho na infraestrutura de arquivamento digital. O objetivo foi criar um consenso sobre os requisitos de um arquivo para fornecer preservação de longo prazo da informação digital. Assim o OAIS abordou questões fundamentais sobre preservação digital que se aplicam a diferentes domínios.

Conhecido como ISO 14721, o modelo fornece uma estrutura comum para a compreensão do ambiente, componentes funcionais e objetos de informação em um sistema de preservação digital. Muitos na comunidade de patrimônio cultural adotaram o OAIS como modelo antes de se tornar um padrão aprovado em 2002 para entender melhor as necessidades de sistemas de preservação digital (CCSDS, 2011; ISO 16363:2012).

Entretanto, não havia um entendimento claro do que significava estar conforme o modelo OAIS, além de usar sua terminologia para descrição do seu arquivo. Apesar da seção de conformidade do OAIS especificar a necessidade de apoiar o modelo de informação e cumprir as responsabilidades obrigatórias, as reivindicações de confiabilidade eram difíceis de justificar ou provar objetivamente. Tornou-se então vital estabelecer critérios claros para determinar o que constituía um repositório confiável (CCSDS, 2011; ISO 16363:2012).

Em 2002, *o Reserch Library Group* (RLG) e a OCLC publicaram em conjunto o documento "T*rusted Digital Repositories: Attributes and Responsibilities*", que forneceu uma estrutura base para repositórios digitais confiáveis, confiáveis e sustentáveis. Ele cobria atributos e responsabilidades para lidar com uma variedade de materiais mantidos por instituições de pesquisa e patrimônio cultural. Ele concentrou atributos organizacionais e técnicos de alto nível e discutiu modelos potenciais para certificação de repositório digital, recomendando o desenvolvimento de programas de certificação e critérios auditáveis para certificar repositórios digitais (CCSDS, 2011; ISO 16363:2012).

Em 2007, foi publicado o *documento Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC), que apresenta um conjunto de critérios e um checklist a serem tomados como referência para a certificação de repositórios

digitais confiáveis. Esse documento serviu de base para a elaboração da norma ISO 16363: 2012, que lista os critérios que um repositório digital confiável deve atender (CONARQ, 2015).

O documento provou ser útil para instituições que lidam com a preservação de longo prazo de recursos do patrimônio cultural e tem sido usado com o OAIS como uma ferramenta de planejamento de preservação digital. Como estrutura, este documento concentrou-se em atributos organizacionais e técnicos de alto nível e discutiu modelos potenciais para certificação de repositório digital. Absteve-se de ser prescritivo sobre a natureza específica de repositórios e arquivos digitais emergentes rapidamente e, em vez disso, reiterou o apelo à certificação de repositórios digitais, recomendando o desenvolvimento de programa de certificação e articulação de critérios auditáveis.

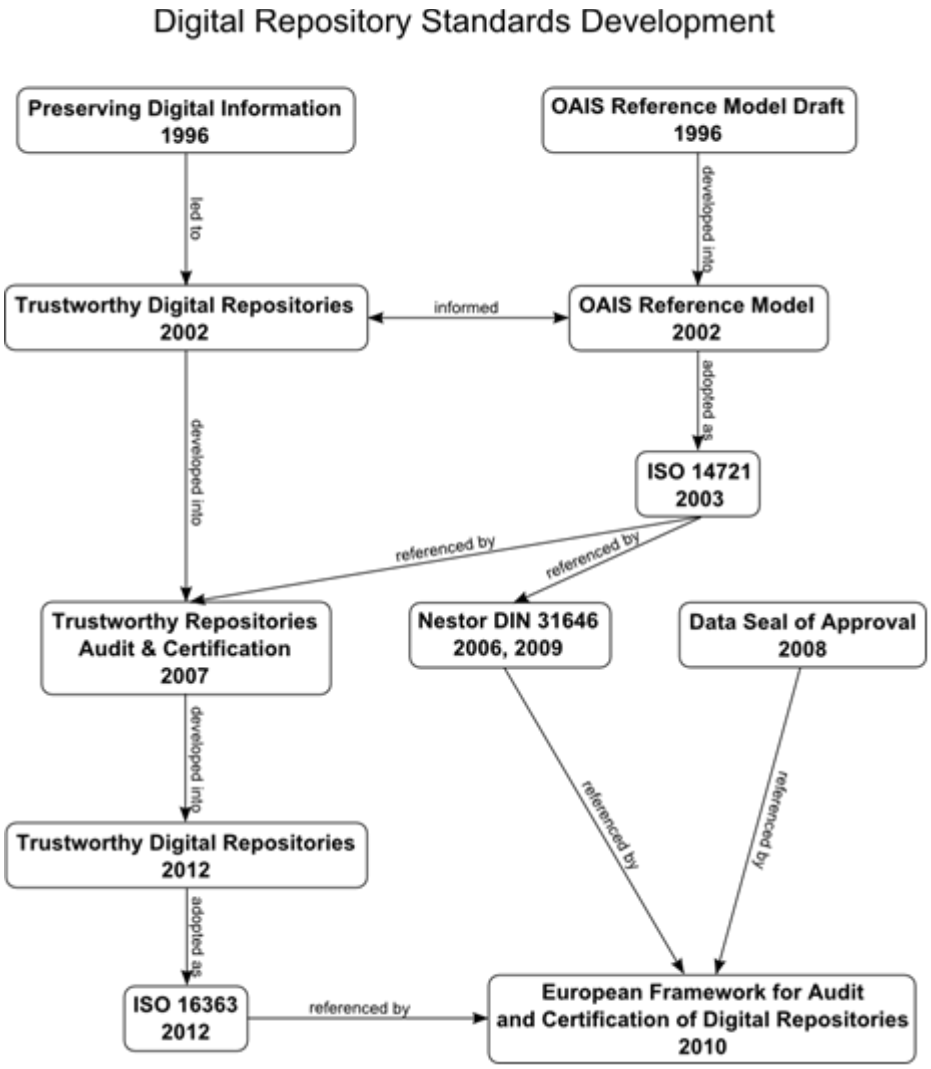
Foram vários os documentos e normas considerados para a elaboração da ISO 16363:

- A família de normas ISO 9000 aborda componentes de garantia de qualidade em uma organização e gerenciamento de sistemas que, eventualmente, não foram desenvolvidos especificamente para avaliar a confiabilidade das organizações que operam repositórios digitais.
- A ISO 17799:2005 foi desenvolvida especificamente para tratar da segurança de dados e dos sistemas de gerenciamento de informações. Apesar dos seus requisitos de segurança da informação buscarem a conformidade da segurança de dados em um nível muito granular, eles não abordam os componentes organizacionais, processuais e de planejamento de preservação necessários para o gerenciamento de longo prazo dos recursos digitais.
- A ISO 15489-1:2001 e ISO 15489-2:2001 estabelecem uma abordagem orientada a processos para a criação e uso de registros digitais, exigindo que as organizações estabeleçam, documentem e mantenham políticas e práticas para gerenciamento de registros, sem se concentrar especificamente em repositórios digitais.
- A ISO 14721:2003, ou *Open Archival Information System Reference* Model, é um modelo de referência que identifica os participantes envolvidos na preservação digital, suas funções e responsabilidades, e os tipos de

informações a serem trocadas durante o processo de armazenamento, *ingest*ão e disseminação a partir de um repositório digital.

Diagrama do desenvolvimento de padrões de repositório digital, incluindo OAIS (ISO 14721) e TDR (ISO 16363).

Figura 4 - Diagrama do desenvolvimento de padrões de repositório digital



Fonte: Nkrabben - CC BY-SA 3.0[2]

O principal objetivo da ISO 16363 é definir um processo de auditoria e certificação para avaliar a confiabilidade dos repositórios digitais. Ela destina-se aos

[2] Disponível em: https://commons.wikimedia.org/wiki/File:Digitalrepositorystandards.png.

responsáveis pela auditoria de repositórios digitais e aos que são responsáveis por repositórios digitais e buscam a medição objetiva da confiabilidade de seu sistema. (CCSDS, 2011; ISO 16363:2012).

A norma está dividida em seções e anexos informativos e normativos. As seções 1-2 são informativas e fornecem uma visão de alto nível da lógica, do ambiente conceitual, de algumas questões importantes do projeto e uma introdução à terminologia e aos conceitos. A Seção 1 fornece propósito e escopo, a justificativa, uma visão da estrutura do documento e a lista de acrônimos, glossário e lista de referências para este documento. A Seção 2 fornece uma visão geral dos critérios de auditoria e certificação e uma discussão de padrões relacionados. As seções 3 a 5 fornecem as métricas normativas pelas quais um repositório digital pode ser avaliado.

Abaixo são listados a estrutura principal de tópicos da norma, todos os itens estão no Anexo I desta pesquisa:

- 1. Introdução
    - 1.1 Objetivo e Escopo
    - 1.2 Aplicabilidade
    - 1.3 Fundamentação
    - 1.4 Estrutura deste Documento
    - 1.5 Definições
    - 1.6 Conformidade
    - 1.7 Referências
- 2. Visão Geral dos Critérios de Auditoria e Certificação
    - 2.1 Um Repositório Digital Confiável
    - 2.2 Evidências
    - 2.3 Normas Relevantes, Melhores Práticas e Controles
- 3. Infraestrutura Organizacional
    - 3.1 Governança e Viabilidade Organizacional
    - 3.2 Estrutura Organizacional E Pessoal
    - 3.3 Responsabilidade Processual E Estrutura Da Política De Preservação
    - 3.4 Sustentabilidade Financeira
    - 3.5 Contratos, Licenças E Responsabilidades

- 4 Gerenciamento De Objetos Digitais
    - 4.1 *Ingest*: Aquisição De Conteúdo
    - 4.2 *Ingest*: Criação Do AIP
    - 4.3 Planejamento De Preservação
    - 4.4 Preservação De AIP
    - 4.5 Gestão Da Informação
    - 4.6 Gerenciamento De Acesso
- 5 Gestão De Risco De Infraestrutura E Segurança
    - 5.1 Gestão De Risco De Infraestrutura Técnica
    - 5.2 Gestão De Risco De Segurança

Em um contexto nacional, a ISO 16363 mostra sua importância, por exemplo, pela Resolução 43 do CONARQ (CONARQ, 2015). Essa resolução aborda os requisitos que um repositório digital deve seguir para poder ser considerado confiável, com base na norma e abrange todos os tipos de materiais digitais, inclusive os documentos arquivísticos. Sua estrutura e diretrizes estão todas fundamentadas pela norma internacional.

A importância da norma se dá ao fornecer uma estrutura para garantir que os repositórios digitais sejam confiáveis, e capazes de preservar o conteúdo digital a longo prazo. Ao seguir as diretrizes e requisitos da ISO 16363, os repositórios digitais podem demonstrar aos seus usuários que estão comprometidos em manter a integridade, autenticidade e acessibilidade de conteúdo digital.

3.12 CONCLUSÕES SOBRE A REVISÃO DE LITERATURA

Diante das múltiplas perspectivas abordadas nos estudos citados, observa-se uma convergência de temas essenciais em torno da preservação digital, repositórios digitais confiáveis, e a implementação de padrões como o OAIS e a ISO 16363. Cada um desses elementos contribui de maneira significativa para a formulação de um ecossistema de informações digitalmente sustentável e confiável.

Os autores apontam o impacto transformativo das ferramentas digitais nas instituições culturais como museus, onde a gestão de coleções é reimaginada e democratizada. Nesse sentido, a implementação de padrões rigorosos, como a ISO

16363, pode assegurar que essas transformações não apenas aumentem o acesso, mas também mantenham a qualidade e confiabilidade das informações ao longo do tempo.

Foi abordada a necessidade da confiabilidade, em relação à custódia de objetos digitais em repositórios digitais. A ISO 16363 pode fornecer um quadro de responsabilidade e autenticidade, ajudando as instituições a definir "dados e propriedades relevantes" que devem ser mantidos para preservar a integridade dos objetos arquivados.

O papel multifacetado de bibliotecas, museus e arquivos na preservação do patrimônio intelectual e cultural indicam que a confiança no conteúdo digital preservado não é simplesmente uma questão de tecnologia, mas também de práticas e políticas institucionais bem definidas. A ISO 16363 oferece um conjunto abrangente de critérios que abordam desde aspectos tecnológicos até questões de governança e sustentabilidade.

No contexto de acesso aberto e comunicação científica, padrões como OAIS e ISO 16363 ganham ainda mais relevância. Eles garantem que os repositórios não sejam apenas veículos para a disseminação de pesquisa, mas também ferramentas que podem proporcionar integridade e autenticidade informacional, aspectos fundamentais para a confiança das comunidades alvo.

Os autores assinalam o desafio inerente de aplicar o modelo OAIS em contextos diversos, especialmente em repositórios institucionais. A coesão entre OAIS e ISO 16363 pode oferecer uma estrutura para a preservação digital, combinando os atributos da responsabilidade administrativa, viabilidade organizacional e sustentabilidade com práticas e desempenhos auditáveis.

4 O TAINACAN

Para aplicar os resultados desta pesquisa, é necessário fazer a análise de um software de repositório digital. Foi então escolhido o software Tainacan para se verificar a conformidade em relação aos requisitos levantados na norma, apontando suas carências e sugerindo aprimoramentos.

O Tainacan é um software livre baseado em pesquisas científicas e experiências de implementação em instituições parceiras. Ele é uma ferramenta flexível e poderosa para o *WordPress*, permitindo a gestão e publicação de coleções digitais com facilidade, mas com todos os requisitos de uma plataforma profissional para repositórios (Feitosa; Oliveira, 2021).

Conforme verbete na *Wikipedia*, “O nome Tainacan vem da lenda de Tainacan dos povos indígenas Carajás. É uma entidade retratada por uma estrela, considerada a estrela vésper ou estrela d’alva, a primeira estrela a brilhar no anoitecer, possibilitando a percepção do espaço, suas diversidades, dimensões, galáxias e conexões (Tainacan, 2023).

Esse sistema de gestão de repositórios digitais *open-source* foi desenvolvido para facilitar a organização, gerenciamento e exibição de conteúdo digital em sites baseados em *WordPress*. Oferece uma variedade de recursos, como a possibilidade de criar coleções de itens digitais, adicionar metadados e configurar diferentes tipos de visualização. O Tainacan pode ser facilmente integrado a sites baseados em *WordPress* como um *plugin* da plataforma.

O *WordPress* é um sistema de gerenciamento de conteúdo (CMS) amplamente utilizado que alimenta mais de 43% dos sites na Internet. Ele é conhecido por sua simplicidade e facilidade de uso para usuários e editores, e sua flexibilidade e recursos ocultos complexos para desenvolvedores. O software é gratuito e de código aberto, permitindo que os usuários o modifiquem e controlem sem nenhuma taxa de licenciamento. Alguns dos recursos do *WordPress* incluem sua simplicidade, flexibilidade, ferramentas fáceis de publicação, gerenciamento de usuários, gerenciamento de mídia, conformidade total com os padrões, sistema de tema fácil, extensibilidade por meio de plug-ins, comentários integrados, otimização de mecanismo de pesquisa, suporte para vários idiomas e fácil instalação e atualizações.

Além disso, inclui importadores para várias outras plataformas de blogs/sites e permite que os usuários façam a gestão do seu conteúdo.

O Tainacan integra o enorme conjunto de *plugins* para o *Wordpress*, acrescentando várias funcionalidades, incluindo:

- Gestão estratificada de usuários;
- Configuração de coleções;
- Recursos de filtros e busca avançada;
- Gestão e configuração de metadados;
- Montagem e controle de taxonomias hierárquicas;
- Relatórios;
- APIs de exportação e importação de dados, e muito mais.

Ele também tem sido amplamente adotado em instituições de memória no Brasil e em outros países, e tem atraído interesse acadêmico crescente.

No Instituto Brasileiro de Museus (IBRAM), a plataforma já é usada por mais de vinte museus federais e se tornou uma referência setorial para a área. Os resultados dessa experiência foram documentados por Martins e Martins (2020) e Feitosa e Oliveira (2021). Na Fundação Nacional das Artes (FUNARTE), o Tainacan foi adotado para organização do acervo do Centro de Documentação em coleções de fotografias, cartazes, vídeos e programas de rádio produzidos pela instituição (Oliveira; Martins, 2019). No Instituto do Patrimônio Histórico e Artístico Nacional (IPHAN), encontra-se em processo de implantação para a organização do acervo do inventário do patrimônio imaterial.

O uso do Tainacan por museus e coleções universitárias vem sendo pesquisado por Martins e Martins (2020, 2021). Os dados das pesquisas mostram que o Tainacan já é usado por mais de 17 universidades públicas e privadas brasileiras. A pesquisa também mostra que dos 536 museus e coleções universitárias existentes no Brasil apenas 152 (28,36%) deles disponibilizam algum tipo de acervo digital em seus sites. Destes, apenas 39 iniciativas utilizam algum software de repositório digital, sendo o Tainacan o mais usado por essas iniciativas, estando presente em 23,09% delas.

Internacionalmente, o Tainacan foi adotado oficialmente por políticas públicas de outros países da América Latina e Europa, o projeto no México é um dos

destaques. Foi iniciada uma parceria com pesquisadores da Universidade Nacional Autónoma de México (UNAM), por meio da qual se construiu uma cooperação técnica com a Secretaria Nacional de Cultura e o projeto Mexicana, responsável pela organização das iniciativas públicas federais mexicanas de digitalização e difusão de acervos digitais em rede. A cooperação já resultou na publicação do acervo digital do *Repositório del Centro de La Imagen*, do Museo Nacional de Culturas Populares e *Museo de los Yaquis* com outros projetos em processo de implantação.

Os relatos de adoção do Tainacan como software para repositórios digitais mostram que suas principais características, a saber:

- Facilidade de tradução e internacionalização;
- Facilidade de adequação às necessidades internas das instituições;
- Facilidade em utilizar qualquer padrão de metadados, e Dublin Core nativo;
- Facilidade de indexação do seu conteúdo pelos principais sites de busca;
- Compatibilidade com qualquer tipo de documento ou acervo em formato digital;
- Navegação, busca facetada e consulta intuitiva;
- Conteúdo completo do repositório para coleta automatizada pelo protocolo de comunicação e consulta aberto OAI-PMH.

São várias ações em andamento envolvendo projetos experimentais, parcerias com universidades e com políticas públicas. O projeto Tainacan tem se tornado uma plataforma de pesquisa e desenvolvimento de iniciativas em torno da temática dos acervos digitais em rede.

4.1 CARACTERÍSTICAS DO SISTEMA

Itens

O Tainacan apresenta itens ao público em uma página do site *WordPress*. Cada item pertence a uma coleção única e pode ser descrito por metadados e pesquisado com filtros. O item obrigatoriamente tem um título e pode ter um

documento, que pode ser um link, arquivo ou texto puro. Além disso, itens têm propriedades adicionais, como miniatura, anexos de arquivo e permissão para comentários.

Taxonomias

Taxonomias são ferramentas de categorização de itens de coleções, compostas por um vocabulário de termos hierarquicamente estruturados, que permitem filtrar itens por categorias. São de nível de repositório e podem ser utilizadas por diferentes coleções.

Metadados

Os metadados são informações que descrevem as características de um item. Eles podem ser herdados por toda a coleção ou específicos de uma coleção. Existem vários tipos de metadados, como texto, numérico, taxonomia e relacionamento, e cada tipo oferece opções diferentes de configuração. Os itens possuem valores de metadados que podem ser usados para criar filtros e especificar consultas em uma pesquisa.

Filtros

O filtro de Metadados permite ao usuário pesquisar itens em consulta usando parâmetros específicos. Ele pode ser criado para uma coleção ou para o nível do Repositório e deve ser baseado em Metadados existentes. A estrutura de filtros fornece a conexão entre a interface de filtragem e a solicitação de itens.

Facetas

As facetas são ferramentas mais poderosas do que os pontos dos Filtros, mas possuindo as mesmas características. Elas permitem uma visão imediata do número de itens em uma coleção com um determinado filtro aplicado, sem precisar de uma pesquisa adicional. São utilizadas em listas de itens para exibir a contagem de itens ao lado das opções de filtragem.

Logs

O log é uma ferramenta que registra todas as alterações realizadas em um repositório de dados, como adições ou exclusões. No painel administrativo do Tainacan, essas mudanças são chamadas de Atividades. O log pode ser visualizado em diferentes níveis, como Repositório, Coleção ou Item, e pode ser usado por um moderador para aprovar ou negar modificações propostas por um editor.

OAI-PMH

Os Repositórios Tainacan também têm um ponto de extremidade OAI-PMH. Por padrão, o OAI-PMH usa Dublin Core como Formato de Metadados.

Coleções

No Tainacan, cada repositório tem coleções, grupos de itens descritos por metadados comuns. Cada item pertence a apenas uma coleção e cada metadado é criado para essa coleção. Uma coleção tem um nome e propriedades relacionadas à exibição, como miniatura, imagem de cabeçalho, modos de exibição e lista padrão.

API

As APIs do *WordPress* permitem que você crie *plugins* para estender o sistema. No Tainacan ela inclui vários parâmetros globais (também chamados de "metaparâmetros") que controlam como a API lida com o tratamento de solicitação/resposta. Estes operam em uma camada acima dos próprios recursos reais e estão disponíveis em todos os recursos.

O tema

O Tainacan interface fornece a extensibilidade para a plataforma. Em conjunto com o *plugin* Tainacan ele fornece recursos para gerenciar e publicar facilmente as coleções digitais com uma bela interface de pesquisa facetada, diferentes visualizações dos itens e coleções. Esse tema permite a personalização das páginas conforme a necessidade da instituição.

O projeto Tainacan opta por construir um caminho alternativo aos tradicionais softwares de repositórios digitais até então existentes, incorporando elementos até então não comuns a esses sistemas, como as conexões com redes sociais, por

exemplo. Usar a plataforma *WordPress* tem se mostrado uma decisão geradora de alto valor técnico.

Tecnicamente o *WordPress* demonstra ser uma tecnologia preocupada e atuante, sobretudo com a iniciativa do projeto Gutemberg, que acompanha as transformações da web em torno da flexibilização e maior grau de liberdade criativa na composição de páginas e sites. Vale ressaltar que este não é um ponto menor em se pensando em tecnologias para estimular a criação de repositórios digitais para instituições de memória considerando, sobretudo, que grande parte desse trabalho de mediação e extroversão cultural pode se valer dessa maior liberdade criativa.

5 PROCEDIMENTOS METODOLÓGICOS

A presente dissertação de mestrado se insere no âmbito da preservação digital, um campo que, nos últimos anos, tem se mostrado cada vez mais vital para a salvaguarda do patrimônio informacional e cultural em um mundo digitalizado. Adotando uma metodologia socioconstrutivista, esta pesquisa assume que o conhecimento é construído na interação entre os indivíduos e o seu ambiente, especialmente no que tange à interação com tecnologias digitais e a preservação de informações digitais.

A experiência do autor no campo da preservação digital e no desenvolvimento de software, liderando a equipe de desenvolvimento do sistema BarraPres do Modelo Hipatia[3] de Preservação Digital do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict), contribuiu profundamente com a pesquisa. Esta experiência não só proporcionou uma compreensão prática das nuances e desafios técnicos inerentes à preservação digital, mas também facilitou uma abordagem mais empática e informada para entender as necessidades, preocupações e expectativas dos usuários desses sistemas.

A orientação do idealizador do Tainacan nesta pesquisa é de valor inestimável. Sua perspectiva não apenas ajuda a aprofundar o entendimento sobre as complexidades técnicas e teóricas do software, mas também fornece insights sobre as intenções, aspirações e visões subjacentes ao melhoramento da ferramenta. Essas características permitem uma compreensão mais rica e multifacetada do campo da preservação digital, que é essencial para a condução de uma pesquisa eficaz e relevante.

No âmbito desta pesquisa, entende-se que os métodos exploratórios, aplicados e qualitativos podem ser usados em conjunto para obter uma visão mais completa e aprofundada do objeto de estudo. Cada tipo de pesquisa tem suas próprias vantagens, e combiná-los pode fornecer uma riqueza de informações.

Entende-se que, no contexto apresentado, esta pesquisa tem características exploratórias. Apresentando a flexibilidade necessária para o trabalho de investigação:

[3] Disponível em: https://hipatia.ibict.br.

> As pesquisas exploratórias têm como principal finalidade desenvolver, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores. De todos os tipos de pesquisa, estas são as que apresentam menor rigidez no planejamento. Habitualmente envolvem levantamento bibliográfico e documental, entrevistas não padronizadas e estudos de caso. Procedimentos de amostragem técnicas quantitativas de coleta de dados não são costumeiramente aplicados nestas pesquisas (Gil, 2008).

Ela também pode ser considerada aplicada, por considerar utilizar seus resultados no software Tainacan:

> A pesquisa aplicada, no que lhe concerne, apresenta muitos pontos de contato com a pesquisa pura, por depender de suas descobertas e se enriquece como seu desenvolvimento; todavia, tem como característica fundamental o interesse na aplicação, utilização e consequências práticas dos conhecimentos. Sua preocupação está menos voltada para o desenvolvimento de teorias de valor universal que para a aplicação imediata numa realidade circunstancial (Gil, 2008).

Tem características qualitativas, pois os critérios identificados da ISO 16363 serão avaliados em relação aos softwares para repositórios digitais:

> Na pesquisa qualitativa, o cientista é em simultâneo, o sujeito e o objeto de suas pesquisas. O desenvolvimento da pesquisa é imprevisível. O conhecimento do pesquisador é parcial e limitado. O objetivo da amostra é de produzir informações aprofundadas e ilustrativas: seja ela pequena ou grande, o que importa é que ela consiga produzir novas informações (Deslauriers, 1991, p. 58).

O objetivo central desta pesquisa foi propor requisitos de tratamento dos objetos digitais pelo software de repositório digital, conforme a norma ISO 16363, e analisar o software Tainacan sob os requisitos propostos, avaliando sua conformidade, apontando as carências e eventuais melhorias. A pesquisa é guiada pelas seguintes hipóteses:

- A norma ISO 16363 possui critérios específicos que orientam como o software de repositório digital deve automatizar rotinas no ambiente de preservação digital.
- É possível criar uma política de gestão de objetos digitais com base na ISO 16363.

- O software Tainacan não atende aos requisitos necessários para ser considerado um repositório digital confiável.

5.1 FASES DA PESQUISA

5.1.1 Delimitação de Critérios

Foi feita análise dos itens da norma ISO 16363, selecionando aqueles que se concentram especificamente no tratamento de pacotes de informação conforme definido pelo modelo OAIS.

Para essa análise foi elaborado quadro com todos os itens dos tópicos 3, 4 e 5. Os tópicos 1 e 2 foram descartados por tratarem de informações da própria norma.

O quadro está dividido em 3 colunas:

- **Coluna 1** – Tópicos - Descrições dos tópicos;
- **Coluna 2** – Responsável - O responsável pela ação que atende aquele tópico;
- **Coluna 3** – Ação - Ação para atender o tópico.

Os responsáveis por cada item foram classificados em:

- **Equipe gestora** – Equipe de pessoas responsáveis pela gestão informacional e institucional do repositório.
- **Software** – Todos os sistemas automatizados para gestão dos pacotes informacionais no repositório nos diferentes momentos da preservação.
- **Equipe de Infraestrutura tecnológica** – Equipe responsável por manter os servidores e softwares que fazem parte do repositório.

As ações atribuídas a cada um dos responsáveis foram:

- **Elaborar documentos –** Elaboração de documentos institucionais, documentos de gestão do repositório, documentação de transparência, documentação técnica informacional.
- **Verificar e validar automaticamente os pacotes –** Recursos tecnológicos para conferência dos pacotes de informação
- **Validar e autenticar o produtor –** Recursos tecnológicos para garantir a autenticidade do produtor da informação a ser preservada**.**

- **Disponibilizar relatório automático com as informações dos pacotes** – Relatórios de transparência das ações de preservação.
- **Controlar automaticamente os identificadores dos pacotes –** Recursos tecnológicos para garantir a integridade dos pacotes.
- **Controlar automaticamente as informações de representação dos pacotes -** Recursos tecnológicos para garantir a integridade dos pacotes.
- **Disponibilizar interface de busca –** Recurso tecnológico para prover acesso ao acervo preservado.
- **Realizar manutenção do ambiente tecnológico –** Ação de rotina da equipe de tecnologia.
- **Executar rotina de testes do ambiente tecnológico –** Ação das equipes para verificação da integridade das rotinas do ambiente tecnológico.

5.1.2 Proposição dos requisitos básicos de gestão de objetos digitais

Foi realizada descrição analítica dos 25 itens selecionados enfatizando a atuação do software em cada tópico. Foi aplicada uma análise SWOT[4], nomeada "Impacto para o Repositório" com o objetivo de avaliar as Forças, Fraquezas, Oportunidades e Ameaças de implantação, conforme se aplicam ao software de repositório digital.

5.1.3 Prova de conceito para análise da conformidade do software Tainacan

Foi realizado uma prova de conceito com o software Tainacan para avaliação, identificação de lacunas e pontos de melhoria. Foi utilizado uma instalação local (*localhost*) com acervo próprio de documentos bibliográficos.

[4] Análise SWOT é um método utilizado para avaliar as Forças, Fraquezas, Oportunidades e Ameaças envolvendo um projeto ou empreendimento. Serve para compreender o contexto interno e externo de uma estratégia ou planejamento.

6 ANÁLISE DA NORMA

A crescente quantidade de informação digital e a complexidade dos seus ambientes de preservação, apresentam desafios significativos para garantir a integridade das informações a longo prazo. Publicada em 2012, a ISO 16363 fornece uma estrutura para a auditoria e certificação de Repositórios Digitais Confiáveis que visa enfrentar esses desafios.

A ISO 16363 é baseada no modelo de referência OAIS, que estabelece uma estrutura conceitual comum para arquivamento digital. A norma define um conjunto de dimensões, agrupadas em três domínios: organizacional, técnico e operacional. Cada dimensão inclui um conjunto de critérios que devem ser atendidos para que um repositório seja considerado confiável.

Para desenvolver um Software de repositório digital conforme a ISO 16363, é necessário seguir os requisitos estabelecidos pela norma. É importante ressaltar que a norma ISO 16363 não é um guia para o desenvolvimento de Software, mas sim um conjunto de diretivas para a certificação de repositórios digitais confiáveis. Seguir essas diretivas habilita o software fazer parte desse ambiente confiável.

Para esta pesquisa, foram analisados todos os itens da norma, a partir da seção 3, com o objetivo de identificar como o s*oftware* de repositório digital deve agir no tratamento dos objetos digitais para garantir sua integridade.

6.1 DELIMITAÇÃO DOS CRITÉRIOS DA NORMA ISO 16363 QUE DEVEM SER ATENDIDOS ESPECIFICAMENTE PELOS SOFTWARE*S* DE REPOSITÓRIOS DIGITAIS

A aplicação rigorosa da norma ISO 16363 em repositórios digitais de preservação evidencia a necessidade de delimitar os critérios específicos que os softwares devem atender. Cada repositório possui particularidades inerentes ao seu tipo de acervo, metadados e comunidade alvo. Portanto, identificar os elementos da norma que se aplicam diretamente aos softwares contribui para uma implementação mais eficaz e adaptada às necessidades específicas de cada realidade. Essa prática também possibilita que os gestores de repositórios façam escolhas informadas ao avaliar ou desenvolver soluções de tecnologia que estejam em conformidade com padrões internacionais.

A necessidade de esses critérios também favorece a auditoria e certificação do repositório. As entidades certificadoras, ao terem um conjunto de critérios bem definidos e alinhados com as funcionalidades do software, podem realizar avaliações mais eficazes, garantindo que o sistema atende aos padrões de confiabilidade, integridade e preservação de longo prazo. Esse nível de detalhamento contribui para a transparência e a confiabilidade do repositório.

Os desenvolvedores de software podem utilizar essas especificações como um roteiro para aprimorar ou desenvolver funcionalidades que atendam aos padrões da ISO 16363. Pode-se também estimular a colaboração e o desenvolvimento conjunto de melhores práticas entre repositórios e desenvolvedores, o que é crucial para a evolução contínua e a sustentabilidade dos sistemas de preservação digital.

Foram analisados todos os tópicos das seções 3, 4 e 5 para estabelecer os responsáveis por cada requisito. Para ilustrar a abrangência de cada responsável, foi proposta a ação que deverá ser feita para atender ao requisito. As seções 1 e 2 da norma foram excluídas da análise por se tratar tópicos referentes a própria norma e definições de aplicação da auditoria.

A análise dos requisitos demonstrou que a norma possui critérios específicos para determinar como o software de repositório digital deve automatizar rotinas no ambiente de preservação, provando como correta a primeira hipótese desta dissertação.

Dos 105 itens analisados, foram definidos 25 requisitos onde a ação fica sob responsabilidade do software e suas rotinas automatizadas. Os itens foram colocados em uma tabela para melhor visualização de cada requisito que será avaliado. Para composição do quadro 3:

- Foram selecionados os itens referentes às responsabilidades do Software;
- Foram excluídos os itens que são os títulos de cada seção da norma;
- Foram agrupados os itens referentes a mesma ação do sistema.

Quadro 3 – Itens da norma que são funcionalidades do software

ITEM		DESCRIÇÃO
1	4.1.3 O repositório deve possuir especificações adequadas que permitam o reconhecimento e análise dos SIPs.	Software

2	4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais.	Software
3	4.1.5 O repositório deve ter um processo de *ingest*ão que verifique cada SIP quanto à integridade e exatidão.	Software
4	4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.	Software
5	4.1.7 O repositório deve fornecer ao produtor/depositante respostas apropriadas em pontos acordados durante os processos de *ingest*ão	Software
6	4.1.8 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para aquisição de conteúdo.	Software
7	4.2.3.1 O repositório deve seguir procedimentos documentados se um SIP não for incorporado a um *AIP* ou descartado e deve indicar porque o SIP não foi incorporado ou descartado.	Software
8	4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os *AIPs*. 4.2.4.1 O repositório deve identificar exclusivamente cada *AIP* dentro do repositório. 4.2.4.1.1 O repositório deve possuir identificadores únicos. 4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do *AIP* e seus componentes para serem únicos dentro do contexto do repositório. 4.2.4.1.3 A documentação deve descrever quaisquer processos usados 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 duplicações. 4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e futuros previsíveis do repositório, como número de objetos.	Software
9	4.2.4.2 O repositório deve possuir um sistema de serviços de ligação/resolução confiáveis para encontrar o objeto identificado de forma única, independentemente de sua localização física.	Software
10	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 alvo. 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.	Software

11	4.2.6 O repositório deve ter processos documentados para adquirir Informações de Descrição de Preservação (*PDI*) para suas Informações de Conteúdo associadas e adquirir *PDI* de acordo com os processos documentados. 4.2.6.1 O repositório deve ter processos documentados para aquisição de *PDI*. 4.2.6.2 O repositório deve executar seus processos documentados para aquisição de *PDI*. 4.2.6.3 O repositório deve garantir que a *PDI* seja persistentemente associada à informação de conteúdo relevante. Designada sobre o contexto.	Software
12	4.2.7 O repositório deve assegurar que as informações de conteúdo dos *AIPs* sejam compreensíveis para a sua *Comunidade alvo* no momento da criação do *AIP*. 4.2.7.1 O Repositório deve ter um processo documentado para testar a compreensão para suas Comunidades alvo 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 informação de conteúdo dos *AIPs*. 4.2.7.3 O repositório deve trazer as Informações de Conteúdo do *AIP* para o nível exigido de compreensão se falhar no teste de compreensão.	Software
13	4.2.8 O repositório deve verificar se cada *AIP* está completo e correto quando é criado.	Software
14	4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção/conteúdo do repositório.	Software
15	4.2.10 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para a criação da *AIP*.	Software
16	4.3.2 O repositório deve possuir mecanismos de monitoramento de seu ambiente de preservação.	Software
17	4.3.2.1 O repositório deve ter mecanismos para monitorar e notificar quando a Informação de Representação for inadequada para a Comunidade alvo entender os acervos de dados.	Software
18	4.3.3.1 O repositório deve possuir mecanismos para criar, identificar ou coletar qualquer Informação de Representação extra necessária.	Software
19	4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.	Software
20	4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs.	Software
21	4.4.2.2 O repositório deve ser capaz de demonstrar que quaisquer ações realizadas nos AIPs estavam conforme a especificação dessas ações.	Software
22	4.5.1 O repositório deve especificar os requisitos mínimos de informação para permitir que a Comunidade alvo descubra e identifique o material de interesse.	Software
23	4.5.3 O repositório deve manter ligação bidirecional entre cada AIP e suas informações descritivas.	Software
24	4.5.3.1 O repositório deve manter as associações entre seus AIPs e suas informações descritivas ao longo do tempo.	Software

25	4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias de gerenciamento de acesso	Software

Fonte: Elaborada pelo autor, 2023.

Como visto na tabela acima, os itens da norma atribuídos ao software são, em sua maioria, para gestão dos pacotes de informação, desde a sua entrada no sistema até a sua disponibilização, com foco na transparência das ações feitas em cada etapa da gestão da preservação.

No quadro 4 tem-se uma separação dos itens por responsável para melhor visualização de cada atribuição. É possível perceber a quantidade de ações que podem ser automatizadas pelos sistemas informatizados que fazem parte do repositório confiável.

Quadro 4 – Resumo das ações atribuídas aos responsáveis

AÇÃO/RESPONSÁVEL
Equipe de Infraestrutura tecnológica
Realizar manutenção do ambiente tecnológico
Equipe gestora
Elaborar documentos
Executar rotina de testes do ambiente tecnológico
Software
Controlar automaticamente as informações de representação dos pacotes
Controlar automaticamente os identificadores dos pacotes
Disponibilizar interface de busca
Disponibilizar relatório automático com as informações dos pacotes
Validar e autenticar o produtor
Verificar e validar automaticamente os pacotes

Fonte: Elaborada pelo autor, 2023.

No quadro 5 tem-se os quantitativos de itens atribuídos para cada responsável.

Quadro 5 – Quantidades de ações atribuídas aos responsáveis

AÇÃO POR RESPONSÁVEL	EQUIPE DE INFRAESTRUTURA TECNOLÓGICA	EQUIPE GESTORA	SOFTWARE	TOTAL GERAL
Controlar automaticamente as informações de representação dos pacotes			8	8
Controlar automaticamente os identificadores dos pacotes			8	8
Disponibilizar interface de busca			1	1
Disponibilizar relatório automático com as informações dos pacotes			15	15
Elaborar documentos		43		43
Executar rotina de testes do ambiente tecnológico		2		2
Realizar manutenção do ambiente tecnológico	21			21
Validar e autenticar o produtor			1	1
Verificar e validar automaticamente os pacotes			6	6
Total Geral	21	45	39	105

Fonte: Elaborada pelo autor, 2023.

A análise realizada focou na avaliação dos requisitos estabelecidos pela norma para softwares de repositórios digitais, especialmente no que diz respeito à automação de rotinas no contexto da preservação digital. Esta análise confirmou a hipótese inicial do estudo. Entre os 105 itens examinados, 25 foram identificados como requisitos diretamente relacionados às funções automatizadas do software.

7 PROPOSIÇÃO DOS REQUISITOS BÁSICOS DE GESTÃO DE OBJETOS DIGITAIS

A partir do estudo dos itens da norma, percebe-se que, para a ISO 16363, a gestão de objetos digitais vem como uma tarefa multidimensional, englobando vários eixos fundamentais que necessitam serem abordados:

- *Ingest*ão (*Ingest*): Nesse primeiro passo para do objeto digital dentro do repositório, a norma determina que cada repositório deve estabelecer procedimentos documentados para assegurar que as informações associadas ao objeto digital são sólidas o suficiente para permitir seu gerenciamento e preservação ao longo do tempo.
- Integridade de Dados: A ISO 16363 determina aos repositórios estabelecer mecanismos que detectem e alertem sobre quaisquer alterações não autorizadas nos pacotes de preservação. Este preceito visa preservar a autenticidade e integridade dos objetos digitais ao longo do tempo.
- Gerenciamento de Acesso: É imperativo que os repositórios mantenham sistemas rigorosos para gerir e documentar o acesso aos objetos digitais sob sua custódia. Estes mecanismos devem abordar questões relativas a quem tem direito de acesso, sob quais condições e quais níveis de interação permitidos com os objetos.
- Planejamento de Preservação: O repositório deve possuir uma estratégia de preservação bem documentada. Tal estratégia deve abranger protocolos para monitorar tanto o estado dos objetos digitais quanto as tecnologias requeridas para acessá-los. Confrontado com alterações ou ameaças emergentes, o repositório deve ser proativo na implementação de medidas para assegurar a continuidade da preservação.
- Gerenciamento de Metadados: A norma enfatiza que a integridade dos metadados está, intrinsecamente, ligada aos objetos digitais. É essencial que esses metadados estejam adequadamente associados aos objetos a que se referem, formando um elo indissociável.

- Manutenção dos *AIPs*: A usabilidade e a autenticidade dos *AIPs* são atributos que requerem manutenção contínua. A norma exige que os repositórios possuam processos sistemáticos que podem envolver atividades como migrações de formato e verificações de erros.

Cada um desses eixos não é isolado, mas um componente de um ecossistema que visa a preservação, o acesso e a autenticidade de objetos digitais em um ambiente de constante evolução tecnológica e organizacional.

7.1 ANÁLISE DOS ITENS

Primeiramente, viu-se a necessidade de se aplicar a análise SWOT sob um aspecto geral de avaliação do uso da ISO 16363 em um repositório digital, possibilitando às equipes uma melhor visualização da sua importância, conforme segue abaixo:

Forças (*Strengths*):

- Padronização Abrangente: A ISO 16363 oferece um conjunto abrangente de critérios para avaliar a confiabilidade de repositórios digitais, garantindo uma abordagem padronizada e abrangente.
- Melhoria Contínua: Facilita a implementação de práticas de melhoria contínua nos sistemas de arquivamento digital.
- Credibilidade Internacional: Como uma norma internacional, a ISO 16363 possui reconhecimento e credibilidade globais, o que eleva o padrão dos repositórios que a adotam.
- Auxílio na Tomada de Decisão: Auxilia organizações e instituições na escolha de sistemas de arquivamento digital confiáveis, baseando-se em critérios internacionalmente aceitos.

Fraquezas (*Weaknesses*):

- Complexidade e Custo: A implementação da ISO 16363 pode ser complexa e onerosa, especialmente para pequenas organizações ou aquelas com recursos limitados.

- Necessidade de Expertise Específica: Requer conhecimento técnico especializado para sua implementação e manutenção, o que pode ser um obstáculo para algumas organizações.
- Rigidez de Critérios: Os critérios rígidos podem não se adaptar bem a todas as situações ou tipos de repositórios digitais, especialmente aqueles com necessidades únicas ou inovadoras.
- Atualização Constante: Devido à rápida evolução tecnológica, a norma pode necessitar de atualizações frequentes para permanecer relevante.

Oportunidades (*Opportunities*):

- Crescente Necessidade de Preservação Digital: A crescente digitalização de conteúdos aumenta a demanda por sistemas de arquivamento confiáveis, destacando a relevância da ISO 16363.
- Parcerias e Colaborações: Possibilidade de formar parcerias e colaborações para compartilhar conhecimentos, práticas e recursos na implementação da norma.
- Inovação Tecnológica: O desenvolvimento de novas tecnologias pode oferecer soluções para simplificar a implementação da ISO 16363 e expandir sua aplicabilidade.

Ameaças (*Threats*):

- Evolução Tecnológica Rápida: Mudanças rápidas na tecnologia podem tornar alguns aspectos da norma obsoletos rapidamente.
- Concorrência de Outras Normas: Outras normas e frameworks de preservação digital podem surgir como alternativas à ISO 16363, oferecendo abordagens diferentes.
- Limitações no Reconhecimento: Embora seja uma norma internacional, pode haver limitações no reconhecimento e na adoção em algumas regiões ou setores.
- Desafios na Implementação: A complexidade e o custo associados podem desencorajar algumas organizações de adotar a norma.

Posteriormente, a análise foi feita também para cada item definido como escopo, para determinar como o software deve agir em um ambiente confiável de preservação digital segundo a norma. São descritas suas atribuições, critérios, recomendações e impacto para o repositório, como segue abaixo:

7.2 TÓPICO 4 DA NORMA - AQUISIÇÃO DE CONTEÚDO (*INGEST*)

7.2.1 Tópico 4.1 - *INGEST*: AQUISIÇÃO DE CONTEÚDO

4.1.3 O repositório deve possuir especificações adequadas que permitam o reconhecimento e análise dos SIPs.

O software precisa ter a criação do *Submission Information Packages (SIPs)* bem documentados e padronizados. A gestão eficaz desses *SIPs*, por meio de informações de pacotes bem-estruturados, garante a responsabilização, transparência e integridade do repositório ao longo do tempo. O software deve incorporar algoritmos de reconhecimento de padrões que possam identificar e validar tipos de arquivos e formatos, incluindo, mas não se limitando a imagens TIFF, arquivos HTML, e diversos formatos de multimídia. É essencial que o software vá além da mera extensão de arquivo para identificar a verdadeira natureza do arquivo, talvez usando *checksums* ou técnicas de análise de assinatura de arquivo, para garantir que o conteúdo é o que aparenta ser.

Também fazem parte das atribuições do software a captura e análise de metadados descritivos. Esses metadados não apenas possibilitam o armazenamento adequado dos SIPs, mas também garantem que sejam recuperados e contextualizados de forma eficaz, satisfazendo as necessidades da comunidade alvo. Esses elementos tendem a garantir a interoperabilidade e a longevidade dos dados; portanto, o software deve ser compatível com padrões de dados publicados para maximizar a utilidade e acessibilidade dos dados armazenados.

Complexidades inerentes aos objetos digitais modernos, que frequentemente compreendem múltiplos tipos de arquivos e estruturas, requerem que o software seja capaz de validar esses componentes de forma geral.

Impactos para o repositório

- Forças
    - Automatização do reconhecimento e validação de formatos
    - Suporte a padrões de metadados para melhor interoperabilidade
- Oportunidades
    - Integração com ferramentas de identificação e validação de formatos já existentes
    - Expansão do suporte para novos padrões de dados publicados
- Fraquezas
    - Complexidade de implementação e manutenção
    - Requisitos de hardware possivelmente altos devido à funcionalidade robusta
- Ameaças
    - Risco de obsolescência do software
    - Possíveis incompatibilidades com futuras versões de SIPs ou novos padrões de arquivo

4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais.

O software deve ser capaz de facilitar a criação e o armazenamento de contratos de apresentação ou depósito juridicamente válidos. Tais contratos não apenas formalizam as transferências de objetos digitais, mas também fornecem um fundamento legal que assegura a autenticidade das fontes.

Desse modo, o software deve ser o agente de segurança. A capacidade de integrar medidas tecnológicas para a autenticação do produtor torna-se obrigatória. Essas tecnologias podem abranger desde a verificação de assinaturas digitais até o uso de protocolos de criptografia. Este é um requisito crucial para manter a integridade do repositório e garantir que os objetos digitais armazenados são genuínos e oriundos de fontes confiáveis.

A manutenção de registros detalhados é outra funcionalidade que o software deve possuir. O sistema deve ser capaz de registrar todas as atividades relacionadas à autenticação e verificação da identidade do produtor. Estes registros se tornam elementos vitais durante auditorias ou avaliações pela comunidade alvo, contribuindo para a transparência e responsabilização.

Impactos para o Repositório

- Forças
    - Redução do risco de aceitação de materiais de fontes não autenticadas
    - A capacidade de criar e manter documentação jurídica e de procedimentos fortalece a integridade do repositório
- Oportunidades
    - A integração com tecnologias de segurança avançadas pode melhorar a robustez do processo de verificação
    - Abertura para auditoria por comunidades designadas pode aumentar a confiança no repositório
- Fraquezas
    - A necessidade de manter atualizados os mecanismos de segurança e autenticação pode ser onerosa
    - A complexidade legal associada aos contratos pode necessitar de conhecimento jurídico, que pode não estar facilmente disponível
- Ameaças
    - Falhas na verificação da identidade do produtor podem comprometer a integridade de todo o repositório
    - Mudanças nas leis ou normas de segurança podem exigir revisões caras e demoradas dos protocolos existentes

4.1.5 O repositório deve ter um processo de ingestão que verifique cada SIP quanto à integridade e exatidão.

É crucial detectar e corrigir erros no SIP, sejam esses erros originados na criação do pacote ou devidos a falhas de transmissão entre o depositante e o repositório. Neste cenário, o software deve servir como um mecanismo para gerar e manter logs de sistema detalhados, que fornecem um rastreamento completo das atividades relacionadas à *ingest*ão dos pacotes. Estes registros são indispensáveis para as atividades de verificação e auditoria, assegurando que o SIP esteja intacto e conforme as especificações.

O software deverá possuir integração com ferramentas e algoritmos especializados para a verificação da integridade dos pacotes submetidos. Estes mecanismos poderão realizar comparações automáticas entre os arquivos, os metadados técnicos e os descritivos, confirmando a integridade antes e após a *ingest*ão.

O software do repositório deve fornecer uma combinação de verificações automáticas, ferramentas de validação e procedimentos bem documentados para garantir que cada SIP seja processado conforme as expectativas e padrões estabelecidos pelo repositório. A implementação eficaz desta verificação protege contra a corrupção de dados, perda de informações e assegura a confiança na preservação a longo prazo.

Impactos para o repositório

- Forças
    - Capacidade de detectar e corrigir erros de forma proativa, o que é crucial para a integridade do acervo.
    - Os registros detalhados oferecem uma linha do tempo auditável, melhorando a transparência e a responsabilidade.
- Oportunidades
    - A otimização do processo de *ingest*ão através de automação e integrações pode aumentar a eficiência e a eficácia do repositório.
    - A flexibilidade para definir critérios de "completude" e "correção" permite adaptar-se às necessidades específicas de diferentes tipos de SIPs.
- Fraquezas
    - A complexidade e a variedade de SIPs podem exigir verificações manuais, o que pode ser demorado e sujeito a erros humanos.
    - A necessidade de manter atualizadas as ferramentas de verificação e os procedimentos pode ser onerosa.
- Ameaças
    - A falha em detectar erros na *ingest*ão pode levar a problemas de integridade de dados que são difíceis de corrigir posteriormente.

- Vulnerabilidades na transmissão de *SIPs* podem ser exploradas para comprometer a integridade do repositório.

4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.

Este requisito destaca a importância de o repositório ter o controle dos SIPs além da verificação de integridade e autenticidade para abranger o controle físico e legal completo dos bits dos objetos digitais. O software deve ser uma ferramenta ativa com funcionalidades para gerar e manter registros detalhados que delineiam o nível de controle que o repositório exerce sobre cada objeto digital, incluindo a localização do armazenamento e as permissões de acesso e modificação.

Paralelamente, o software precisa ter uma base de dados de metadados capaz de registrar e organizar todos os objetos digitais e seus metadados associados. Estas informações devem ser suficientemente detalhadas para validar a integridade dos objetos, e podem incluir variáveis como o tamanho do arquivo, a soma de verificação (*checksums*), a localização e o número de cópias existentes. Tal catálogo de metadados não apenas apoia a integridade dos dados, mas também serve como fonte para a auditoria e o monitoramento contínuo.

Impacto para o repositório

- Forças
  - A capacidade de demonstrar controle físico e legal robusto aumenta a confiança dos depositantes e usuários.
  - A robustez do catálogo de metadados facilita as operações de auditoria e as verificações de integridade, tornando o repositório mais confiável.
- Oportunidades
  - Avanços em tecnologias de controle de acesso e criptografia podem aumentar ainda mais o controle físico do repositório sobre seus objetos digitais.
  - As evoluções no campo dos direitos digitais podem fornecer novas abordagens para estabelecer controle legal.
- Fraquezas

- A falta de controle físico ou legal suficiente pode impedir atividades de preservação eficazes.
- Dependência de sistemas de terceiros para controle físico (como fornecedores de armazenamento em nuvem) pode apresentar riscos.

- Ameaças
  - Alterações nas leis de direitos autorais ou outras regulações podem comprometer o controle legal do repositório sobre seus objetos.
  - Vulnerabilidades de segurança no software de gestão ou no armazenamento físico podem resultar na perda de controle sobre os objetos digitais.

4.1.7 O repositório deve fornecer ao produtor/depositante respostas apropriadas em pontos acordados durante os processos de ingestão.

Este requisito enfatiza a importância da comunicação entre o repositório e o Produtor/Depositante durante o processo de *ingest*ão para garantir que o Produtor possa acompanhar o progresso do processo de *ingest*ão e verificar se não ocorreram erros ou perdas inadvertidas de SIPs.

O software deve ser capaz de documentar e monitorar o fluxo de trabalho do processo de *ingest*ão de dados. Deve oferecer recursos que permitam ao repositório configurar pontos específicos de notificação para o produtor/depositante. Estes pontos podem incluir etapas de validação de SIPs, transformações ou normalizações de dados e transferências de custódia.

Deve ter implementado geração automática de relatórios, correspondência via e-mail ou a criação de memorandos que podem ser compartilhados com os produtores/depositantes.

Impacto para o repositório

- Forças
  - Aumenta a transparência e a confiança entre o repositório e os produtores/depositantes.
  - Evita a perda inadvertida de Informações de Conteúdo por meio de relatórios e verificações regulares.

- Oportunidades
    - O uso de tecnologias de validação para certificar a integridade dos dados pode adicionar outra camada de confiança.
    - A adoção de padrões abertos pode facilitar a interoperabilidade com outros sistemas.
- Fraquezas
    - A falta de comunicação adequada pode resultar em falhas no processo de *ingest*ão e, consequentemente, na perda de dados.
    - A sobrecarga administrativa de gerar relatórios frequentes pode ser uma preocupação.
- Ameaças
    - Mudanças nos requisitos legais ou contratuais podem exigir revisões nos procedimentos de relatório, implicando em custos adicionais.
    - A falta de cumprimento rigoroso deste requisito pode colocar em risco a certificação do repositório sob a ISO 16363.

4.1.8 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para aquisição de conteúdo.

Neste requisito entende-se que o software de preservação digital deve oferecer um sistema de registro que seja capaz de capturar todas as ações, tanto administrativas quanto de processos, relacionadas à aquisição de conteúdo. Assim, atende a necessidade de rastreabilidade e autenticidade dos registros, que devem ser vinculados de forma indelével aos objetos digitais correspondentes.

O software deve garantir essa vinculação, assegurando um nível apropriado de integridade e autenticidade. Neste contexto, os metadados de preservação devem ser levantados para serem auditáveis e diretamente associados aos objetos digitais pertinentes.

Impacto para o repositório

- Forças
    - A presença de registros contemporâneos aumenta a confiabilidade e a transparência do repositório.

    - Facilita o processo de auditoria ao fornecer registros autênticos e rastreáveis.
- Oportunidades
    - A integração com tecnologias de validação atualizadas pode aumentar a confiabilidade dos registros.
    - A capacidade de adaptar-se a diferentes padrões internacionais oferece uma maior flexibilidade.
- Fraquezas
    - A necessidade de manter registros detalhados pode ser onerosa em termos de recursos computacionais e de armazenamento.
    - O sistema de registro deve ser mantido e atualizado regularmente, o que pode ser custoso.
- Ameaças
    - A falha em manter registros precisos e autênticos pode comprometer a integridade do repositório e resultar em falhas na auditoria.
    - Alterações em padrões ou regulamentações podem exigir modificações nos sistemas de registro, o que pode ser um desafio em termos de tempo e recursos.

7.2.2 Tópico 4.2 - Alimentação (*INGEST*): criação do AIP

4.2.3.1 O repositório deve seguir procedimentos documentados se um SIP não for incorporado a um AIP ou descartado e deve indicar porque o SIP não foi incorporado ou descartado.

É papel do software garantir que os SIPs recebidos tenham sido tratados de maneira apropriada e, em particular, que não tenham sido perdidos acidentalmente. No tratamento informacional desses registros é importante que sejam vinculados com metadados descritivos relevantes que forneçam informações contextuais sobre os objetos digitais envolvidos. Esta camada de metadados contribui para a rastreabilidade, e eventuais auditorias.

É necessário manter registros atualizados e detalhados dos fluxos de trabalho, desde a *ingest*ão até a transformação em *AIP*. As políticas, práticas recomendadas e a lógica de transformação de *SIP* em *AIP* devem estar estritamente documentadas,

bem como a sua rastreabilidade em caso de descarte e as razões específicas para tal decisão.

Impacto para o repositório

- Forças
    - Maior transparência na gestão de *SIPs*, o que melhora a confiança dos depositantes.
    - Facilitação de auditorias internas e externas.
- Oportunidades
    - Oportunidade para melhoria contínua com base em casos de *SIPs* não incorporados.
    - Possibilidade de integrar com sistemas de gerenciamento de documentos e outros sistemas de informação para melhor rastreabilidade.
- Fraquezas
    - Manter uma documentação rigorosa pode ser desafiador e consome tempo e recursos.
- Ameaças
    - Falhas na documentação podem resultar em perda de confiança e falhas nas auditorias.

4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs.

4.2.4.1 O repositório deve identificar exclusivamente cada AIP dentro do repositório.

4.2.4.1.1 O repositório deve possuir identificadores únicos.

4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do AIP e seus componentes de forma a serem únicos dentro do contexto do repositório.

4.2.4.1.3 A documentação deve descrever quaisquer processos usados 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 duplicações.

4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e futuros previsíveis do repositório, como número de objetos.

A eficácia do mecanismo de identificação tem implicações diretas para a integridade, rastreabilidade e acessibilidade dos *AIPs* armazenados. A garantia de identificadores únicos e persistentes não só cumpre uma função administrativa, mas também é fundamental para a preservação a longo prazo e a auditabilidade dos recursos

O software deve prover meios para disponibilizar a documentação formal das políticas adotadas na criação de identificadores. Deve ainda, ter mecanismos para rastrear as eventuais mudanças desses identificadores ao longo do tempo. Também é função do software impedir as possíveis duplicações.

Impacto para o repositório

- Forças
    - Integridade dos Dados: O uso de identificadores persistentes e únicos garante que cada *AIP* possa ser rastreado e gerenciado eficazmente ao longo do tempo, mantendo a integridade dos dados.
    - Auditabilidade: A presença de identificadores exclusivos facilita o processo de auditoria, uma vez que cada *AIP* pode ser facilmente localizado e verificado.
    - Acessibilidade: A utilização de identificadores bem-estruturados, melhora a facilidade com que os usuários finais e sistemas podem localizar e acessar AIPs.
- Oportunidades
    - Escalabilidade: Um sistema de identificação bem planejado oferece a possibilidade de expansão contínua, adaptando-se às necessidades futuras do repositório.

- Integração com Padrões Globais: A conformidade com ISO 16363 pode facilitar a integração com outros sistemas de preservação e metadados, oferecendo oportunidades para colaboração em larga escala.

- Fraquezas
  - Complexidade na Implementação: Dependendo da escala do repositório e do número de AIPs, a implementação de um sistema de identificação único e persistente pode ser tecnicamente desafiadora.
  - Custos Operacionais: Manter um sistema robusto de identificação pode exigir investimentos contínuos em termos de recursos financeiros e humanos.
- Ameaças
  - Obsolescência Tecnológica: A tecnologia em evolução pode tornar certos métodos de identificação obsoletos, exigindo atualizações frequentes.
  - Erro Humano: A complexidade do sistema pode levar a erros na atribuição ou manutenção dos identificadores, que podem ser difíceis de corrigir posteriormente.

4.2.4.2 O repositório deve ter um sistema de serviços confiáveis de vinculação/resolução a fim de encontrar o objeto exclusivamente identificado, independentemente de sua localização física.

Garantir a rastreabilidade e acessibilidade de Arquivos de Informação Preservada (AIPs) é vital em um cenário em que a infraestrutura de armazenamento e os recursos de software podem mudar com o tempo. Os repositórios necessitam de uma estratégia consolidada para assegurar que os identificadores atribuídos aos AIPs sejam consistentes em qualquer momento. A confiabilidade e integridade desses sistemas de identificação são fundamentais para a manutenção da cadeia de custódia e da prova de autenticidade dos pacotes.

Impacto para o repositório

- Forças
  - Rastreabilidade: Facilita a auditoria e a verificação do ciclo de vida dos AIPs.

    - Acessibilidade: Garante que os AIPs possam ser localizados e acessados quando necessário, independentemente de mudanças na infraestrutura.
- Fraquezas
    - Complexidade Técnica: O estabelecimento e manutenção de um sistema confiável podem exigir expertise técnico especializado.
    - Riscos de Falha: Um sistema mal projetado pode levar à perda de rastreabilidade e, consequentemente, à perda de dados cruciais.
- Oportunidades
    - Interoperabilidade: A conformidade com padrões abertos pode facilitar a integração com outros sistemas e repositórios.
    - Escalabilidade: Um bom sistema de identificação é fundamental para o crescimento e expansão do repositório.
- Ameaças
    - Obsolescência: A dependência de tecnologias ou padrões que podem se tornar obsoletos é um risco.
    - Custo: O desenvolvimento e manutenção de sistemas de vinculação/resolução eficazes podem ser custosos a longo prazo.

4.2.5 O repositório terá acesso a ferramentas e recursos necessários para fornecer informações de representação para todos os objetos digitais que 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 alvo.

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.

É possível incorporar algoritmos e bibliotecas para identificação automática do tipo de arquivo de cada objeto de dados recebido, conforme o requisito 4.2.5.1. Podendo ser feito por meio de técnicas como análise de assinatura de arquivo e correspondência de padrões.

Para atender ao requisito 4.2.5.2 deve prover também, meios para se agregar informações de representação aos objetos digitais. Em relação aos itens 4.2.5.3 e 4.2.5.4, o software pode ser projetado para integrar-se facilmente a registros externos dessas informações.

Impacto para o repositório

- Forças:
    - Facilitação da categorização, armazenamento e acessibilidade dos objetos de dados.
    - Melhoria da compreensibilidade e reutilização dos dados ao longo do tempo.
- Fraquezas:
    - Dependência de ferramentas e registros externos para identificação e associação de IR.
    - Complexidade e custo associados à determinação e gestão de IR.
- Oportunidades:
    - Adoção de padrões e práticas recomendadas na indústria.
    - Colaborações interinstitucionais para compartilhamento de recursos e conhecimentos.
- Ameaças:
    - Perda de acesso a ferramentas ou registros externos essenciais.
    - Evolução das necessidades da *Comunidade Alvo* que exigem atualizações frequentes da IR.

4.2.6 O repositório deve ter processos documentados para aquisição de Informações de Descrição de Preservação (PDI) para suas Informações de Conteúdo associadas e adquirir PDI de acordo com os processos documentados.

4.2.6.1 O repositório deve ter processos documentados para aquisição de PDI.

4.2.6.2 O repositório deve executar seus processos documentados para aquisição de PDI.

4.2.6.3 O repositório deve garantir que a PDI seja persistentemente associada à informação de conteúdo relevante.

Esse requisito enfatiza a importância de ter processos documentados para o *Preservation Description Information* (PDI). A *PDI* é um conjunto de metadados que garantem a autenticidade, integridade, e usabilidade de longo prazo dos objetos digitais armazenados em um repositório.

Após a documentação dos processos, o software deve prover alternativas automatizadas, que capturam, validam, e armazenam a *PDI* conforme definido nos processos. A automação, pode melhorar a eficiência da captura, mas devem ter a possibilidade de serem auditadas regularmente.

O software precisa ser concebido de maneira a garantir que o *PDI* coletada esteja permanentemente associado à respectiva Informação de conteúdo. Geralmente é realizado através de identificadores únicos, que permitem um mapeamento inequívoco entre a *PDI* e o objeto digital. A implementação desses princípios em um software envolveria a criação de módulos específicos para a gestão da *PDI*. Estes módulos seriam responsáveis pela captura automática de metadados, validação de integridade, e associação permanente dessas informações com os respectivos objetos digitais.

Impacto para o repositório

- Forças:
    - Adoção de processos bem documentados melhora a consistência e confiabilidade da aquisição de *PDI*.
    - Fortalece a capacidade do repositório para fornecer uma trilha auditável e alegações de autenticidade.
- Fraquezas:
    - Falhas na execução ou na associação de *PDI* podem comprometer a integridade e a confiabilidade dos objetos digitais.

    - Dependência de expertise para manter e atualizar os processos documentados e o software utilizado.
- Oportunidades:
    - Aperfeiçoamento contínuo dos processos e práticas, alimentado por feedback da *Comunidade Alvo* e auditorias.
    - Colaboração com outros repositórios e organizações para melhorar os padrões e ferramentas para a gestão de *PDI*.
- Ameaças:
    - Riscos relacionados à segurança dos dados e ao acesso não autorizado.
    - Risco de desatualização de software e documentação, tornando o processo obsoleto.

4.2.7 O repositório deve assegurar que as informações de conteúdo dos AIPs *sejam compreensíveis para a sua Comunidade alvo no momento da criação do AIP.*

> *4.2.7.1 O Repositório terá um processo documentado para testar a compreensibilidade para suas Comunidades Designadas das Informações de Conteúdo dos* AIPs *na sua criação.*
>
> *4.2.7.2 O repositório executará o processo de teste para cada classe de Informação de Conteúdo dos* AIPs*.*
>
> *4.2.7.3 O repositório deve trazer a Informação de Conteúdo do AIP até o nível necessário de compreensibilidade se falhar no teste de compreensibilidade.*

Para a correta preservação digital o software deve ter processos automatizados e documentados que verifiquem a compreensibilidade da Informação de Conteúdo dos AIPs. Envolve não apenas o armazenamento da informação, mas também a validação por meio de algoritmos ou fluxos de trabalho que verifiquem sua inteligibilidade e utilidade para a comunidade alvo. Métodos podem incluir a execução de scripts que verifiquem a integridade e a legibilidade de conjuntos de dados ou formatos de arquivo.

O requisito 4.2.7.2 especifica que o software deve executar esses testes de compreensibilidade para cada classe de Informação de Conteúdo dos AIPs. Isso

significa que o sistema deve ser flexível o suficiente para lidar com uma variedade de tipos e formatos de informação. Ele também deve ser escalável para aplicar essas verificações em grandes volumes de dados. Tais testes devem ser registrados e auditáveis, permitindo não apenas a verificação posterior, mas também a revisão e atualização contínua dos critérios de compreensibilidade à medida que as necessidades da comunidade alvo evoluem.

Se um teste de compreensibilidade falhar, como apontado em 4.2.7.3, o software deve fornecer informações para que medidas corretivas possam ser implementadas. Pode envolver, por exemplo, a adição de metadados, a conversão de arquivos para formatos mais acessíveis, ou mesmo a inclusão de documentação suplementar.

Impacto para o repositório

- Forças:
    - Testes eficazes e bem documentados fortalecem a confiança da comunidade alvo.
    - Processos de melhoria de compreensibilidade garantem a utilidade dos AIPs a longo prazo.
- Fraquezas:
    - Falha em garantir a compreensibilidade pode resultar em informação preservada inútil.
    - O processo pode ser laborioso e necessitar de recursos consideráveis.
- Oportunidades:
    - Engajamento ativo com a *Comunidade Alvo* pode fornecer insights valiosos para melhorar a compreensibilidade.
    - Cooperação com outros repositórios e entidades de normalização para desenvolver melhores práticas.
- Ameaças:
    - Mudanças na linguagem ou na tecnologia podem tornar os *AIPs* incompreensíveis com o tempo.

- Fatores externos, como a perda de especialistas em domínio ou financiamento insuficiente, podem prejudicar os esforços para melhorar a compreensibilidade.

4.2.8 O repositório deve verificar se cada AIP está completo e correto quando é criado.

A verificação de integridade e exatidão dos AIPs no momento de sua criação é ponto fundamental para estabelecer a confiabilidade do repositório digital. Para o software, essa verificação pode ser automatizada usando uma combinação de algoritmos de *hash*, *checksums* e outras técnicas criptográficas para assegurar que o *AIP* não sofreu alterações indesejadas durante o processo de *ingest*ão e criação. Além disso, o software pode também realizar uma comparação entre o SIP e o AIP para garantir que a transformação entre os dois não introduziu erros ou inconsistências. O software deverá também manter registros detalhados dessas operações, permitindo futuras auditorias.

A documentação deve detalhar o fluxo de trabalho de verificação adotado pelo repositório, desde a recepção do SIP até a criação e armazenamento do *AIP*. Deve incluir informações sobre quais verificações são realizadas, em que etapas do processo elas ocorrem e como são registradas. Isto contribui para a transparência e confiabilidade do repositório.

Impacto para o repositório

- Forças:
  - Estabelece uma base sólida para a confiabilidade dos AIPs.
  - Facilita o rastreamento e a auditoria futura.
- Fraquezas:
  - Pode ser um processo que consome tempo e recursos, especialmente para grandes volumes de dados.
- Oportunidades:
  - A conformidade com este requisito pode ser um diferencial para ganhar a confiança dos *stakeholders*.
  - Potencial para automatização e otimização do processo.
- Ameaças:

- Falha no cumprimento deste requisito pode comprometer todo o sistema de preservação.
- Mudanças em padrões ou formatos de dados podem exigir atualizações constantes no processo de verificação.

4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção/conteúdo do repositório.

O repositório deve possibilitar sua auditoria por um mecanismo independente para verificar a integridade de todo o conteúdo armazenado. Para o software, isso pode ser realizado por meio de verificações periódicas no conteúdo armazenado, fazendo uso de metadados, *checksums* e outros identificadores para assegurar que o conteúdo permanece íntegro. Essa funcionalidade de auditoria seria especialmente projetada para operar de forma independente dos outros componentes do sistema, garantindo uma camada adicional de segurança e confiabilidade.

Esse requisito determina que um registro de auditoria detalhado deve ser mantido com informações como as datas em que as verificações foram realizadas, os algoritmos ou métodos utilizados para a verificação e os resultados dessas verificações. Este mecanismo de auditoria pode também cruzar referências com acordos documentados entre o produtor e o repositório, bem como registros do material recebido e outras ações associadas.

Impacto para o repositório

- Forças:
  - Garante um nível adicional de segurança e confiabilidade para os *stakeholders*.
  - Facilita a conformidade com padrões de auditoria e regulamentos legais.
- Fraquezas:
  - Implementar tal mecanismo pode ser complexo e oneroso em termos de recursos.
- Oportunidades:
  - Melhoria da reputação e da confiabilidade do repositório.

    - Oportunidades para identificar e corrigir problemas antes que se tornem críticos.
- Ameaças:
    - Falha em implementar um mecanismo eficaz pode comprometer a integridade da coleção.
    - Vulnerabilidade a erros humanos ou falhas de sistema durante o processo de auditoria.

4.2.10 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para a criação da AIP.

O requisito destaca a importância de manter registros atualizados das ações e processos administrativos relacionados à criação do AIP. Para implementar essa diretriz, o software deve prover um mecanismo sofisticado de relatórios e rastreamento integrado em todas as fases do ciclo de vida do *AIP*. Esta funcionalidade não apenas armazena metadados administrativos, mas também associa esses registros diretamente ao objeto *AIP*. Esta abordagem permite uma correspondência direta entre o objeto preservado e as ações administrativas e processuais que afetaram sua criação e manutenção.

Estes registros contemporâneos funcionam como uma camada de metadados de auditoria e devem ser projetados para serem imutáveis e protegidos contra adulteração. Um sistema de *hash*, pode verificar a integridade dos registros ao longo do tempo. Esses registros devem ser acessíveis apenas a pessoal autorizado e devem ser mantidos de forma segura para garantir sua integridade. Adicionalmente, devem ser concebidos para serem interoperáveis facilitando a validação independente e a auditoria.

A necessidade de tais registros ultrapassa a mera conformidade com as diretrizes; ela atua como uma garantia de transparência e responsabilidade e são um componente fundamental para estabelecer a confiabilidade do repositório, permitindo que ele justifique suas práticas e assegure à comunidade alvo que os *AIPs* são gerenciados e preservados de acordo com os padrões aceitos.

Impacto para o repositório

- Forças:
    - Aprimora a capacidade do repositório de provar a autenticidade e a integridade dos AIPs.
    - Facilita a auditoria e o cumprimento das normas e regulamentações.
- Fraquezas:
    - Requer uma implementação tecnológica robusta e possivelmente complexa.
- Oportunidades:
    - Alinha o repositório com melhores práticas de governança de dados e transparência.
    - Potencial para melhorar a eficiência operacional por meio de análises de logs.
- Ameaças:
    - Risco de falha no registro de atividades críticas, o que pode comprometer a integridade do repositório.
    - A inadequada manutenção dos registros pode resultar em não conformidade com os padrões ISO.

7.2.3 Tópico 4.3 - Plano de preservação

4.3.2 O repositório deve possuir mecanismos de monitoramento de seu ambiente de preservação.

O requisito 4.3.2 aborda a importância de monitorar ativamente o ambiente de preservação para assegurar que a informação arquivada permaneça compreensível e utilizável ao longo do tempo, especialmente para a comunidade alvo. O software deve prover alertas automatizados quando detectar que um determinado formato de arquivo está se aproximando da obsolescência. Além disso, deve ser capaz de se integrar com registros externos para buscar atualizações e disponibilizar informações claras, periodicamente, para melhor atender a comunidade alvo.

Impacto para o repositório

- Forças:

    - Permite ao repositório antecipar problemas antes que se tornem críticos.
    - Melhora a qualidade e a usabilidade dos dados preservados.
- Fraquezas:
    - Requer recursos adicionais para monitoramento contínuo.
- Oportunidades:
    - Facilita a conformidade com os padrões ISO e outras regulamentações.
    - Abre canais de comunicação com a *Comunidade Alvo* para melhorar a qualidade dos serviços.
- Ameaças:
    - Falha na monitorização pode resultar em perda de dados ou em dados tornando-se inutilizáveis.
    - Riscos associados à dependência de registros externos para monitoramento.

4.3.2.1 O repositório deve ter mecanismos para monitorar e notificar quando a Informação de Representação for inadequada para a Comunidade alvo entender os acervos de dados.

Esse requisito determina que o repositório identifique e responda proativamente quando as Informações de Representação se tornarem obsoletas ou inadequadas para a comunidade alvo. O objetivo é demonstrar que a preservação digital não é apenas guardar arquivos, mas manter a informação contextual compreensível ao logo do tempo.

O software deve prover mecanismos de registro que monitoram a viabilidade de implementação de diferentes formatos e metadados. Esse recurso pode ser por meio de conexões automáticas de serviços que fazem esse serviço e prover painéis informativos para a comunidade alvo.

Impacto para o repositório

- Forças:
    - Mantém muita relevância e utilidade da informação preservada para a Comunidade Alvo.

    - Pode reduzir o risco de obsolescência ao manter-se atualizado com as tecnologias e práticas atuais.
- Fraquezas:
    - Pode ser oneroso, tanto em termos de recursos financeiros como humanos, manter sistemas de monitorização e notificação.
- Oportunidades:
    - Aperfeiçoamento dos processos e políticas de preservação com base nos feedbacks e necessidades da *Comunidade Alvo*.
    - Adaptação proativa às mudanças tecnológicas que podem afetar a adequação das informações de representação.
- Ameaças:
    - Se a monitorização e as notificações falharem, há o risco de que as informações de representação se tornem inadequadas para a *Comunidade Alvo*.

4.3.3.1 O repositório deve possuir mecanismos para criar, identificar ou coletar qualquer Informação de Representação extra, se necessário.

O requisito 4.3.3.1 destaca a necessidade de mecanismos que permitam ao repositório reunir ou criar informações de representação adicionais para garantir a compreensibilidade e a usabilidade do conteúdo digital. O software pode prover painéis informativos, conectados a serviços de monitoramento externos, que mostrem a aproximação da obsolescência ou inviabilidade das informações, incluindo formatos.

Impacto para o repositório

- Forças:
    - Capacidade de antecipar e reagir a obsolescência tecnológica.
    - Mantém a usabilidade e a compreensibilidade das informações a longo prazo.
- Fraquezas:
    - Requer recursos adicionais para monitoramento e aquisição de informação de representação extra.
- Oportunidades:

- Aumenta a confiança da *Comunidade Alvo* no repositório.
- Abertura para colaboração e integração com outras instituições e serviços.

- Ameaças:
  - Falha na atualização de informações de representação pode levar à perda de acesso ou compreensão do conteúdo.

4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.

O requisito 4.3.4 enfatiza a importância de o repositório fornecer evidências da eficácia de suas atividades de preservação. Serve como um meio de responsabilidade e transparência, demonstrando que a informação permanece acessível, compreensível e utilizável ao longo do tempo para a Comunidade alvo. Assim, o software pode prover mecanismos para prova contínua de usabilidade dos objetos digitais e prover relatórios periódicos dessas rotinas.

Impacto para o repositório

- Forças:
  - Estabelece confiança na Comunidade Alvo.
  - Permite a avaliação contínua da eficácia das atividades de preservação.
- Fraquezas:
  - Necessita de recursos humanos e computacionais para auditorias e testes regulares.
- Oportunidades:
  - Melhoria contínua com feedback da *Comunidade Alvo*.
  - Estabelecimento de melhores práticas no setor de preservação digital.
- Ameaças:
  - Falha em fornecer provas suficientes pode erodir a confiança da *Comunidade Alvo*.
  - Falha na integridade do arquivo se as práticas de preservação não forem eficazes.

7.2.4 Tópico 4.4 - Preservação do *AIP*

4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs.

O requisito 4.4.1.2 enfatiza a necessidade de monitoramento ativo da integridade dos AIPs. Cabe ao software fornecer mecanismos automatizados para gerar e armazenar informações de fixidez (*checksums*) de cada objeto digital e *AIP* com registro detalhados e seguros, inclusive sendo guardados separadamente para evitar adulterações

Impacto para o repositório

- Forças:
    - Garante a autenticidade e integridade dos AIPs.
    - Facilita a auditoria e o cumprimento de normas de governança de dados.
- Fraquezas:
    - Requer um investimento em recursos computacionais e humanos para monitoramento e verificação contínuos.
- Oportunidades:
    - Fortalece a confiança das partes interessadas, incluindo financiadores e a *Comunidade Alvo*.
    - Permite intervenções proativas em caso de comprometimento da integridade dos dados.
- Ameaças:
    - Uma falha no monitoramento pode comprometer a integridade dos AIPs e erodir a confiança das partes interessadas.

4.4.2.2 O repositório deve ser capaz de demonstrar que quaisquer ações realizadas nos AIPs *estavam conforme a especificação dessas ações.*

O requisito destaca a importância de manter a conformidade nas ações executadas em AIPs. É necessário uma rigorosa documentação e práticas de auditoria para garantir que as operações realizadas nos AIPs estão alinhadas com as políticas e procedimentos estabelecidos.

Nesse cenário o software deve manter registros dos metadados relacionados às ações realizadas nos AIPs, permitindo que auditorias sejam realizadas conforme as especificações documentadas.

Impacto para o repositório

- Forças:
    - Aumenta a transparência e responsabilidade nas operações de preservação.
    - Fortalece a confiança das Comunidades Designadas e outros *stakeholders*.
- Fraquezas:
    - Necessita de recursos adicionais para auditorias regulares.
    - Pode ter implicações para o desempenho do sistema.
- Oportunidades:
    - Facilita o processo de auditoria externa e certificação.
    - Contribui para a melhoria contínua através do feedback de auditoria.
- Ameaças:
    - Não conformidade pode levar a comprometimento de dados e perda de reputação.
    - O risco de erro humano na interpretação e implementação dos procedimentos.

7.2.5 Tópico 4.5 - Gestão da informação

4.5.1 O repositório deve especificar os requisitos mínimos de informação para permitir que a Comunidade alvo acesse e identifique o material de interesse.

O requisito estabelece a necessidade de um repositório especificar as informações mínimas facilitar a pesquisa do material por parte da Comunidade Alvo. Implica que o software deve permitir a inclusão, armazenamento e recuperação de metadados de acesso, como o Dublin Core, para cada objeto digital.

Impacto para o repositório

- Forças:
    - Facilita a descoberta de material, melhorando a utilidade e acessibilidade.
    - Aumenta a eficiência na recuperação de informações.
- Fraquezas:
    - Exige investimento em hardware e software para suportar funcionalidades avançadas de pesquisa.
    - Podem necessitar de manutenção contínua para assegurar a qualidade dos metadados.
- Oportunidades:
    - Melhora o engajamento com a *Comunidade Alvo*.
    - Abre portas para colaborações e parcerias baseadas em padrões de metadados.
- Ameaças:
    - Metadados inadequados ou incompletos podem levar a ineficiências na descoberta.
    - A falha em atender às expectativas da *Comunidade Alvo* pode resultar em menor confiança no repositório.

4.5.3 O repositório deve manter ligação bidirecional entre cada AIP e suas informações descritivas.

O requisito mostra a importância de manter uma ligação bidirecional entre cada *AIP* e as suas informações descritivas correspondentes. Desse modo, o software deve armazenar os metadados e suas associações utilizando recursos como identificadores únicos, permitindo que as informações descritivas apontem para pelo menos um pacote. Todo esse procedimento, assim como o fluxo de trabalho e a arquitetura técnica, devem ser documentados para eventuais auditorias e transparência.

Impacto para o repositório

- Forças:
    - Melhora a confiabilidade e a integridade dos dados.

    - Facilita a recuperação e localização de AIPs e seus metadados associados.
- Fraquezas:
    - Requer uma arquitetura de software bem planejada e possivelmente complexa.
    - Pode exigir mais recursos computacionais e de armazenamento.
- Oportunidades:
    - Possibilidade de integração com outros sistemas ou redes que utilizem padrões de metadados semelhantes.
    - Melhora a reputação e confiabilidade do repositório.
- Ameaças:
    - A falha na implementação deste requisito pode comprometer a integridade dos AIPs.
    - Mudanças na tecnologia ou padrões de metadados podem exigir atualizações frequentes.

4.5.3.1 O repositório deve manter as associações entre seus AIPs *e suas informações descritivas ao longo do tempo.*

Esse item estende a necessidade de manter associações entre AIPs e suas informações descritivas, enfatizando a importância da persistência dessas associações ao longo do tempo. O software deve prover mecanismos para monitorar a Integridade das associações e manter registros detalhados das atividades que afetam a integridade dos *AIPs* e suas associações com as informações descritivas.

Essas ações devem permitir que as associações possam ser restauradas, caso haja necessidade e implementar auditorias automatizadas que validem a integridade das associações depois das modificações.

Impacto para o repositório

- Forças:
    - Garante que as informações descritivas estão sempre associadas aos seus respectivos AIPs, aumentando a confiabilidade.
- Fraquezas:

    - Pode exigir recursos computacionais significativos para monitoramento e manutenção contínuos.
- Oportunidades:
    - Aprimora a resiliência e robustez do repositório contra falhas de software ou *hardware*.
- Ameaças:
    - A negligência na manutenção dessas associações pode levar à perda de acessibilidade e comprometimento da integridade dos dados.

7.2.6 Tópico 4.6 – Gestão de acesso

4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias no gerenciamento de acesso.

O requisito estabelece a importância de registrar e revisar falhas e anomalias no sistema de gerenciamento de acesso. O objetivo é identificar potenciais ameaças de segurança e falhas que possam comprometer a integridade dos dados armazenados. O software deve manter logs detalhados dos eventos de acesso, incluindo tentativas bem-sucedidas e falhas. Deve permitir realizar análises automatizadas dos logs para identificar anomalias que possam indicar ameaças de segurança e ser capaz de emitir alertas em tempo real para as revisões necessárias.

Impacto para o repositório

- Forças:
    - A detecção precoce de anomalias pode prevenir comprometimentos de segurança.
- Fraquezas:
    - A necessidade de manter e revisar logs pode exigir recursos adicionais, tanto em termos de armazenamento como de poder computacional.
- Oportunidades:
    - A integração com outras soluções de segurança pode fornecer uma camada extra de proteção.
- Ameaças:

- Falha em cumprir este requisito pode tornar o repositório vulnerável a ataques externos e internos.

7.3 CONSIDERAÇÕES SOBRE A PROPOSIÇÃO DOS REQUISITOS APRESENTADOS

Para Carvalho, *et. al*. (2014), o arcabouço normativo estabelecido pela ISO 16363 tem como objetivo funcionar como uma instrumentalidade para a auditoria, avaliação e possível certificação de repositórios digitais. Este referencial não apenas estipula os parâmetros documentais requeridos para conduzir um procedimento de auditoria eficaz, mas também define os critérios mínimos que os auditores devem atender, esboçando assim o itinerário para um processo de certificação bem-sucedido.

Ao implementar esta norma em um ecossistema de repositórios institucionais, a meta é reforçar a confiança dos usuários da comunidade alvo. Esse aumento de confiança é alcançado por meio da instauração de um ambiente transparente, onde os processos relativos à gestão, preservação e acesso aos objetos digitais são explicitamente declarados e verificáveis.

O resultado da análise e proposição dos requisitos da ISO 16363, destaca itens que detalham a necessidade de se desenvolver um sistema que garanta a integridade, autenticidade e acessibilidade de objetos digitais a longo prazo, juntamente com um monitoramento contínuo do ambiente de preservação, para identificar possíveis ameaças à estabilidade dos dados, seja por obsolescência tecnológica ou por outros fatores externos. O desenvolvimento dessas funcionalidades, pode possibilitar ações preventivas ou corretivas em tempo hábil, evitando a perda de informações valiosas e mantendo a confiança da comunidade alvo.

A necessidade de registros atualizados das ações e processos administrativos associados à criação dos pacotes de Informação fortalece a governança do repositório, melhorando seus processos de guarda e na verificação independente das ações de preservação.

Os requisitos analisados provaram como correta a hipótese de ser possível a construção de uma política de gestão de objetos digitais, a partir da ISO 16363, destacando o papel do software no processo. Entretanto, a implementação desses

requisitos estabelece um precedente para a excelência em preservação e gestão de dados, com implicações que se estendem muito além do software, mas envolve todo o esforço institucional para a preservação digital.

8 PROVA DE CONCEITO DO SOFTWARE TAINACAN EM RELAÇÃO AOS ITENS DA NORMA ISO 16363 PROPOSTOS COMO REQUISITOS BÁSICOS

Vale lembrar que o objetivo dessa análise é avaliar o Tainacan como um software para preservação digital em um Repositório Digital Confiável, onde se garanta, ao longo do tempo, a autenticidade dos objetos digitais que estão sob a gestão do sistema.

A autenticidade funciona como uma medida de integridade e confiabilidade dos objetos digitais no repositório. Para Duranti (2005), um documento autêntico é aquele que está "livre de fraude ou corrupção", o que enfatiza a necessidade de garantir que os documentos digitais mantenham suas características originais desde o momento da sua criação.

Arellano (2006) destaca a necessidade de se controlar os diferentes aspectos do objeto digital para garantir a originalidade de um registro eletrônico. Neste cenário que padrões internacionais, como a ISO 16363, ganham relevância. A implementação desses critérios na política de preservação institucional fornece um grau de confiabilidade necessário para os usuários que dependem desses documentos para diversos fins. Qualquer estratégia de preservação digital eficaz deve incorporar mecanismos para o monitoramento e a atualização de metadados, e assegurar a autenticidade ao longo do ciclo de vida dos objetos digitais dando base para um ecossistema de preservação digital resiliente e confiável.

Nesse contexto, o Tainacan, como sistema de gestão, possui grande capacidade para armazenamento e catalogação de objetos digitais. No entanto, para se tornar um sistema totalmente aderente às normas da ISO 16363, é necessário desenvolver modificações e aprimoramentos no software. Abaixo são destacados os pontos críticos que justificam a avaliação e possíveis modificações do Tainacan para melhor se alinhar às especificações da norma.

8.1 ADESÃO AO MODELO OAIS

O modelo OAIS (ISO 14.721:2012) enquanto estrutura conceitual que oferece arcabouço para a preservação de longo prazo de informações digitais, precisa ser seguido com rigoroso critério para assegurar a integridade, acessibilidade e sustentabilidade dos objetos digitais.

O Tainacan não foi criado como um sistema que garanta a integridade, autenticidade e acessibilidade de objetos digitais a longo prazo, conforme o modelo OAIS. Para o Tainacan atingir conformidade com o esse modelo e, por consequência, ser aderente aos requisitos da ISO 16363, é necessário que ele seja capaz de seguir seus principais critérios.

Em relação aos pacotes de informação, o sistema precisa implementar processos para criar SIPs e transformá-los em AIPs. Incluindo no processo a validação e/ou conversão de formatos, a verificação de metadados e a avaliação de integridade.

Deve ainda melhorar seu gerenciamento de metadados para facilitar o descobrimento, a classificação e o acesso aos AIPs. Envolve a manutenção de registros administrativos, em ambiente com soluções de armazenamento que sejam de fácil adaptação ao aumento da capacidade, sejam redundantes, seguros e com métodos para monitorar a integridade dos pacotes ao longo do tempo.

Também é fundamental implementar interfaces e APIs[5] para facilitar a interoperabilidades dos Pacotes de Informação para Disseminação (DIPs) gerados a partir dos *AIPs*, integrando funções para monitorar as mudanças em tecnologias e práticas de usuário para garantir a preservação contínua dos ativos digitais.

8.2 METADADOS E PROVENIÊNCIA

A ISO 16363 coloca grande ênfase na rastreabilidade e na documentação de objetos digitais. O Tainacan deve ser capaz de capturar, gerenciar e preservar, todas as categorias de metadados que registram o histórico de alterações, acessos e contexto dos objetos digitais. Essa gestão garante que as informações sejam tão completas quanto possível para que todo o conjunto que está sendo preservado, seja compreendido ao longo do tempo.

8.3 INTEROPERABILIDADE

O Tainacan já possui um protocolo OAI-PMH (Protocolo para Coleta de Metadados) implementado. É necessário aprimorar a comunicação com outros

[5] Recurso de programação que permite a interação entre diferentes *softwares* de maneira padronizada.

sistemas, caso o repositório necessite fazer, por exemplo, uma preservação compartilhada.

8.4 SEGURANÇA E ACESSO

Mecanismos de segurança aprimorados são necessários para garantir a autenticidade e a integridade dos objetos digitais armazenados. As estratégias de segurança devem incluir autenticação multifatorial e políticas rigorosas de controle de acesso para proteger os AIPs. Relatórios para auditoria são componente principal nesse item, fornecendo um histórico imutável de todas as interações com o sistema.

8.5 AUDITORIAS

O Tainacan deve implementar um sistema para auditorias internas e externas como operação contínua, para manter a integridade dos dados e a segurança do sistema. Embasada em algoritmos criptografados e com a capacidade de produzir relatórios detalhados sobre o estado do sistema, cada transação, seja ela de acesso, leitura ou gravação, deve ser registrada e auditada seguindo políticas estritas. Periodicamente, o sistema deve permitir realizar análises de riscos para identificar vulnerabilidades.

A auditoria externa, por sua vez, oferece uma avaliação imparcial da conformidade do sistema com padrões internacionais. Este processo, preferencialmente conduzido por terceiros independentes, enfatiza a transparência para que os resultados destas avaliações possam ser publicamente acessíveis, satisfazendo a responsabilização pública e reforçando a confiança no sistema para a comunidade alvo. As recomendações provenientes de auditorias externas servem como um roteiro para melhorias contínuas, a serem implementadas de forma sistemática.

Para desenvolver as capacidades de gerenciamento dos pacotes, segurança, auditoria e transparência, é necessário desenvolver um módulo ou extensão especializada dentro do Tainacan para lidar com essas necessidades, agregando metadados apropriados e garantindo a integridade dos dados ao longo do tempo. Este módulo servirá como um sistema de acompanhamento, monitorando constantemente a integridade e segurança dos dados, ao mesmo tempo que oferece mecanismos para

a verificação objetiva e aprimoramento contínuo de toda a iniciativa do repositório digital confiável.

8.6 CONSIDERAÇÕES SOBRE A CONFORMIDADE DO TAINACAN

A avaliação do sistema provou como correta a hipótese de o software Tainacan não possuir os requisitos necessários para fazer parte de um repositório digital confiável.

Entretanto, apesar de não ter sido desenvolvido em função da necessidade da preservação digital confiável, o Tainacan possui em sua estrutura nativa elementos que atendem alguns itens da norma, conforme o quadro 6:

Quadro 6 – Indicação das conformidades do Tainacan

ITEM		CONFORMIDADE
1	4.1.3 O repositório deve possuir especificações adequadas que permitam o reconhecimento e análise dos SIPs.	Não possui qualquer gestão de pacotes de informação
2	4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais.	Atende em parte com seu sistema nativo de acesso, possibilidade de autenticação em dois fatores e/ou conexão com outros validadores de acesso como assinaturas digitais, mas carece de um registro detalhado dessas ações.
3	4.1.5 O repositório deve ter um processo de *ingest*ão que verifique cada SIP quanto à integridade e exatidão.	Não possui qualquer gestão de pacotes de informação
4	4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.	Não possui qualquer gestão de pacotes de informação
5	4.1.7 O repositório deve fornecer ao produtor/depositante respostas apropriadas em pontos acordados durante os processos de *ingest*ão	Não possui qualquer gestão de pacotes de informação
6	4.1.8 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para aquisição de conteúdo.	Não possui qualquer gestão de pacotes de informação
7	4.2.3.1 O repositório deve seguir procedimentos documentados se um SIP não for incorporado a um *AIP* ou descartado e deve indicar porque o SIP não foi incorporado ou descartado.	Não possui qualquer gestão de pacotes de informação

8	4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs. 4.2.4.1 O repositório deve identificar exclusivamente cada *AIP* dentro do repositório. 4.2.4.1.1 O repositório deve possuir identificadores únicos. 4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do *AIP* e seus componentes para serem únicos dentro do contexto do repositório. 4.2.4.1.3 A documentação deve descrever quaisquer processos usados 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 duplicações. 4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e futuros previsíveis do repositório, como número de objetos.	Atende em parte, por possuir mecanismo nativo que garante a identificação única do registro (*permalink*), mas não possui qualquer gestão para garantir que não sejam alterados.
9	4.2.4.2 O repositório deve possuir um sistema de serviços de ligação/resolução confiáveis para encontrar o objeto identificado de forma única, independentemente de sua localização física.	Atende em parte, por possuir mecanismo nativo que garante a identificação única do registro, mas não possui qualquer gestão de pacotes de informação
10	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 alvo. 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.	Atende em parte, por possuir mecanismo valida o tipo de arquivo que pode entrar no repositório, mas não possui qualquer gestão de pacotes de informação
11	4.2.6.1 O repositório deve ter processos documentados para aquisição de *PDI*. 4.2.6.2 O repositório deve executar seus processos documentados para aquisição de *PDI*. 4.2.6.3 O repositório deve garantir que a *PDI* seja persistentemente associada à informação de conteúdo relevante. Designada sobre o contexto.	Atende em parte, por possuir mecanismo nativo flexível para construir/disponibilizar os metadados necessários a preservação digital, mas não possui qualquer gestão de pacotes de informação

12	4.2.7 O repositório deve assegurar que as informações de conteúdo dos AIPs sejam compreensíveis para a sua *Comunidade alvo* no momento da criação do *AIP*. 4.2.7.1 O Repositório deve ter um processo documentado para testar a compreensão para suas Comunidades alvo 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 informação de conteúdo dos AIPs. 4.2.7.3 O repositório deve trazer as Informações de Conteúdo do *AIP* para o nível exigido de compreensão se falhar no teste de compreensão.	Não possui qualquer gestão de pacotes de informação
13	4.2.8 O repositório deve verificar se cada *AIP* está completo e correto quando é criado.	Não possui qualquer gestão de pacotes de informação
14	4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção/conteúdo do repositório.	Não possui mecanismo que possibilite essa auditoria interna ou externa
15	4.2.10 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para a criação da *AIP*.	Não possui qualquer gestão de pacotes de informação
16	4.3.2 O repositório deve possuir mecanismos de monitoramento de seu ambiente de preservação.	Não possui mecanismo que possibilite essa auditoria interna ou externa
17	4.3.2.1 O repositório deve ter mecanismos para monitorar e notificar quando a Informação de Representação for inadequada para a Comunidade alvo entender os acervos de dados.	Não possui mecanismo que possibilite essa verificação
18	4.3.3.1 O repositório deve possuir mecanismos para criar, identificar ou coletar qualquer Informação de Representação extra necessária.	Atende em parte por possuir mecanismo nativo que facilita a integração de novos metadados ao fluxo de publicação
19	4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.	Não possui mecanismo que possibilite essa verificação
20	4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs.	Não possui qualquer gestão de pacotes de informação
21	4.4.2.2 O repositório deve ser capaz de demonstrar que quaisquer ações realizadas nos AIPs estavam conforme a especificação dessas ações.	Não possui qualquer gestão de pacotes de informação
22	4.5.1 O repositório deve especificar os requisitos mínimos de informação para permitir que a Comunidade alvo descubra e identifique o material de interesse.	Atende plenamente com seu sistema nativo de recuperação das informações
23	4.5.3 O repositório deve manter ligação bidirecional entre cada *AIP* e suas informações descritivas.	Não possui qualquer gestão de pacotes de informação

24	4.5.3.1 O repositório deve manter as associações entre seus *AIPs* e suas informações descritivas ao longo do tempo.	Não possui qualquer gestão de pacotes de informação
25	4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias de gerenciamento de acesso.	Atende em parte, com *plugins* externos é possível fazer registro das falhas, mas carece de integração para gerar relatório de auditoria

Fonte: Elaborada pelo autor, 2023.

A análise do Tainacan em relação aos tópicos listados revela aspectos específicos do desempenho da ferramenta:

1. Reconhecimento e Análise de SIPs (4.1.3): O repositório não possui gestão de pacotes de informação, o que indica uma lacuna na capacidade de reconhecer e analisar SIPs.

2. Verificação da Identidade do Produtor (4.1.4): O repositório atende parcialmente este critério através de sistemas de acesso, autenticação em dois fatores e conexões com validadores de acesso. Entretanto, carece de um registro detalhado dessas ações.

3. Integridade e Exatidão dos SIPs (4.1.5, 4.1.6, 4.1.7, 4.1.8): O repositório não apresenta gestão de pacotes de informação para verificar a integridade e exatidão dos SIPs, nem possui controle suficiente sobre os Objetos Digitais, além de não fornecer respostas apropriadas durante a ingestão e não conter registros de processos de administração relevantes.

4. Gestão de AIPs (4.2.3.1 a 4.2.9): Há uma ausência de gestão de pacotes de informação para tratar de AIPs incluindo a falta de procedimentos para SIPs não incorporados, inexistência de mecanismos para verificar a integridade da coleção e a não realização de testes de compreensão para as Comunidades alvo.

5. Identificação Única e Persistente de AIPs (4.2.4 a 4.2.4.1.5): O repositório atende em parte a estes critérios, com um sistema para identificação única, mas não assegura a gestão para manter os identificadores inalterados e não verifica duplicidades.

6. Ferramentas e Recursos para Informações de Representação (4.2.5, 4.2.6.1 a 4.2.6.3): O repositório atende parcialmente, validando tipos de arquivos e permitindo a construção de metadados, mas sem gestão adequada de pacotes de informação.

7. Compreensibilidade de Informações de Conteúdo (4.2.7): Não há gestão de pacotes de informação para assegurar a compreensibilidade das informações de conteúdo.

8. Monitoramento e Eficácia das Atividades de Preservação (4.3.2, 4.3.3.1, 4.3.4, 4.4.1.2, 4.4.2.2): O repositório carece de mecanismos para monitoramento e verificação da eficácia das atividades de preservação, embora atenda em parte na criação e coleta de Informações de Representação adicionais.

9. Requisitos de Informação e Ligação Bidirecional (4.5.1, 4.5.3, 4.5.3.1): O repositório atende plenamente aos requisitos mínimos de informação para descoberta e identificação de materiais, mas não mantém uma gestão de pacotes de informação para associação entre AIPs e informações descritivas.

10. Registro e Revisão de Falhas de Gerenciamento de Acesso (4.6.1.1): Atende parcialmente, com possibilidade de registro de falhas por meio de *plugins* externos, mas sem integração adequada para auditoria. No quadro 7 tem-se as quantidades:

Quadro 7 – Quantitativos da análise do Tainacan

CONFORMIDADE	QUANTIDADE
Atende em parte com seu sistema nativo de acesso, possibilidade de autenticação em dois fatores e/ou conexão com outros validadores de acesso como assinaturas digitais, mas carece de um registro detalhado dessas ações.	1
Atende em parte por possuir mecanismo nativo que facilita a integração de novos metadados ao fluxo de publicação	1
Atende em parte, com *plugins* externos é possível fazer registro das falhas, mas carece de integração para gerar relatório de auditoria	1
Atende em parte, por possuir mecanismo nativo flexível para construir/disponibilizar os metadados necessários a preservação digital, mas não possui qualquer gestão de pacotes de informação	3

Atende em parte, por possuir mecanismo nativo que garante a identificação única do registro (*permalink*), mas não possui qualquer gestão para garantir que não sejam alterados.	8
Atende em parte, por possuir mecanismo nativo que garante a identificação única do registro, mas não possui qualquer gestão de pacotes de informação	1
Atende em parte, por possuir mecanismo valida o tipo de arquivo que pode entrar no repositório, mas não possui qualquer gestão de pacotes de informação	5
Atende plenamente com seu sistema nativo de recuperação das informações	1
Não possui mecanismo que possibilite essa auditoria interna ou externa	2
Não possui mecanismo que possibilite essa verificação	2
Não possui qualquer gestão de pacotes de informação	16

Fonte: Elaborada pelo autor, 2023.

Esta análise evidencia que os requisitos propostos nesta pesquisa, podem apontar conformidades e não conformidades em avaliações de software de repositórios digitais. Ela mostrou que, embora o Tainacan atenda a alguns critérios de gestão de informação digital conforme a ISO 16363, há várias áreas significativas nas quais ele não possui a gestão necessária de pacotes de informação ou processos adequados, impactando sua eficácia geral na preservação digital.

9 CONCLUSÃO

A evolução da ciência e da tecnologia serve como alicerce fundamental para o progresso socioeconômico de uma nação. A transformação do panorama da produção intelectual, instigada pelo advento e pela difusão em larga escala da rede mundial de computadores, permeia contextos anteriormente inacessíveis. Este acesso democratizado a dados e informações científicas avançou de maneira vertiginosa, acarretando, concomitantemente, uma elevada sensibilidade quanto à necessidade de estratégias eficazes para a conservação e a manutenção desses ativos informacionais.

A relevância da preservação digital no cenário contemporâneo é inegável, ainda mais diante do volume crescente de documentos digitais criados. A ISO 16363 vem como norma internacional alinhando as necessidades de auditoria e certificação para repositórios digitais. Segundo Santos e Flores (2020), a norma oferece uma base multidimensional para avaliar a confiabilidade de repositórios digitais, incluindo critérios de infraestrutura organizacional, gestão do objeto digital e segurança da informação. O padrão contribui para o aumento da confiança dos usuários e da comunidade alvo no repositório e seu conteúdo, o que fomenta maior adoção e credibilidade dos sistemas de preservação digital (Bodero Poveda, Giusti e Morales Alarcón, 2021).

Repositórios digitais, conforme a ISO 16363, fornecem não apenas um armazenamento seguro, mas também um ecossistema propício para a gestão eficaz de objetos digitais e seus metadados. Seus requisitos potencializam a interoperabilidade entre diferentes repositórios, permitindo a troca de objetos digitais e metadados, promovendo maior colaboração e compartilhamento de recursos (Santos e Flores, 2020). Esse cenário contribui para uma infraestrutura de preservação digital mais concreta e segura, garantindo a preservação de longo prazo.

Ao se propor requisitos mínimos para gestão de pacotes de informação no software de repositório digital, tem-se um caminho para a melhoria contínua dos processos e sistemas de preservação digital. O software que tenha esses requisitos implementados, possibilita aos repositórios aderirem às melhores práticas estabelecidas pela ISO 16363, para avaliar e refinar continuamente suas operações, tanto de forma autônoma quanto por meio de certificadores externos.

Ressalta-se que, a aplicabilidade desses requisitos no contexto da preservação digital é multifacetada. Primeiramente, para os desenvolvedores de software, eles servem como um roteiro detalhado que orienta o processo de criação e manutenção de sistemas para a guarda de longo prazo. Estes requisitos funcionam guiando o desenvolvimento de funcionalidades essenciais, como a integridade dos dados, a gestão eficiente de metadados, a interoperabilidade e a segurança. Ao aderirem a esses requisitos, os desenvolvedores podem assegurar que seus produtos não apenas atendam às necessidades atuais dos usuários, mas também estejam preparados para os desafios futuros da preservação digital.

Para as instituições encarregadas da preservação digital, os requisitos de software definidos desempenham um papel importante na seleção de ferramentas e plataformas adequadas. Eles fornecem um critério objetivo para avaliar diferentes soluções de software, garantindo que a escolha final esteja alinhada com as melhores práticas da área e com as necessidades específicas da instituição.

Para gestores e tomadores de decisão, que podem não ter conhecimento especializado em certificação de preservação digital, a clareza nos requisitos de software oferece uma base sólida para entender as implicações de diversas opções tecnológicas. Isso tende a permitir que gestores façam escolhas informadas e responsáveis, mesmo sem um conhecimento técnico profundo na área.

Nesse contexto de importância da preservação digital e padronização dos softwares de repositórios digitais, a prova de conceito envolvendo o Tainacan, um software livre de produção nacional, exemplificou essa importância, onde apesar de não estar conforme a norma analisada, mostrou-se uma ferramenta flexível para adaptação a diferentes tipos de acervos, aprimoramento da transparência, melhoria dos conjuntos de metadados, entre outras. Entretanto, torná-lo compatível com os preceitos do modelo OAIS e da norma ISO 16363 são fatores fundamentais para sua eficácia como um sistema de preservação digital. O papel do software, como o Tainacan, na adequação às diretrizes da norma ressalta a necessidade de uma análise minuciosa dos componentes tecnológicos que integram o ecossistema de preservação digital.

Esta pesquisa cumpriu seu objetivo ao propor requisitos de gestão de objetos digitais, para estudos e construção de software de gestão de objetos digitais em

ambientes confiáveis de preservação digital, sob os critérios da ISO 16363. A análise permitiu delimitar os critérios que devem ser atendidos pelo software, propor recomendações e parâmetros de uso, e analisar a conformidade do Tainacan diante dos itens da norma, cumprindo-se os objetivos específicos.

A pesquisa também obteve êxito ao validar os pressupostos, demonstrando que: a norma ISO 16363 possui critérios específicos para determinar como o software de repositório digital deve automatizar rotinas no ambiente de preservação; Foi possível estabelecer requisitos de gestão de objetos digitais, a partir da ISO 16363, destacando o papel do software no processo.

Ao se definir requisitos de gestão de objetos digitais em software para repositórios digitais, percebe-se a possibilidade de se construir sistemas que atendam as necessidades de um repositório digital confiável. Dessa maneira, aprimorar o Tainacan para um sistema de repositórios digitais confiáveis configura uma tarefa acadêmica e profissional de alta relevância. Esta meta é amplamente incentivada pela necessidade crescente de métodos eficientes de preservação confiável e acesso a informações digitais em bibliotecas, museus, arquivos e quaisquer outras unidades de informação. Sua adequação aos rigorosos padrões da ISO 16363 e do modelo de referência OAIS serve como um paradigma para o desenvolvimento de sistemas confiáveis, e sua implementação oferece potenciais benefícios significativos para a comunidade científica.

A pesquisa mostrou que são vários os requisitos necessários para o Tainacan para atender as normas de preservação. É necessário desenvolver uma nova arquitetura no software para executar a gestão e interoperabilidade dos pacotes de informação. O sistema precisa mudar seus mecanismos para prover a comunidade alvo de informações para auditoria e certificação. O cumprimento rigoroso desses critérios da ISO 16363 permitirá uma avaliação transparente, por meio de recursos como registros e logs de atividades, oferecendo rastreabilidade dos objetos digitais.

A gestão de metadados é outro ponto importante para dar base às estratégias de preservação a longo prazo. O Tainacan deve desenvolver funcionalidades que assegurem a integridade, validação e agregação de metadados administrativos, metadados de gestão e metadados de preservação e quaisquer outros necessários para compor os pacotes de informação.

É necessário ainda implementar uma melhor segurança dos dados. Neste sentido, a incorporação de mecanismos como criptografia dos pacotes e/ou arquivos, é fundamental para a integridade e segurança dos objetos digitais armazenados. Adicionalmente, o sistema deve ser capaz de detectar e alertar para quaisquer alterações não autorizadas, outra exigência da ISO 16363.

A flexibilidade de desenvolvimento do sistema dá ao Tainacan a possibilidade de ser um sistema de monitoramento contínuo que avalia o estado dos objetos digitais e das tecnologias necessárias para acessá-los. Podendo ser uma solução completa para o planejamento da preservação cultural da instituição. Esse planejamento assegurará que o repositório possa responder proativamente às mudanças, não só do ambiente tecnológico, mas também dos outros aspectos previstos na norma.

Além das diretrizes técnicas, vale ressaltar que o envolvimento da comunidade alvo é vital para o sucesso do projeto. Consultas públicas, revisões especializadas e testes de usabilidade podem oferecer informações valiosas para o desenvolvimento do sistema. Dada a importância do Tainacan, o engajamento com seus usuários finais não é essencial.

É importante também considerar a sustentabilidade do projeto. Estratégias de financiamento, bem como planos para atualizações e manutenção constantes, devem ser parte integral do repositório. Sem uma visão de longo prazo, mesmo os sistemas mais bem desenhados podem se tornar obsoletos ou inviáveis.

A adequação do Tainacan, bem como de qualquer software para repositório digital, aos padrões da ISO 16363 e do modelo OAIS tem o potencial de revolucionar a forma como as informações digitais são preservadas e acessadas na comunidade científica.

É pertinente dizer que esse estudo permitiu visualizar a possibilidade de expandir o Tainacan para além das responsabilidades de apenas gerir os objetos digitais no ambiente confiável de preservação digital, mas também, dele ser um sistema amplo de gestão de todo o repositório digital confiável. Seguindo os requisitos da ISO 16363, há a possibilidade de desenvolver módulos de gestão para cada seção da norma permitindo, ainda mais, o controle, gestão e transparência do ambiente de preservação, principalmente para instituições menores que não tenham recursos

financeiros ou de pessoal, mas precisam se preocupar com a integridade do seu acervo digital ao longo do tempo.

A materialização deste projeto colocaria o Tainacan na vanguarda dos sistemas de repositório digital confiável, estabelecendo um novo padrão de excelência e confiabilidade em preservação digital. A pesquisa para essa expansão poderá ser tratada em uma tese de doutorado e, além de ampliar consideravelmente o alcance e a aplicabilidade do Tainacan, poderá oferecer requisitos valiosos para desenvolvedores, pesquisadores, acadêmicos e instituições interessadas em garantir a preservação eficaz, o acesso a dados e objetos digitais ao longo do tempo em seus ambientes digitais seguros de preservação.

Por fim, entende-se que a definição precisa de requisitos de software na preservação digital é um elemento chave que beneficia todos os envolvidos no processo, desde os desenvolvedores até os gestores e os usuários finais das informações preservadas. Esta dissertação reforça a ideia de que a clareza nos requisitos não é apenas uma prática técnica, mas uma estratégia essencial que permeia todas as facetas da preservação digital, contribuindo significativamente para a sustentabilidade e acessibilidade do patrimônio digital para as gerações futuras.

REFERÊNCIAS

ANDREW, Theo. **Intellectual Property and Electronic Theses**. Report. [*S. l.*]: JISC Legal Information Services, set. 2004. Disponível em: https://era.ed.ac.uk/handle/1842/612. Acesso em: 19 mar. 2023.

ARAÚJO, Carlos Alberto Ávila. O que é Ciência da Informação? **Informação & informação**, v. 19, n. 1, p. 01–30, 2014. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/15958. Acesso em: 19 mar. 2023.

BARROS, Diego Bil Silva; FERRER, Igor Dias; MAIA, Cleusa Maria de Souza. Auditoria de repositórios digitais preserváveis. **Revista Ibero-Americana de Ciência da Informação**, v. 11, n. 1, p. 300–313, 1 fev. 2018. Disponível em: https://doi.org/10.26512/rici.v11.n1.2018.8572. Acesso em: 22 mar. 2023.

BODERO POVEDA, Elba; DE GIUSTI, Marisa; MORALES ALARCÓN, Cristian. La preservación digital a largo plazo y las bases de la planificación estratégica. **3C TIC: Cuadernos de desarrollo aplicados a las TIC**, v. 10, n. 3, p. 17–39, 29 set. 2021. Disponível em: https://doi.org/10.17993/3ctic.2021.103.17-39. Acesso em: 07 abr. 2023.

BODERO POVEDA, Elba María; DE GIUSTI, Marisa Raquel; MORALES, Cristian. Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica. **Revista Interamericana de Bibliotecología**, v. 45, 2022. Disponível em: https://revistas.udea.edu.co/index.php/RIB/article/view/344178. Acesso em: 12 fev. 2023.

BRAGA, Tiago Emmanuel Nunes; HOLANDA, Alex Pereira; PIGNATARO, Tatiana Canelhas. Resolução RDC-Arq Conarq: uma análise dos novos requisitos informacionais propostos. **Revista Brasileira de Preservação Digital**, v. 3, p. e022004–e022004, 12 jul. 2022. Disponível em: https://doi.org/10.20396/rebpred.v3i00.16583. Acesso em: 05 abr. 2023.

CAMARGO, L. S. A.; VIDOTTI, S. B. G. Uma estratégia de avaliação em repositórios digitais. **Repositório FEBAB**, 2008. Disponível em: http://repositorio.febab.org.br/items/show/4158 . Acesso em: 1 abr. 2022.

CCSDS. **Reference Model for an Open Archival Information System (OAIS)**. 2012. 135 f. NASA, Washington DC, 2012. Disponível em: https://public.ccsds.org/Pubs/650x0m2.pdf. Acesso em: 12 out. 2022.

CONARQ. (Brasil). **Resolução nº 43: Diretrizes para implementação de repositórios arquivísticos digitais confiáveis - RDC-Arq**. [*S. l.*]: Ministério da Justiça, 2015. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-43-de-04-de-setembro-de-2015. Acesso em: 12 abr. 2022.

CORDA, María Cecilia; VIÑAS, Mariela; VALLEFÍN, Camila. Preservar la producción académica digital para el futuro. **Informatio. Revista del Instituto de Información de la Facultad de Información y Comunicación**, v. 25, n. 2, p. 41–61, 14 dez. 2020. Disponível em: https://doi.org/10.35643/Info.25.2.2. Acesso em: 09 maio 2022.

CRUZ MUNDET, José Ramón; CARRERA, Carmen Díez. Sistema de Información de Archivo Abierto (OAIS): luces y sombras de un modelo de referencia. **Investigación Bibliotecológica: archivonomía, bibliotecología e información**, v. 30, n. 70, p. 221–247, 24 out. 2016. Disponível em: https://doi.org/10.1016/j.ibbai.2016.10.010. Acesso em: 23 jun. 2022.

DURANTI, Luciana. La Conservación a largo plazo de documentos electrónicos auténticos: hallazgos del Proyecto InterPARES. [S. l.]: **Ayuntamiento de Cartagena**, 2005.

FEITOSA, A. C. A.; OLIVEIRA, A. A. A difusão digital nos museus Ibram: a implantação do Projeto Tainacan. **Revista Eletrônica Ventilando Acervos, especial (1)**, p. 70–90, 2021. Disponível em: https://ventilandoacervos.museus.gov.br/wp-content/uploads/2021/08/A5-Amanda-de-Almeida.pdf. Acesso em 18 jul. 2022.

FLORES, Daniel; ROCCO, Brenda; SANTOS, Henrique. Cadeia de custódia para documentos arquivísticos digitais. **Acervo**, v. 29, 23 maio 2019. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/717. Acesso em 22 out. 2023.

GIESECKE, Joan. Institutional Repositories: Keys to Success. **Journal of Library Administration**, v. 51, n. 5–6, p. 529–542, jul. 2011. Disponível em: https://doi.org/10.1080/01930826.2011.589340. Acesso em: 12 jan. 2023.

GIUSTI, Marisa Raquel De; VILLARREAL, Gonzalo Luján. Revisão de diferentes implementações para a preservação digital: para uma proposta metodológica de preservação e auditoria de confiança de RI. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 16, n. 2, p. 273–292, 19 abr. 2018. Disponível em: https://doi.org/10.20396/rdbci.v16i2.8651589. Acesso em 15 abr. 2022.

GIUSTI, Marisa Raquel De. **Una metodología de evaluación de repositorios digitales para asegurar la preservación en el tiempo y el acceso a los contenidos**. 2014. Tese de Doutorado. Universidad Nacional de La Plata. Disponível em: http://sedici.unlp.edu.ar/handle/10915/43157. Acesso em: 14 jun. 2022.

INNARELLI, Humberto Celeste. Preservação digital: a influência da gestão dos documentos digitais na preservação da informação e da cultura. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 9, n. 1, p. 72–87, 25 fev. 2011. Disponível em: https://doi.org/10.20396/rdbci.v8i2.1934. Acesso em: 25 jul. 2022.

LEHMKUHL, Camila Schwinden; MACEDO, D. D. J. D.; SILVA, E. Uma Análise Qualitativa dos Repositórios Digitais Arquivísticos Confiáveis (RDC-Arq). **Semantic Scholar**, 2018. Disponível em: https://www.semanticscholar.org/paper/UMA-AN%C3%81LISE-QUALITATIVA-DOS-REPOSIT%C3%93RIOS-DIGITAIS-Lehmkuhl-Macedo/a1aaae1aadd0f5892f038ea7671f5a99c5a84a1b. Acesso em: 15 abr. 2022.

MÁRDERO ARELLANO, Miguel Ángel. **Critérios para a preservação digital da informação científica**. 2008. Disponível em: https://repositorio.unb.br/handle/10482/1518. Acesso em: 14 jun. 2022.

MARTINS, Luciana Conrado; MARTINS, Dalton Lopes. Experimentações sociotécnicas para organização e difusão de coleções digitais universitárias: o caso do projeto Tainacan. **Revista CPC**, v. 15, n. 30esp, p. 34–61, 21 dez. 2020. Disponível em: https://doi.org/10.11606/issn.1980-4466.v15i30espp34-61. Acesso em: 08 ago. 2023.

OCHOA-GUTIÉRREZ, Jaider; GIRALDO, Reinaldo Andrés Sáenz; TAMAYO, Tatiana Tirado. Experiencias de gestión de los procesos de preservación digital a partir del modelo OAIS en repositorios institucionales. **Anales de Documentación**, v. 24, n. 1, 16 mar. 2021. DOI 10.6018/analesdoc.428141. Disponível em: https://revistas.um.es/analesdoc/article/view/428141. Acesso em: 24 maio 2022.

OCLC, Working Group. Trusted Digital Repositories: Attributes and Responsibilities. 1 ago. **Research Libraries Group, 2002**. Disponível em: https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf. Acesso em: 19 jun. 2022.

OLIVEIRA, Luis Felipe Rosa de; MARTINS, Dalton Lopes. Fundação Nacional de Arte: estudo de caso da migração e publicação dos dados do acervo digital com o software livre Tainacan. **Repositório Institucional da UnB**, 2019. Disponível em: https://repositorio.unb.br/handle/10482/35798. Acesso em: 21 mar. 2023.

OTLET, P. **El Tratado De Documentacion**. [*S. l.*]: MURCIA, 2004. Disponível em: https://books.google.com.br/books?id=SSWcnZGLH0gC. Acesso em: 27 ago. 2023.

PEDROSO IZQUIERDO, Evelyn. Breve historia del desarrollo de la Ciencia de la Información. **ACIMED**, v. 12, n. 2, p. 1–1, abr. 2004. Disponível em: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200007. Acesso em: 13 out. 2022.

Perens, B. The Open Source Definition. In: DiBona, S. Ockman, & M. Stone (Eds.), Open Sources: **Voices from the Open Source Revolution**. Sebastopol: O'Reilly Media, 1999.

RIBEIRO, Claudio José Silva. Modelo de Maturidade para Repositórios Digitais: um caminho para sua adoção na gestão de dados de pesquisa. **Liinc em Revista**, v. 15,

n. 2, 11 dez. 2019. DOI 10.18617/liinc.v15i2.4816. Disponível em: https://revista.ibict.br/liinc/article/view/4816. Acesso em: 3 jan. 2023.

RLG/NARA. **Trustworthy repositories audit & certification**. [*S. l.*]: OCLC, 2007.

ROCHA, Vânia Melo da. Benefícios e desafios da preservação digital: uma análise para a gestão de um repositório digital confiável. **UNIRIO**, 2016. Disponível em: http://www.repositorio-bc.unirio.br:8080/xmlui/handle/unirio/11140. Acesso em: 30 jun. 2022.

SANTOS, Henrique Machado dos. Auditoria de repositórios arquivísticos digitais confiáveis: uma análise das normas ISO 14721 e ISO 16363. **Manancial**, 2018. Disponível em: http://repositorio.ufsm.br/handle/1/15909. Acesso em: 8 ago. 2022.

SANTOS, Henrique Machado dos; FLORES, Daniel. Infraestrutura organizacional necessária ao repositório arquivístico digital confiável: um diálogo com a ISO 16363. **Revista Brasileira de Biblioteconomia e Documentação**, v. 16, n. 0, p. 1–29, 17 jan. 2020. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/1305. Acesso em 17 mar. 2022.

SANTOS, Henrique Machado dos; FLORES, Daniel. Interoperabilidade entre repositórios arquivísticos digitais confiáveis. **ÁGORA**: Arquivologia em debate, [S. l.], v. 30, n. 60, p. 213–234, 2019. Disponível em: https://agora.emnuvens.com.br/ra/article/view/879. Acesso em: 17 jun. 2023.

SANTOS JUNIOR, Ernani Rufino dos. Repositórios institucionais de acesso livre no Brasil**:** estudo Delfos. **Repositório Institucional da UnB**, 2010. Disponível em: https://repositorio.unb.br/handle/10482/5343. Acesso em: 17 set. 2022.

SARACEVIC, Tefko. A natureza interdisciplinar da ciência da informação. **Ciência da Informação**, v. 24, n. 1, 1995. DOI 10.18225/ci.inf..v24i1.608. Disponível em: https://revista.ibict.br/ciinf/article/view/608. Acesso em: 10 jan. 2023.

SERRA SERRA, Jordi. Gestión y conservación de los documentos electrónicos desde la perspectiva archivística: un nuevo escenario de actuación. 2007. [S. l.]: Universitat Jaume I (Castelló), 2007. Disponível em: http://eprints.rclis.org/11313/. Acesso em: 27 out. 2023.

SHINTAKU, Milton; MEIRELLES, Rodrigo França. **Manual do DSpace: administração de repositórios**. [*S. l.*]: EDUFBA, 2010. Disponível em: https://repositorio.ufba.br/handle/ri/769. Acesso em: 20 set. 2022.

SHINTAKU, Milton; VIDOTTI, Silvana Aparecida Borsetti Gregorio. Bibliotecas e repositórios no processo de publicação digital. **BIBLOS**, v. 30, n. 1, p. 61–80, 14 nov. 2016. Disponível em: https://repositorio.furg.br/handle/1/7042. Acesso em: 23 set. 2023.

SHINTAKU, Milton; SEABRA JUNIOR, Rui Ferreira. Abertura da ciência e os editores científicos. In: SHINTAKU, Milton; SALES, Luana Farias (Orgs.) Ciência aberta para editores científicos. Botucatu, SP: ABEC, 2019. p. 29-34. DOI: Disponível em: http://dx.doi.org/10.21452/978-85-93910-02-9.cap4S. Acesso em 14 set. 2022.

STALLMAN, Richard. **Free software, free society: Selected essays of Richard M. Stallman**. Lulu.com, 2002.

TAINACAN. *In*: Wikipédia, a enciclopédia livre. [*S. l.*: *s. n.*], 22 mar. 2023. Disponível em: https://pt.wikipedia.org/w/index.php?title=Tainacan&oldid=65541781. Acesso em: 24 mar. 2023.

VECHIATO, Fernando Luiz (Org); MARQUES, Clediane de Araujo Guedes (Org); KOSHIYAMA, Débora Costa Araújo Di Giacomo (Org); MOURA, Elisângela Alves de (Org); TORINO, Emanuelle (Org); MAIA, Maria Aniolly Queiroz (Org); MARQUES, Tércia Maria Souza de Moura (Org). **Repositórios digitais: teoria e prática**. [*S. l.*]: EDUTFPR, 2017. Disponível em: https://repositorio.ufrn.br/handle/123456789/24189. Acesso em: 19 jun. 2022.

WATERS, Donald; GARRETT, John. **Preserving Digital Information, Report of the Task Force on Archiving of Digital Information**. [*S. l.*: *s. n.*], 1996. Disponível em: https://www.clir.org/pubs/reports/pub63/. Acesso em: 30 jun. 2022.

ANEXO

Análise dos tópicos da ISO 16363

TÓPICOS	RESPONSÁVEL	AÇÃO
● 1. Introdução ○ 1.1 Objetivo e Escopo ○ 1.2 Aplicabilidade ○ 1.3 Fundamentação ○ 1.4 Estrutura deste Documento ○ 1.5 Definições ○ 1.6 Conformidade ○ 1.7 Referências	Não fez parte da pesquisa	Não fez parte da pesquisa
● 2. Visão Geral dos Critérios de Auditoria e Certificação ○ 2.1 Um Repositório Digital Confiável ○ 2.2 Evidências ○ 2.3 Normas Relevantes, Melhores Práticas e Controles	Não fez parte da pesquisa	Não fez parte da pesquisa

3. Infraestrutura organizacional		
3.1 Governança e Viabilidade Organizacional		
3.1.1 O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, retenção de longo prazo, gerenciamento e acesso à informação digital. **Exemplos:** Declaração de missão ou carta do repositório ou da sua organização-mãe que especificamente se destina ou implicitamente a preservação de informações e/ou outros recursos sob a sua finalidade; um mandato regulamentar legal, estatutário ou governamental aplicável ao repositório que aborde especifica ou implicitamente a preservação, retenção, gestão e acesso a informações e/ou outros recursos sob sua finalidade	Equipe gestora	Elaborar documentos
3.1.2 O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório terá no suporte de longo prazo de sua missão. **Exemplos:** Plano Estratégico de Preservação; atas da reunião; documentação das decisões administrativas tomadas.	Equipe gestora	Elaborar documentos
3.1.2.1 O repositório deve ter um plano de sucessão adequado, planos de contingência e/ou acordos de caução em vigor caso o repositório deixe de operar ou a instituição governante ou financiadora mude substancialmente seu escopo. **Exemplos:** Plano(s) escrito(s) de sucessão e contingência; declaração explícita e específica que documenta a intenção de garantir a continuidade do repositório, bem como as medidas tomadas e a serem tomadas para garantir a continuidade; depósito de código crítico, Software e metadados suficientes para permitir a reconstituição do repositório e seu conteúdo em caso de falha do repositório; acordos explícitos com organizações sucessoras documentando as medidas a serem tomadas para garantir a transferência completa e formal da responsabilidade pelo conteúdo digital do repositório e ativos relacionados, e concedendo os direitos necessários para garantir a continuidade dos serviços de conteúdo e repositório.	Equipe gestora	Elaborar documentos

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 caução. **Exemplos:** Políticas administrativas, procedimentos, protocolos, requisitos; orçamentos e documentos de análise financeira; calendários fiscais; plano(s) de negócios; qualquer evidência de acompanhamento ativo e preparação.	Equipe gestora	Elaborar documentos
3.1.3 O repositório deve ter uma Política de Coleta ou outro documento que especifique o tipo de informação que irá preservar, reter, gerenciar e fornecer acesso. **Exemplos de maneiras que o Repositório pode demonstrar que está a cumprir este requisito:** Política de recolha e documentos comprovativos; Política de Preservação, missão, objetivos e visão do repositório.	Equipe gestora	Elaborar documentos
3.2 Estrutura organizacional e pessoal		
3.2.1 O repositório deve ter identificado e estabelecido as funções que precisa desempenhar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir essas funções. **Não consta exemplos**	Equipe gestora	Elaborar documentos
3.2.1.1 O repositório deve ter identificado e estabelecido as funções que precisa desempenhar. **Exemplos:** Um plano de pessoal; definições de competência; descrições dos trabalhos; planos de desenvolvimento profissional do pessoal; certificados de formação e acreditação; além disso, evidências de que o repositório revisa e mantém esses documentos à medida que os requisitos evoluem.	Equipe gestora	Elaborar documentos

3.2.1.2 O repositório deve ter o número adequado de funcionários para dar suporte a todas as funções e serviços. **Exemplos:** Organogramas; definições de funções e responsabilidades; comparação dos níveis de pessoal com os padrões e padrões da indústria	Equipe gestora	Elaborar documentos
3.2.1.3 O repositório deve ter em vigor um programa ativo de desenvolvimento profissional que forneça à equipe oportunidades de desenvolvimento de habilidades e conhecimentos. **Exemplos:** Planos e relatórios de desenvolvimento profissional; requisitos de formação e orçamentos de formação, documentação das despesas de formação (montante por pessoal); objetivos de desempenho e documentação de atribuições e realizações da equipe, cópias de certificados concedidos.	Equipe gestora	Elaborar documentos
3.3 Responsabilidade processual e estrutura da política de preservação		
3.3.1 O repositório deve ter definido sua Comunidade alvo e a(s) base(s) de conhecimento associada(s) e deve ter essas definições adequadamente acessíveis. **Exemplos:** Uma definição escrita da Comunidade alvo.	Equipe gestora	Elaborar documentos
3.3.2 O repositório deve ter Políticas de Preservação em vigor para garantir que seu Plano Estratégico de Preservação seja cumprido. **Exemplos:** Políticas de preservação; Declaração de Missão de Repositório.	Equipe gestora	Elaborar documentos
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 as práticas da comunidade evoluem. **Exemplos:** Documentação escrita atual e passada sob a forma de Políticas de Preservação, Planos Estratégicos de Preservação e Planos de Implementação de Preservação,	Equipe gestora	Elaborar documentos

Procedimentos, Protocolos e Fluxos de Trabalho; especificações dos 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.		
3.3.3 O repositório deve ter um histórico documentado das mudanças em suas operações, procedimentos, Software e hardware. **Exemplos:** Inventários de equipamentos de capital; documentação da aquisição, implementação, atualização e desativação de Software e hardware de repositório crítico; agendas e políticas de retenção e descarte de arquivos, cópias de versões anteriores de políticas e procedimentos; atas de reuniões.	Equipe gestora	Elaborar documentos
3.3.4 O repositório deve comprometer-se com a transparência e responsabilidade em todas as ações de suporte à operação e gestão do repositório que afetem a preservação do conteúdo digital ao longo do tempo. **Exemplos:** Relatórios de auditorias e certificações financeiras e técnicas; divulgação de documentos de governança, revisões independentes de programas e contratos e acordos com provedores de financiamento e serviços críticos.	Equipe gestora	Elaborar documentos
3.3.5 O repositório deve definir, coletar, rastrear e fornecer adequadamente suas medições de integridade de informações. **Exemplos:** Definição escrita ou especificação das medidas de integridade do repositório (por exemplo, *checksum* computado ou valor *hash*); documentação dos procedimentos e mecanismos de monitorização das medições de integridade e de resposta aos resultados de medições de integridade que indiquem que o conteúdo digital está em risco; um processo de auditoria para coleta, rastreamento e apresentação de medições de integridade; Política de Preservação e documentação do fluxo de trabalho.	Equipe gestora	Elaborar documentos

3.3.6 O repositório deve se comprometer com um cronograma regular de autoavaliação e certificação externa. **Exemplos:** Listas de verificação preenchidas e datadas de autoavaliações e/ou auditorias de terceiros; certificados concedidos para conformidade com as normas ISO relevantes; calendários e evidências de alocações orçamentárias adequadas para futura certificação.	Equipe gestora	Elaborar documentos
3.4 Sustentabilidade financeira		
3.4.1 O repositório deve ter processos de planejamento de negócios de curto e longo prazo para sustentar o repositório ao longo do tempo. **Exemplos:** Planos estratégicos, operacionais e/ou de negócios atualizados, plurianuais; demonstrações financeiras anuais auditadas; previsões financeiras com múltiplos cenários orçamentários; planos de contingência; análise de mercado.	Equipe gestora	Elaborar documentos
3.4.2 O repositório deve ter práticas e procedimentos financeiros transparentes, conforme as normas e práticas contábeis relevantes e auditados por terceiros segundo os requisitos legais territoriais. **Exemplos:** Requisitos demonstrados de divulgação para planejamento e práticas de negócios; citações e/ou exemplos de requisitos, normas e práticas contábeis e de auditoria; demonstrações financeiras anuais auditadas.	Equipe gestora	Elaborar documentos
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). **Exemplos:** Documentos de gestão de riscos que identificam ameaças percebidas e potenciais e respostas planeadas ou implementadas (um registro de riscos); documentos de planejamento de investimentos em infraestrutura tecnológica; análises de custo/benefício; documentos e carteiras de investimento financeiro; requisitos e exemplos de licenças, contratos e gestão de ativos; evidência de revisão baseada no risco.	Equipe gestora	Elaborar documentos

3.5 contratos, licenças e responsabilidades		
3.5.1 O repositório deve ter e manter contratos apropriados ou acordos de depósito para materiais digitais que ele gerencia, preserva e/ou aos quais fornece acesso. **Exemplos:** Contratos e licenças de depósito devidamente assinados e executados conforme as leis e regulamentos locais, nacionais e internacionais; políticas sobre acordos de depósito de terceiros; definições dos níveis de serviço e utilizações permitidas; políticas de repositório sobre o tratamento de "obras órfãs" e resolução de litígios de direitos de autor; relatórios de avaliações independentes de risco dessas políticas; procedimentos para rever e manter regularmente acordos, contratos e licenças.	Equipe gestora	Elaborar documentos
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. **Exemplos:** Contratos, contratos de depósito; especificação(ões) de direitos transferidos para diferentes tipos de conteúdos digitais (se aplicável); declarações políticas sobre os direitos de preservação necessários.	Equipe gestora	Elaborar documentos
3.5.1.2 O repositório deve ter especificado todos os aspectos apropriados de aquisição, manutenção, acesso e retirada em acordos por escrito com os depositantes e outras partes relevantes. **Exemplos:** Contratos de submissão, contratos de depósito e ações de doação devidamente executados; procedimentos operacionais padrão escritos	Equipe gestora	Elaborar documentos
3.5.1.3 O repositório deve ter políticas escritas que indiquem quando ele aceita a responsabilidade pela preservação do conteúdo de cada conjunto de objetos de dados enviados. **Exemplos:** Contratos de submissão, contratos de depósito e ações de doação devidamente executados; recibo de confirmação enviado de volta ao produtor/depositante.	Equipe gestora	Elaborar documentos
3.5.1.4 O repositório deve ter políticas em vigor para lidar com responsabilidades e contestações de propriedade/direitos.	Equipe gestora	Elaborar documentos

Exemplos: Definição de direitos, licenças e permissões a obter de produtores e contribuintes de conteúdo digital; citações de leis e regulamentos relevantes; política de resposta aos desafios; histórico documentado para responder a desafios de maneiras que não inibem a preservação; registros de assessoria jurídica relevante buscados e recebidos.		
3.5.2 O repositório deve rastrear e gerenciar os direitos de propriedade intelectual e as restrições de uso do conteúdo do repositório conforme exigido pelo acordo de depósito, contrato ou licença. **Exemplos:** 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 depositante; amostras de acordos e outros documentos que especificam e abordam direitos de propriedade intelectual; documentação de monitoramento por repositório ao longo do tempo de alterações de *status* e posse da propriedade intelectual em conteúdo digital mantido pelo repositório; resultados do monitoramento, metadados que capturam informações de direitos.	Equipe gestora	Elaborar documentos
4 Gerenciamento de objetos digitais		
4.1 *Ingest* (Alimentação): Aquisição de conteúdo		
4.1.1 O repositório deve identificar a Informação de Conteúdo e as Propriedades da Informação que o repositório irá preservar. **Exemplos:** Declaração de missão; submissão de contratos/depósitos/atos de presente. Documentos da Política de Fluxo de Trabalho e Preservação, incluindo definição por escrito de propriedades mencionado no contrato de depósito/escritura de presente; procedimentos de processamento por escrito; documentação de propriedades a serem preservadas.	Equipe gestora	Elaborar documentos
4.1.1.1 O repositório deve ter procedimento(s) para identificar as Propriedades da Informação que irá preservar. **Exemplos:** Definições das Propriedades de Informação que devem ser preservadas; Contratos de submissão/depósitos, políticas de preservação, procedimentos de processamento por escrito, documentação de fluxo de trabalho.	Equipe gestora	Elaborar documentos

4.1.1.2 O repositório deverá ter um registro das Informações de Conteúdo e das Propriedades das Informações que irá preservar. **Exemplos:** Políticas de preservação, manuais de processamento, inventários ou pesquisas de coleta, registros de tipos de informações de conteúdo, estratégias de preservação adquiridas e planos de ação.	Equipe gestora	Elaborar documentos
4.1.2 O repositório deve especificar claramente as informações que precisam ser associadas às Informações de Conteúdo específicas no momento de seu depósito. **Exemplos:** Requisitos de transferência; acordos de arquivo de produtores; Planos de fluxo de trabalho para produzir o *AIP*.	Equipe gestora	Elaborar documentos
4.1.3 O repositório deve possuir especificações adequadas que permitam o reconhecimento e análise dos SIPs. **Exemplos:** Informações de embalagem para os SIPs; Informações de Representação para os Dados de Conteúdo *SIP*, incluindo especificações documentadas de formato de arquivo; padrões de dados publicados; documentação de construção de objetos válidos.	Software	Verificar e validar automaticamente os pacotes
4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais. **Exemplos:** Contratos de apresentação/depósito/escritura de presente juridicamente vinculativos, prova de medidas tecnológicas adequadas; registros de procedimentos e autenticações.	Software	Validar e autenticar o produtor
4.1.5 O repositório deve ter um processo de *ingest*ão que verifique cada *SIP* quanto à integridade e exatidão. **Exemplos:** Documentos e arquivos de log do sistema do(s) sistema(s) que executam o(s) procedimento(s) de *ingest*ão; registros ou registros de ficheiros recebidos durante o processo de transferência e *ingest*ão; documentação de procedimentos operacionais padrão, procedimentos detalhados e/ou fluxos de trabalho; formatar registros; definições de completude e correção.	Software	Verificar e validar automaticamente os pacotes
4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.	Software	Disponibilizar relatório automático com as informações dos pacotes

Exemplos: Documentos mostrando o nível de controle físico que o repositório realmente tem. Um banco de dados separado/catálogo de metadados que lista todos os objetos digitais no repositório e metadados suficientes para validar a integridade desses objetos (tamanho do arquivo, soma de verificação, *hash*, localização, número de cópias etc.)		
4.1.7 O repositório deve fornecer ao produtor/depositante respostas apropriadas em pontos acordados durante os processos de *ingest*ão **Exemplos:** Submissão de contratos/depósitos/atos de presente; documentação do fluxo de trabalho; procedimentos operacionais padrão; evidência de "relatar de volta", como relatórios, correspondência, memorandos ou e-mails.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.1.8 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para aquisição de conteúdo. **Exemplos:** Documentação escrita das decisões e/ou medidas tomadas; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes, recibos de confirmação enviados de volta aos provedores.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.2 *Ingest*: criação do *AIP*		
4.2.1 O repositório deve ter para cada *AIP* ou classe de AIPs preservados pelo repositório uma definição associada que seja adequada para análise do AIP e adequada às necessidades de preservação de longo prazo. Não constam exemplos	Equipe gestora	Disponibilizar relatório automático com as informações dos pacotes
4.2.1.1 O repositório deve ser capaz de identificar qual definição se aplica a qual AIP. **Exemplos:** Documentação que vincula claramente cada *AIP*, ou classe de AIPs, à sua definição.	Equipe gestora	Elaborar documentos
4.2.1.2 O repositório deve ter uma definição de cada *AIP* que seja adequada para preservação de longo prazo, permitindo a identificação e análise de todos os componentes necessários dentro daquele *AIP*. **Exemplos:** Demonstração do uso das definições para extrair informações de conteúdo e *PDI* (*Provenance, Access Rights, Context, Reference e Fixity Information)* dos *AIPs*. Deve-se notar	Equipe gestora	Elaborar documentos

que a proveniência de um objeto digital, por exemplo, pode ser estendida ao longo do tempo para refletir ações adicionais de preservação.		
4.2.2 O repositório deve ter uma descrição de como os AIPs são construídos a partir dos SIPs. **Exemplos:** *Process description documents*; Documentação da relação SIP-AIP; Documentação clara de como os AIPs são derivados de SIPs.	Equipe gestora	Elaborar documentos
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 porque o *SIP* não foi incorporado ou descartado. **Exemplos:** Arquivos de processamento do sistema; registros de eliminação; acordos/atos de doação de doadores ou depositantes; sistema de rastreamento de proveniência; ficheiros de registro do sistema; process *description documents;* Documentação da relação *SIP* com *AIP*; documentação clara de como os AIPs são derivados de SIPs; documentação do padrão/processo contra o qual ocorre a normalização; documentação do resultado da normalização e como o *AIP* resultante é diferente do(s) *SIP*(s).	Software	Disponibilizar relatório automático com as informações dos pacotes
4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs. **Exemplos no tópico 4.2.4.1.5**	Software	Controlar automaticamente os identificadores dos pacotes
4.2.4.1 O repositório deve identificar exclusivamente cada AIP dentro do repositório. **Exemplos no tópico 4.2.4.1.5**	Software	Controlar automaticamente os identificadores dos pacotes
4.**2.4.1.1** O repositório deve possuir identificadores únicos. **Exemplos no tópico 4.2.4.1.5**	Software	Controlar automaticamente os identificadores dos pacotes
4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do AIP e seus componentes para serem únicos dentro do contexto do repositório. **Exemplos no tópico 4.2.4.1.5**	Software	Controlar automaticamente os identificadores dos pacotes

4.2.4.1.3 A documentação deve descrever quaisquer processos usados para alterações em tais identificadores. **Exemplos no tópico 4.2.4.1.5**	Software	Controlar automaticamente os identificadores dos pacotes
4.2.4.1.4 O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais de duplicações. **Exemplos no tópico 4.2.4.1.5**	Software	Controlar automaticamente os identificadores dos pacotes
4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e futuros previsíveis do repositório, como número de objetos. **Exemplos:** Isto é necessário para garantir que cada *AIP* possa ser encontrado sem ambiguidades no futuro. Isso também é necessário para garantir que cada *AIP* possa ser distinguido de todos os outros AIPs no repositório.	Software	Controlar automaticamente os identificadores dos pacotes
4.2.4.2 O repositório deve possuir um sistema de serviços de ligação/resolução confiáveis para encontrar o objeto identificado de forma única, independentemente de sua localização física. **Exemplos:** Documentação que descreve a convenção de nomenclatura e a evidência física de sua aplicação (por exemplo, *logs*).	Software	Controlar automaticamente os identificadores dos pacotes
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. **Exemplos no tópico 4.2.5.4**	Software	Controlar automaticamente as informações de representação dos pacotes

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 alvo. **Exemplos no tópico 4.2.5.4**	Software	Controlar automaticamente as informações de representação dos pacotes
4.2.5.3 O repositório deve ter acesso às Informações de Representação necessárias. **Exemplos no tópico 4.2.5.4**	Software	Controlar automaticamente as informações de representação dos pacotes
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. **Exemplos:** Subscrição ou acesso a registros de informações de representação (incluindo registros de formato); registros visíveis em itens locais (com ligações persistentes a objetos digitais); Registros de banco de dados que incluem Informações de Representação e um link persistente para objetos digitais relevantes.	Software	Controlar automaticamente as informações de representação dos pacotes
4.2.6 O repositório deve ter processos documentados para aquisição de Informações de Descrição de Preservação (*PDI*) para suas Informações de Conteúdo associadas e adquirir *PDI* conforme os processos documentados.		
4.2.6.1 O repositório deve ter processos documentados para aquisição de *PDI*. **Exemplos no tópico 4.2.6.3**	Software	Controlar automaticamente as informações de representação dos pacotes
4.2.6.2 O repositório deve executar seus processos documentados para aquisição de *PDI*. **Exemplos no tópico 4.2.6.3**	Software	Controlar automaticamente as informações de representação dos pacotes
4.2.6.3 O repositório deve garantir que a *PDI* seja persistentemente associada à informação de conteúdo relevante. **Exemplos:** Procedimentos operacionais padrão; manuais que descrevem procedimentos de *ingest*ão; documentação visível sobre como o repositório adquire e gerencia a informação de descrição de preservação (*PDI*); Criação de *checksums* ou *digests*, consultando a *Comunidade Alvo* sobre o contexto.	Software	Controlar automaticamente as informações de representação dos pacotes

4.2.7 O repositório deve garantir que as Informações de Conteúdo dos AIPs sejam compreensíveis para sua Comunidade alvo no momento da criação do *AIP*.		
4.2.7.1 O Repositório deve ter um processo documentado para testar a compreensão para suas Comunidades alvo das Informações de Conteúdo dos AIPs em sua criação. **Exemplos no tópico 4.2.7.3**	Software	Verificar e validar automaticamente os pacotes
4.2.7.2 O repositório deve executar o processo de teste para cada classe de informação de conteúdo dos AIPs. **Exemplos no tópico 4.2.7.3**	Software	Verificar e validar automaticamente os pacotes
4.2.7.3 O repositório deve trazer as Informações de Conteúdo do *AIP* para o nível exigido de compreensão se falhar no teste de compreensão. **Exemplos:** Procedimentos de ensaio a executar contra as explorações digitais para garantir a sua compreensão perante a *Comunidade alvo* definida; registros de tais testes sendo realizados e avaliados;	Software	Verificar e validar automaticamente os pacotes
4.2.8 O repositório deve verificar se cada *AIP* está completo e correto quando é criado. **Exemplos:** Descrição do procedimento que verifica a integridade e a exatidão dos AIPs; registros do procedimento.	Software	Verificar e validar automaticamente os pacotes
4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção/conteúdo do repositório. **Exemplos:** Documentação fornecida para 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 das datas de ação associada (recepção, ação, etc.); registros de verificações periódicas.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.2.10 O repositório deve conter registros contemporâneos de ações e processos de administração relevantes para a criação da *AIP*. **Exemplos:** Documentação escrita das decisões e/ou medidas tomadas com carimbos de data e hora; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes.	Software	Disponibilizar relatório automático com as informações dos pacotes

4.3 Planejamento de preservação		
4.3.1 O repositório deve ter estratégias de preservação documentadas relevantes para seu acervo. **Exemplos:** Documentação identificando cada risco de preservação identificado e a estratégia para lidar com esse risco.	Equipe gestora	Elaborar documentos
4.3.2 O repositório deve possuir mecanismos de monitoramento de seu ambiente de preservação. **Exemplos:** Questionamentos da Comunidade alvo do repositório.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.3.2.1 O repositório deve ter mecanismos para monitorar e notificar quando a Informação de Representação for inadequada para a Comunidade alvo entender os acervos de dados. **Exemplos:** Assinatura de um serviço de registro de informação de representação; assinatura de um serviço de vigilância tecnológica, pesquisas entre seus membros da Comunidade Designados, processos de trabalho relevantes para lidar com essas informações.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.3.3 O repositório deve possuir mecanismos para alterar seus planos de preservação em decorrência de suas atividades de monitoramento. Exemplos: Planos de preservação ligados a vigilância tecnológica formal ou informal; planejamento ou processos de preservação temporizados para intervalos mais curtos (por exemplo, não mais de cinco anos); comprovação de atualizações frequentes de políticas de preservação e planos de preservação; seções de políticas de preservação que abordam como os planos podem ser atualizados e que abordam com que frequência os planos são necessários para serem revisados e reafirmados ou atualizados.	Equipe gestora	Elaborar documentos
4.3.3.1 O repositório deve possuir mecanismos para criar, identificar ou coletar qualquer Informação de Representação extra necessária. **Exemplos:** Assinatura de um serviço de registro de formato; assinatura de um serviço de relógio de tecnologia; planos de preservação.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.	Software	Disponibilizar relatório automático com as informações dos pacotes

Exemplos: Coleta de metadados de preservação adequados; prova de usabilidade de objetos digitais selecionados aleatoriamente mantidos dentro do sistema; registro demonstrável para manter objetos digitais utilizáveis ao longo do tempo; Sondagens comunitárias designadas.		
4.4 Preservação de *AIP*		
4.4.1 O repositório deve ter especificações de como os AIPs são armazenados até o nível de bit. **Exemplos:** Documentação do formato de AIPs; Descrição da linguagem de especificação de dicionário de entidades de dados e de LESTE (DEDSL) dos componentes de dados (ver referências [B6] e [B7]).	Equipe gestora	Elaborar documentos
4.4.1.1 O repositório deve preservar as Informações de Conteúdo dos AIPs. **Exemplos:** Documentação do procedimento de fluxo de trabalho de preservação; documentação do procedimento de fluxo de trabalho; Documentos de Política de Preservação que especificam o tratamento de *AIPs* e em que circunstâncias podem ser excluídos; Capacidade de demonstrar a sequência de conversões para um *AIP* para qualquer objeto digital ou grupo de objetos ingeridos; Documentação que vincula objetos ingeridos e os AIPs atuais.	Equipe gestora	Elaborar documentos
4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs. **Exemplos:** Informações de fixidade (por exemplo, *checksums*) para cada objeto digital ingerido/*AIP*; registros de verificações de fixação; Documentação de como as informações de AIPs e fixidez são mantidas separadas; Documentação de como os AIPs e os registros de adesão são mantidos separados.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.4.2 O repositório deve conter registros atualizados de ações e processos de administração relevantes para o armazenamento e preservação dos AIPs. **Exemplos:** Documentação escrita das decisões e/ou medidas tomadas; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes.	Equipe gestora	Elaborar documentos
4.4.2.1 O repositório deve ter procedimentos para todas as ações realizadas nos AIPs. **Exemplos:** Documentação escrita que descreve todas as ações que podem ser executadas contra um *AIP*.	Equipe gestora	Elaborar documentos

4.4.2.2 O repositório deve ser capaz de demonstrar que quaisquer ações realizadas nos AIPs estavam conforme a especificação dessas ações. **Exemplos:** 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 conforme os processos documentados.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.5 Gestão da informação		
4.5.1 O repositório deve especificar os requisitos mínimos de informação para permitir que a Comunidade alvo descubra e identifique o material de interesse. **Exemplos:** Recuperação e informação descritiva, metadados de descoberta, como o Dublin Core, e outra documentação descrevendo o objeto.	Software	Disponibilizar interface de busca
4.5.2 O repositório deve capturar ou criar informações descritivas mínimas e garantir que esteja associado ao *AIP*. **Exemplo:** Metadados descritivos; identificador ou localizador persistente, único ou persistente interno, ou externo associado ao *AIP* (consulte também 4.2.4 sobre identificador único persistente); documentação do sistema e arquitetura técnica; acordos de depositante; documentação de política de metadados, incorporando detalhes dos requisitos de metadados e uma declaração descrevendo onde a responsabilidade por sua aquisição abrange; *process workflow documentation.*	Equipe gestora	Elaborar documentos
4.5.3 O repositório deve manter ligação bidirecional entre cada *AIP* e suas informações descritivas. **Exemplos:** Metadados descritivos; identificador ou localizador único e persistente associado ao *AIP*; Relação documentada entre o *AIP* e seus metadados; documentação do sistema e arquitetura técnica; process *workflow documentation.*	Software	Controlar automaticamente as informações de representação dos pacotes
4.5.3.1 O repositório deve manter as associações entre seus AIPs e suas informações descritivas ao longo do tempo. **Exemplos:** Registro pormenorizado da manutenção ou verificação contínua da integridade dos dados e das suas relações com as informações descritivas associadas, especialmente após a reparação ou modificação do *AIP*; informações descritivas legadas; persistência de identificador	Software	Disponibilizar relatório automático com as informações dos pacotes

ou localizador; Relação documentada entre a *AIP* e suas informações descritivas; documentação do sistema e arquitetura técnica; *process workflow documentation.*		
4.6 Gerenciamento de acesso		
4.6.1 O repositório deve cumprir as Políticas de Acesso. **Exemplos:** Declarações de políticas que estão disponíveis para as comunidades de usuários; informações sobre as capacidades do usuário (matrizes de autenticação); logs e trilhas de auditoria de solicitações de acesso; testes explícitos de alguns tipos de acesso.	Equipe gestora	Elaborar documentos
4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias de gerenciamento de acesso. **Exemplos**: Logs 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.	Software	Disponibilizar relatório automático com as informações dos pacotes
4.6.2 O repositório deve seguir políticas e procedimentos que permitam a disseminação de objetos digitais que sejam rastreáveis aos originais, com evidências que comprovem sua autenticidade. **Exemplos:** Documentos de projeto do sistema; Instruções de trabalho (se as quedas envolverem processamento manual); passo a passo do processo; produção de uma cópia de amostra com prova de autenticidade; documentação dos requisitos da comunidade para prova de autenticidade.	Equipe gestora	Elaborar documentos
4.6.2.1 O repositório deve registrar e agir sobre relatórios de problemas sobre erros em dados ou respostas de usuários. **Exemplos:** Documentos de projeto do sistema; Instruções de trabalho (se as quedas envolverem processamento manual); passo a passo do processo; Registros de encomendas e produção *DIP*; documentação de relatórios de erros e as ações tomadas.	Equipe gestora	Elaborar documentos
5 Gestão de risco de infraestrutura e segurança		

5.1 Gestão de risco de infraestrutura técnica		
5.1.1 O repositório deve identificar e gerenciar os riscos às suas operações e objetivos de preservação associados à infraestrutura do sistema. **Exemplos:** 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, por exemplo, *Apache*, *iRODS*, *Fedora*); recriação de arquivos a partir de backups.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1 O repositório deve empregar relógios de tecnologia ou outros sistemas de notificação de monitoramento de tecnologia **Exemplos:** Gestão de relatórios periódicos de avaliação tecnológica. Comparação da tecnologia existente com cada nova avaliação.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.1 O repositório deve possuir tecnologias de hardware adequadas aos serviços que presta às comunidades alvo. **Exemplos:** Manutenção de tecnologia comunitária designada atualizada, expetativa e perfis de uso; fornecimento de largura de banda adequada para suportar demandas de consumo e uso; elicitação sistemática de feedback sobre adequação de hardware e serviço; manutenção de um inventário de hardware atual.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.2 O repositório deve ter procedimentos para monitorar e receber notificações quando forem necessárias mudanças na tecnologia de hardware. Exemplos: Auditorias de capacidade em comparação a uso real; auditorias de taxas de erro observadas; auditorias de gargalos de desempenho que limitam a capacidade de atender aos requisitos de acesso da comunidade de usuários; documentação de avaliações de vigilância tecnológica; documentação de atualizações de tecnologia de fornecedores	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.3 O repositório deve ter procedimentos para avaliar quando são necessárias alterações no hardware atual. Exemplos: Procedimentos de avaliação em vigor; experiência documentada da equipe em cada subsistema de tecnologia.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico

5.1.1.1.4 O repositório deve ter procedimentos, compromisso e financiamento para substituir hardware quando a avaliação indicar a necessidade de fazê-lo. **Exemplos:** Declaração de compromisso para fornecer níveis de serviço esperados e contratados; provas de ativos financeiros em curso destinados à aquisição de hardware; demonstração de economia de custos através do custo amortizado do novo sistema.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.5 O repositório deve possuir tecnologias de Software adequadas aos serviços que presta às comunidades alvo. **Exemplos:** Manutenção de tecnologia atualizada, expetativa e perfis de uso; fornecimento de sistemas de Software adequados para suportar as demandas de consumo e uso; elicitação sistemática de feedback sobre adequação de Software e serviço; manutenção de um inventário de Software atual.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.6 O repositório deve ter procedimentos para monitorar e receber notificações quando forem necessárias alterações de Software. **Exemplos:** Auditorias de capacidade em comparação a uso real; auditorias de taxas de erro observadas; auditorias de gargalos de desempenho que limitam a capacidade de atender aos requisitos de acesso da comunidade de usuários; documentação de avaliações de vigilância tecnológica; documentação de atualizações de Software de fornecedores.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.7 O repositório deve ter procedimentos para avaliar quando são necessárias alterações no Software atual. **Exemplos:** Procedimentos de avaliação em vigor; experiência documentada da equipe em cada subsistema de tecnologia de Software.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.1.8 O repositório deve ter procedimentos, compromisso e financiamento para substituir o Software quando a avaliação indicar a necessidade de fazê-lo. **Exemplos:** Declaração de compromisso para fornecer níveis de serviço esperados e contratados; provas de ativos financeiros em curso destinados à aquisição de Software; demonstração de economia de custos através do custo amortizado do novo sistema.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.2 O repositório deve ter suporte de *hardware* e Software adequado para funcionalidade de backup suficiente para preservar o conteúdo do repositório e rastrear as funções do repositório. **Exemplos:** Documentação do que está sendo feito backup e com que frequência; log de auditoria/inventário de backups; validação de backups concluídos; plano, política e	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico

documentação de recuperação de desastres; brocas de incêndio; testes de backups; contratos de suporte para hardware e Software para mecanismos de backup; demonstrou a preservação de metadados do sistema, como controles de acesso, localização de réplicas, trilhas de auditoria, valores de *checksum*.		
5.1.1.3 O repositório deve ter mecanismos eficazes para detectar corrupção ou perda de bits. **Exemplos:** Documentos que especificam mecanismos de deteção e correção de erros de bits utilizados; análise de risco; relatórios de erros; análise de ameaças; análise periódica da integridade dos repositórios.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.3.1 O repositório deve registrar e relatar à sua administração todos os incidentes de corrupção ou perda de dados, e medidas devem ser tomadas para reparar/substituir dados corrompidos ou perdidos. **Exemplos:** Procedimentos relacionados à comunicação de incidentes aos administradores; Registros de metadados de preservação (por exemplo, *PDI*); comparação de logs de erros com relatórios para administração; procedimentos de escalonamento relacionados à perda de dados; rastreamento de fontes de incidentes; ações de correção tomadas para remover fontes de incidentes.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
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 risco-benefício. **Exemplos:** Registro de risco (lista de todos os patches disponíveis e análise de documentação de risco); evidência de processos de atualização (por exemplo, servidor *update manager daemon*); documentação relacionada com as instalações de atualização.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.5 O repositório deve ter processos definidos para mídia de armazenamento e/ou mudança de hardware (por exemplo, atualização, migração). **Exemplos:** Documentação dos processos de migração; políticas relacionadas ao suporte, manutenção e substituição de hardware; documentação dos ciclos de vida de suporte esperados do fabricante de hardware; políticas relacionadas à migração de registros para sistemas de hardware alternativos.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.6 O repositório deve ter processos críticos identificados e documentados que afetem sua capacidade de cumprir com suas responsabilidades obrigatórias. **Exemplos:** Matriz de rastreabilidade entre processos e requisitos obrigatórios.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico

5.1.1.6.1 O repositório deve ter um processo de gerenciamento de mudanças documentado que identifique mudanças em processos críticos que possam afetar a capacidade do repositório de cumprir com suas responsabilidades obrigatórias. Exemplos: Documentação do processo de gestão de mudanças; avaliação do risco associado a uma mudança de processo; análise dos impactos esperado de uma mudança de processo; comparação de logs de mudanças reais em processos em comparação a análises associadas de seu impacto e criticidade.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.1.1.6.2 O repositório deve ter um processo para testar e avaliar o efeito das mudanças nos processos críticos do repositório. **Exemplos:** Procedimentos de teste documentados; documentação dos resultados de testes anteriores e prova de alterações efetuadas em resultado de testes; análise dos impactos de uma mudança de processo.	Equipe gestora	Elaborar documentos
5.1.2 O repositório deve gerenciar o número e a localização das cópias de todos os objetos digitais. **Exemplos:** Testes de recuperação aleatória; validação da existência de objetos para cada localização registada; validação de um local registrado para cada objeto em sistemas de armazenamento; informações de verificação da proveniência e da fixação; registro de localização/registro de objetos digitais em comparação com o número esperado e localização de cópias de objetos específicos.	Equipe gestora	Executar rotina de testes do ambiente tecnológico
5.1.2.1 O repositório deve ter mecanismos para garantir que qualquer/múltiplas cópias de objetos digitais sejam sincronizadas. **Exemplos:** Fluxos de trabalho de sincronização; análise do sistema de quanto tempo leva para que as cópias sejam sincronizadas; procedimentos/documentação de processos de sincronização.	Equipe gestora	Executar rotina de testes do ambiente tecnológico
5.2 Gestão de risco de segurança		
5.2.1 O repositório deve manter uma análise sistemática dos fatores de risco de segurança associados a dados, sistemas, pessoal e planta física.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico

Exemplos: o repositório emprega os códigos de prática encontrados na lista de controle de sistema da série ISO 27000; análise de risco, ameaça ou controle.		
5.2.2 O repositório deve ter implementado controles para lidar adequadamente com cada um dos riscos de segurança definidos. **Exemplos:** O repositório emprega os códigos de prática encontrados na série de normas ISO 27000; lista de controlo do sistema; análises de risco, ameaça ou controle; e adição de controles baseados na detecção e avaliação de riscos contínuos. O repositório mantém a certificação ISO 17799.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.2.3 A equipe do repositório deve ter funções, responsabilidades e autorizações delineadas relacionadas à implementação de mudanças no sistema. **Exemplos:** O repositório emprega os códigos de prática encontrados na série de normas ISO 27000; lista de controle do sistema; análises de risco, ameaça e adição de meios para detecção e avaliação de riscos contínuos. O repositório mantém a certificação ISO 17799.	Equipe de Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico
5.2.4 O repositório deve ter plano(s) adequado(s) de preparação para desastres e recuperação, incluindo pelo menos um backup externo de todas as informações preservadas com uma cópia externa do(s) plano(s) de recuperação. **Exemplos:** O repositório emprega os códigos de prática encontrados na série de normas ISO 27000; planos de desastre e recuperação; informação e prova de pelo menos uma cópia fora do local da informação preservada; plano de continuidade do serviço; documentação vinculando funções com atividades; dados geológicos, geográficos ou meteorológicos locais ou avaliações de ameaças. O repositório mantém a certificação ISO 17799.	Infraestrutura tecnológica	Realizar manutenção do ambiente tecnológico

Fonte: Elaborada pelo do autor, 2023.