DOI: 10.5433/1981-8920. 2023v28n4p179

REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS (RDC-ARQ): CONCEITOS, PADRÕES E TECNOLOGIAS

TRUSTWORTHY DIGITAL ARCHIVAL REPOSITORIES: CONCEPTS, STANDARDS AND TECHNOLOGIES

Sânderson Lopes Dorneles[a]
Renato Fernandes Corrêa[b]
Daniel Flores[c]

RESUMO
Objetivo: este estudo consistiu em analisar pesquisas relacionadas à repositório arquivístico digital confiável, explorando seus conceitos fundamentais no contexto da gestão arquivística de documentos, e examinando as especificações de requisitos para o seu funcionamento e avaliação da confiabilidade. **Metodologia:** foi realizada uma pesquisa bibliográfica com base em revisão sistemática de literatura, sendo selecionados 40 trabalhos recuperados das bases de dados Brapci, Scopus e *Web of Science*, e por meio da análise de conteúdo foram categorizadas temáticas inerentes aos repositórios arquivísticos digitais confiáveis. **Resultados:** foram identificadas temáticas sobre as características de repositórios digitais, relativas a confiança e princípios arquivísticos. Assim como foram identificados modelos de requisitos e normas para auditoria e certificação, além de plataformas digitais para a preservação de documentos arquivísticos ao longo do tempo. **Conclusões:** para a preservação digital eficaz em repositório arquivístico digital confiável, deve-se aderir a padrões consolidados, estabelecer políticas organizacionais sólidas, realizar auditorias frequentes, e obter certificações que atestem sua confiabilidade. A integração de tecnologia, comprometimento institucional e uma gestão de documentos abrangente é essencial para garantir a preservação e acesso de longo prazo aos documentos digitais para futuras gerações.

Descritores: Preservação digital. Repositórios digitais. Modelo de informação. Certificação.

[a] Doutorando em Ciência da Informação pela Universidade Federal de Pernambuco (UFPE). Docente do Curso de Arquivologia da Universidade Estadual da Paraíba (UEPB). João Pessoa, Brasil. E-mail: sanderson.dorneles@gmail.com

[b] Doutor em Ciência da Computação pela Universidade Federal de Pernambuco (UFPE). Docente do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Pernambuco (UFPE), Recife, Brasil. E-mail: renato.correa@ufpe.br

[c] Doutor em Ciência da Informação pela Universidade Federal do Rio de Janeiro (UFRJ). Docente do Curso de Graduação em Biblioteconomia da Universidade Federal de Alagoas (UFAL) e da Universidade Federal Fluminense (UFF), Niterói, Brasil. E-mail: df@id.uff.br

1 INTRODUÇÃO

A preservação de documentos arquivísticos digitais transcende a mera preocupação com os requisitos tecnológicos ou mesmo com ações de *backup* ou estratégias de migração, conversão, etc, fora de uma abordagem sistêmica da preservação digital. Envolve, igualmente, a formulação de políticas e estratégias para garantir a segurança, a autenticidade e a confiabilidade das informações em ambiente digital. Este imperativo abarca não apenas os documentos criados digitalmente, os chamados documentos nato-digitais, mas também aqueles que passam por uma transição dos formatos tradicionais, como em suporte papel, para o ambiente digital através de processos de digitização, ou mesmo, quando é reproduzido em ambientes digitais, um processo de negócio que era analógico, daí a digitalização.

Como o resultado da digitização é a obtenção de representantes digitais de documentos originados do meio analógico, tem-se toda uma preocupação na manutenção ao longo do tempo destes documentos que podem servir de fonte de prova, desde que, mantenham suas características de autenticidade e confiabilidade.

Quando se fala de autenticidade, se faz imperioso abordar os seus cinco elementos, sendo os dois primeiros, os componentes de identidade e integridade, e os três seguintes, a preservação, a transmissão no tempo e a custódia digital. Qualquer um destes elementos que sejam perdidos ou corrompidos, coloca em risco a manutenção da autenticidade destes documentos de arquivo.

Nesse sentido, a preservação digital abrange uma série de desafios técnicos, organizacionais e sociais. Frank (2022) destaca que esses desafios são amplos e multifacetados, exigindo abordagens variadas para serem superados. A necessidade de preservar documentos digitais, que enfrentam vulnerabilidades como alteração, obsolescência e custos de preservação, é uma preocupação crescente na era digital. Barros, Ferrer e Maia (2018) enfatizam que a rápida evolução tecnológica agrava esses problemas, tornando a preservação digital uma tarefa ainda mais complexa. Isso sugere que, além das

soluções técnicas, é crucial desenvolver estratégias adaptativas que possam acompanhar o ritmo acelerado das mudanças tecnológicas (Andrade; Chagas, 2021).

Além da facilidade de produção e compartilhamento, os documentos digitais trazem consigo preocupações significativas quanto à sua degradação física e ao acesso futuro. Gava e Flores (2020) ressaltam que, apesar das vantagens, essas preocupações não podem ser ignoradas, pois afetam diretamente a longevidade e a usabilidade dos documentos. Essa reflexão leva à consideração da importância de uma abordagem proativa na gestão de documentos digitais, que inclua não apenas medidas de preservação, mas também políticas de atualização e migração de dados para evitar a obsolescência.

A preservação digital carece de uma gestão ativa para garantir o acesso contínuo. Corrado (2019) argumenta que essa gestão deve ir além da tecnologia, incorporando políticas e estratégias claras para manter a integridade dos documentos ao longo do tempo. Isso implica que a preservação digital deve ser vista como um processo contínuo e dinâmico, que envolve não apenas a implementação de tecnologias avançadas, mas também a criação de um ambiente organizacional favorável à manutenção da autenticidade e acessibilidade dos documentos digitais (Gomes; Autran, 2020).

Além da tecnologia, a preservação digital depende fortemente de políticas, processos e compromissos organizacionais. Barros, Ferrer e Maia (2018) sublinham que essa é uma prática multidisciplinar, que requer atenção aos aspectos legais, administrativos e culturais da gestão da informação digital. A reflexão sobre esses aspectos leva ao reconhecimento de que a preservação digital é um campo complexo que exige a colaboração de diversas áreas do conhecimento. Gava e Flores (2022) complementam essa visão, ressaltando a importância de uma abordagem integrada para garantir a efetiva preservação digital. Isso indica que a formação de profissionais capacitados em diferentes áreas é essencial para enfrentar os desafios da preservação digital de forma eficaz e sustentável.

Assim, como estágios evolutivos para uma transformação digital, a

crescente digitização e digitalização, o armazenamento de documentos de arquivo em ambiente digital têm suscitado questionamentos críticos sobre a confiabilidade e segurança dos documentos mantidos em repositórios arquivísticos digitais. Esses questionamentos podem levar a novos modelos de negócio disruptivos, o que, efetivamente se caracterizaria em uma transformação digital, caso contrário, não passaria de uma digitalização, onde seria reproduzido fielmente o processo de negócio analógico, em um ambiente digital.

Nesse contexto, o conceito de Repositório Arquivístico Digital Confiável (RDC-Arq), cunhado no âmbito do Conselho Nacional de Arquivos (CONARQ), emerge como uma abordagem fundamental para garantir a autenticidade, confiabilidade, segurança e acesso dos documentos de arquivo digitais de maneira confiável ao longo do tempo, garantindo uma cadeia de custódia digital para os documentos, nativos digitais ou representantes digitais.

Sendo assim, suscita-se o seguinte problema de pesquisa: Quais aspectos envolvem os Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) para garantir a autenticidade, cadeia de custódia digital, confiabilidade e acesso aos documentos de arquivo em formato digital ao longo do tempo?

Dessa forma, a presente pesquisa tem como objetivo analisar pesquisas sobre RDC-Arq, incluindo seus conceitos fundamentais no contexto da gestão arquivística de documentos e da preservação digital sistêmica, além de especificações de requisitos para o seu funcionamento e avaliação da confiabilidade desses repositórios.

Para tanto, este artigo se encontra estruturado da seguinte forma: a seção 1 de introdução, contextualiza e apresenta o objetivo da pesquisa; na seção 2 são detalhados os procedimentos metodológicos da pesquisa; já a seção 3 apresenta e discute os resultados da pesquisa; para então, na seção 4 serem tecidas as considerações finais.

2 PROCEDIMENTOS METODOLÓGICOS

A pesquisa bibliográfica com base em revisão sistemática de literatura (RSL) teve como fluxo de seleção dos estudos, o que está descrito no Quadro 1,

com a data de coleta no dia 04 de dezembro de 2023.

Quadro 1 – Fluxo da pesquisa

Identificação			**Seleção**		**Elegibilidade**		**Inclusão**
Bases de dados	Termos de busca	Resultados	Exclusão (duplicados)	Exclusão (não pertinência de título e resumo)	Elegíveis	Exclusão (não pertinência ou inacessibilidade de texto completo)	
Brapci	repositório* arquivístico* *AND* digita* *AND* confiáve*	34	3	2	29	1	28
Scopus	*"trustworthy digital repositories" OR "trusted digital repository" AND "archival" OR "archive"*	32	4	2	26	16	10
Web of Science	*"trustworthy digital repositories" OR "trusted digital repository" AND "archival"*	17	5	1	11	9	2
Total	*****	**83**	**12**	**5**	**66**	**25**	**40**

Fonte: Elaborado pelos autores (2024).

Para a análise dos 40 estudos selecionados, foi utilizada a metodologia de análise de conteúdo de Bardin (2011), que consiste em identificar, categorizar e interpretar os significados presentes no material analisado. Dessa forma, foram categorizadas temáticas referentes ao RDC-Arq.

E, essas temáticas foram identificadas e analisadas no *software* ATLAS.ti 9, que consiste em uma ferramenta usada por pesquisadores para analisar dados qualitativos, como entrevistas, transcrições e documentos. Ele oferece recursos como codificação de texto, busca, filtragem e visualizações gráficas para ajudar os usuários a explorarem padrões e temas nos documentos.

3 ANÁLISE DE RESULTADOS

Na revisão sistemática da literatura (RSL), realizou-se uma análise de conteúdo de 40 artigos selecionados com o intuito de explorar perspectivas

associadas ao RDC-Arq, focando na relação entre diversos aspectos para a garantia de preservação digital sistêmica e a manutenção de documentos digitais ao longo do tempo em uma cadeia de custódia digital.

Como resultado dessa investigação, identificaram-se as seguintes temáticas: Repositório digital; Repositório Digital Confiável (RDC); Modelo OAIS (ISO 14721); Auditoria e certificação de repositório digital confiável; Modelos de requisitos e norma para auditoria e certificação (TRAC, NESTOR, DRAMBORA, *CoreTrustSeal*, ACTDR e ISO 16363); Repositório Arquivístico Digital Confiável (RDC-Arq); e Plataformas para a preservação digital de documentos de arquivo (*Archivematica*, Repositório de Objetos Digitais Autênticos (RODA) e Hipátia).

Nesse sentido, esta revisão constitui a base teórica do artigo, eliminando a necessidade de uma seção exclusivamente dedicada a essa fundamentação. Tal abordagem é justificada pela análise dos resultados, que por si só oferece o embasamento teórico necessário. Dessa forma, procede-se à apresentação detalhada sobre os temas identificados, os quais englobam aspectos essenciais para assegurar a preservação de documentos em repositórios arquivísticos digitais confiáveis ao longo do tempo.

3.1 REPOSITÓRIO DIGITAL

O conceito de repositório digital tem sido objeto de análise e discussão na literatura especializada, evidenciando sua complexidade e multifuncionalidade. Rocha (2015), ao abordar este tema, destaca que um repositório digital não deve ser simplificado como um mero armazém de documentos, mas sim compreendido em sua ampla gama de componentes e funcionalidades.

De acordo com a *Computer Science at Cornell University* (*apud* Rocha, 2015), um repositório digital é um sistema informatizado destinado ao armazenamento e distribuição de coleções de uma biblioteca digital. Essa perspectiva é complementada por Martins (2008 *apud* Rocha, 2015) e Lynch e Lippincott (2005 *apud* Rocha, 2015), que ampliam a definição para abranger coleções de informação digital construídas de diversas maneiras e para diferentes propósitos, além de um conjunto de serviços oferecidos pela instituição para a gestão e difusão da produção técnica e científica em meios

digitais.

Rocha (2015) avança em sua definição ao considerar o repositório digital como um ambiente tecnológico complexo, que integra soluções informatizadas para a captura, armazenamento, preservação e acesso aos objetos de informação digitais. Este ambiente é caracterizado pela interação entre *hardware*, *software*, serviços, coleções de informação digital e metadados associados, visando apoiar a gestão de materiais digitais pelo tempo necessário.

O Conselho Nacional de Arquivos (2020 *apud* Chaves, 2023) reforça essa visão ao descrever o repositório digital como um complexo que suporta o gerenciamento de materiais digitais, composto por *hardware*, *software*, metadados, infraestrutura organizacional, além de procedimentos normativos e técnicos. Santos e Flores (2015) enfatizam a importância da autenticidade e da preservação em longo prazo dentro dos repositórios digitais, então, em uma cadeia de custódia digital, destacando a necessidade de implementar ferramentas para estratégias de preservação e metadados padronizados, bem como o registro de ações realizadas sobre os documentos digitais para garantir a confiabilidade dos conteúdos.

Além disso, Santos e Flores (2015) salientam a importância da conformidade com normas e padrões estabelecidos, a colaboração com outros serviços de preservação digital e a busca por interoperabilidade com outros repositórios e sistemas informatizados, o que contribui para a segurança e confiabilidade do repositório digital. Rocha (2015) e Gava e Flores (2020) discutem as aplicações dos repositórios digitais em diferentes contextos, como arquivos de documentação corrente, arquivos permanentes, bibliotecas digitais, coleções de obras de arte digital, entre outros, destacando a relevância dos repositórios institucionais e temáticos na reunião da produção científica de uma instituição ou de uma área específica.

Dessa forma, os repositórios digitais representam uma estrutura complexa e multifacetada, essencial para a gestão, preservação e disseminação da produção técnica e científica em meios digitais, demandando um enfoque integrado que contemple aspectos tecnológicos, organizacionais e normativos para assegurar sua eficácia e sustentabilidade a longo prazo.

3.2 Repositório Digital Confiável (RDC)

Conforme já discutido, os repositórios digitais emergem como pilares fundamentais na gestão, preservação e disseminação do conhecimento e de recursos digitais. Essas plataformas desempenham um papel crítico no armazenamento seguro e no acesso a uma ampla variedade de conteúdos digitais, desde documentos acadêmicos e científicos até coleções digitais de bibliotecas e arquivos.

Contudo, a eficácia desses repositórios não se mede apenas pela sua capacidade de armazenamento ou pela diversidade de conteúdos que conseguem abrigar, mas, fundamentalmente, pela confiabilidade e pela garantia de preservação e acesso contínuo aos recursos digitais ao longo do tempo. Nesse contexto, surgem os Repositórios Digitais Confiáveis (RDCs), que assumem um papel central, exigindo uma análise aprofundada de seus atributos, responsabilidades e desafios para assegurar que cumpram sua missão fundamental de fornecer acesso sustentável e confiável a longo prazo.

Nesse sentido, os Repositórios Digitais Confiáveis (RDCs) têm sido objeto de estudo e discussão por diversos autores ao longo dos anos, evidenciando sua importância fundamental no contexto da preservação digital e do acesso a longo prazo a recursos digitais. Corrado (2019) ressalta a definição de um RDC como um ente cuja missão primordial é fornecer acesso confiável e de longo prazo aos recursos digitais gerenciados para uma comunidade designada, tanto no presente quanto no futuro. Esta missão envolve uma série de responsabilidades e expectativas detalhadas, como a manutenção a longo prazo dos recursos digitais em nome dos depositantes e para o benefício de usuários atuais e futuros.

A conformidade com padrões e modelos estabelecidos, como o modelo de referência *Open Archival Information System* (OAIS) e a norma ISO 16363, é enfatizada por Rocha (2015) e pelo Conselho Nacional de Arquivos (2015 *apud* Gava; Flores, 2020) como essencial para a autenticidade, confiabilidade, acesso e preservação dos dados geridos pelos RDCs. Essa conformidade garante que os repositórios operem dentro de um *framework* reconhecido que assegura a

integridade e a preservação dos recursos digitais ao longo do tempo.

Além disso, a sustentabilidade e responsabilidade fiscal são destacadas por autores como um pilar para a viabilidade de longo prazo dos RDCs. Corrado (2019) menciona que os repositórios devem demonstrar uma gestão fiscal e organizacional responsável, assegurando recursos suficientes para sua manutenção e operação futura. Isso está intrinsecamente relacionado à tecnologia e segurança, onde Rocha (2015) e Barros, Ferrer e Maia (2018) apontam a necessidade de sistemas tecnológicos adequados e seguros que garantam a proteção e a integridade dos dados.

A prática de auditorias e processos de certificação, conforme descrito por Barros, Ferrer e Maia (2018), emerge como uma metodologia para validar a confiabilidade e a autenticidade dos RDCs. Esses processos são cruciais para estabelecer a confiança entre os usuários e os depositantes, demonstrando que os repositórios estão comprometidos com a preservação digital de longo prazo.

A interseção entre preservação digital e acesso é um tema recorrente, com Jantz e Giarlo (2007) enfatizando que a preservação não pode ser dissociada do acesso. Os RDCs devem, portanto, criar um ambiente onde ambos são possíveis, garantindo que os objetos preservados permaneçam acessíveis para gerações futuras, daí depreende-se que os RDCs como ambiente de preservação e acesso se dividem em duas plataformas, uma de preservação e outra de acesso e difusão/transparência ativa.

Desafios relacionados à adaptação tecnológica são abordados por Barros, Ferrer e Maia (2018), que salientam a rápida evolução tecnológica como um fator que exige dos RDCs uma constante atualização de políticas, estratégias e normas. Isso é essencial para manter a confiabilidade e a relevância dos repositórios diante das mudanças tecnológicas.

Na presente revisão sistemática da literatura acerca de Repositórios Digitais Confiáveis, observou-se um destaque para a relevância dos RDCs possuírem uma missão claramente estabelecida, conformidade com padrões e modelos reconhecidos, uma gestão responsável e a habilidade para adaptar-se às inovações tecnológicas.

Esses elementos são fundamentais para assegurar que os RDCs

cumpram seu papel vital na preservação e no acesso a longo prazo aos recursos digitais, conforme evidenciado por autores como Rocha (2015), Corrado (2019) e Barros, Ferrer e Maia (2018).

3.3 MODELO OAIS (ISO 14721)

O Modelo de Referência *Open Archival Information System* (OAIS), que traduzido ao português consiste em Sistema Aberto de Arquivamento de Informação (SAAI), conforme delineado por Barbau *et al.* (2013, 2014), oferece uma estrutura conceitual e terminológica que serve de base para a descrição, comparação e implementação de sistemas de arquivamento digital. Esse modelo se destaca pela sua ampla adoção em esforços de preservação de dados em todo o mundo, servindo como um guia para o desenvolvimento de soluções personalizadas de preservação digital. Pigliapoco (2019) acrescenta que a norma ISO 14721:2012 formaliza o OAIS, prevendo a criação de uma entidade responsável pela conservação do conteúdo digital e sua disponibilização para uma comunidade específica de usuários.

Dentro do modelo OAIS, várias funções e responsabilidades são identificadas, abrangendo desde a ingestão de dados até o acesso e a administração do sistema de arquivamento, conforme apontam Ambracher e Conrad (2021). Essas funções garantem a preservação a longo prazo e o acesso da informação. A flexibilidade é uma característica fundamental do OAIS, permitindo sua adaptação a diferentes contextos tecnológicos, como destacam Gava e Flores (2022). Essa abordagem aberta promove a adaptação e implementação do modelo em diversas plataformas, facilitando a preservação digital de longo prazo em uma variedade de ambientes.

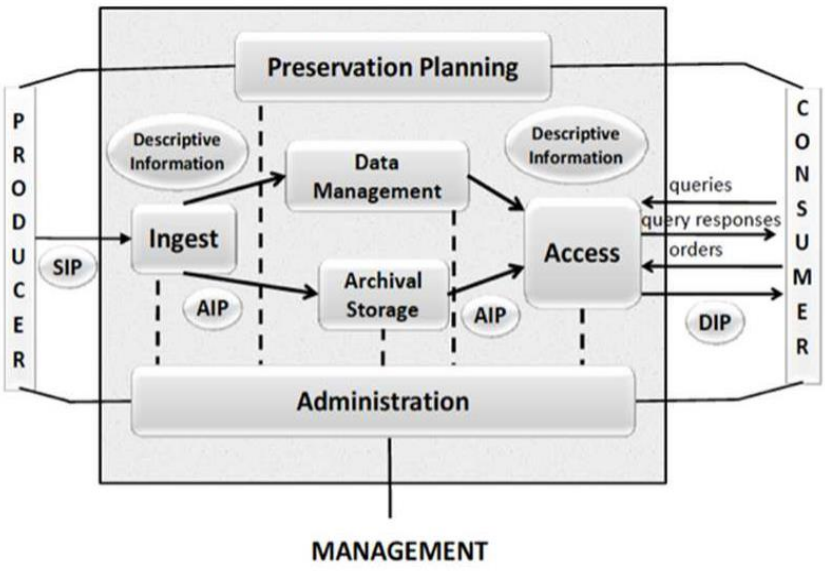
Apesar dos seus muitos benefícios, o modelo OAIS apresenta desafios, particularmente em relação à sua complexidade e à necessidade de estudos mais aprofundados para compreender sua aplicação na arquivística. Santos e Flores (2019, 2022) discutem a importância de explorar as funções de descrição e acesso do modelo, assim como sua aderência aos princípios de proveniência e organicidade dentro do campo da Arquivologia. Essa análise revela como o OAIS preenche lacunas teóricas surgidas com a evolução dos documentos

digitais arquivísticos e se apresenta como a norma mais importante de preservação digital no mundo.

A adaptação do modelo para normas específicas de diferentes países, como a norma brasileira NBR 15472:2007[1] (Gomes; Autran, 2020), mesmo que já descontinuada, demonstra sua aplicabilidade e relevância além das fronteiras, adaptando-se a variados contextos nacionais e disciplinares. Isso sublinha a capacidade do OAIS de orientar a preservação digital em um espectro global, oferecendo um referencial teórico e prático para instituições que buscam manter documentos digitais acessíveis e preservados ao longo do tempo.

O funcionamento do modelo OAIS pode ser descrito através de suas principais entidades funcionais e os fluxos de informação entre elas, conforme a Figura 1.

Figura 1 - Modelo Funcional OAIS



Fonte: Ambracher e Conrad (2021, p. 2191).

Na Figura 1, observa-se que, o fluxo de informação inicia-se com a ingestão (ou admissão, de acordo com o referencial adotado) de dados, onde os Pacotes de Informação para Submissão - *Submission Information Package* (SIPs) são recebidos e preparados para armazenamento e gerenciamento. A

[1] No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) atualizou a norma NBR 15472:2007 com a publicação da ABNT NBR ISO 14721:2021.

administração abrange a negociação de acordos de submissão com os produtores e a garantia da qualidade dos SIPs. Uma vez que os SIPs são validados, eles são transformados em Pacotes de Informação para Arquivamento - *Archival Information Package* (AIPs), que são armazenados para preservação a longo prazo. Informações descritivas são extraídas dos AIPs e gerenciadas para facilitar o acesso e a recuperação das informações armazenadas. A função de acesso coordena as solicitações de informação, transformando AIPs em Pacotes de Informação para Disseminação - *Dissemination Information Package* (DIPs) para entrega aos usuários. Por fim, o planejamento de preservação monitora o ambiente do OAIS para formular estratégias de preservação eficazes.

Sendo assim, o modelo OAIS não apenas fornece um esquema para a preservação digital confiável e eficaz, mas também promove uma compreensão mais profunda das complexidades associadas à gestão de longo prazo de documentos digitais arquivísticos, reforçando sua posição como um padrão essencial na preservação digital global.

3.4 Auditoria e Certificação de Repositório Digital Confiável

Os estudos analisados nessa RSL convergem para a importância fundamental da auditoria e certificação de repositórios digitais, destacando sua relevância para a preservação digital, a confiabilidade e a gestão de documentos de arquivo digitais. Inicialmente, é evidenciada a percepção de que a auditoria atua como uma ferramenta crítica de confiança, onde autores como Barros, Ferrer e Maia (2018) salientam a essencialidade da auditoria para verificar a segurança e a confiança depositadas nos repositórios digitais. Santos e Flores (2015) e Santos (2019) reforçam essa visão, caracterizando a auditoria como um processo sistemático e ao longo da cadeia de custódia digital, ademais documentado para a obtenção de evidências e avaliação da conformidade com os critérios estabelecidos. A importância da comunicação da qualidade e profissionalismo dos repositórios digitais por meio da auditoria e certificação é enfatizada por Donaldson (2020), que destaca o papel desses processos na apresentação dos repositórios a uma ampla rede profissional.

A certificação é apresentada como um mecanismo chave para a garantia da confiabilidade dos repositórios digitais. Thomaz (2007 *apud* Santos; Flores, 2015), Andrade e Chagas (2021) e Frank (2022) discutem a função da certificação na identificação e gestão de riscos, enquanto Reilly e Waltz (2014 *apud* Donaldson, 2020) ressaltam o aspecto colaborativo e iterativo da certificação como uma "conversa" entre o repositório e suas partes interessadas.

Adentrando nos procedimentos e metodologias de auditoria, Santos e Flores (2015) ilustram a necessidade de verificar a conformidade dos repositórios com as normas estabelecidas, considerando infraestruturas física, técnica e tecnológica. Santos (2019) complementa, indicando que a certificação se baseia em padrões como *Trustworthy Repository Audit & Certification* (TRAC), *Network of Expertise in long-term Storage* (NESTOR), *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) e *Audit And Certification of Trustworthy Digital Repositories* (ACTDR), que fornecem uma estrutura metodológica para a avaliação da confiabilidade dos repositórios. Além disso, Santos (2019) expande o entendimento de auditoria para incluir a avaliação dos procedimentos ao longo do ciclo de vida dos documentos arquivísticos, evidenciando uma perspectiva holística e abrangente, o que leva para a abordagem sistêmica da preservação digital e em uma visão de governança, muito mais que de gestão.

No que tange à evolução e aos desafios enfrentados na certificação de repositórios digitais, o desenvolvimento de padrões internacionais para a certificação emerge como tema recorrente em muitos dos estudos analisados.

Sobre isso, Vardigan e Whiteman (2007) relatam que a evolução dos padrões e métricas para a certificação de repositórios digitais confiáveis é um reflexo dos esforços colaborativos internacionais realizados ao longo de várias décadas. Essa jornada começou com o projeto RLG/OCLC (*Research Libraries Group*/*Online Computer Library Center*) sobre metadados de preservação em 2002, seguido de um projeto liderado pelo *Center for Research Libraries* (CRL), financiado pela *Mellon Foudation*, que visava desenvolver métricas de certificação para repositórios. Uma força-tarefa composta por membros do *Research Libraries Group* (RLG) e da Administração Nacional de Arquivos e

Registros - *National Archives and Records Administration* (NARA) trabalhou no desenvolvimento de requisitos de certificação, no delineamento de um processo de certificação e na identificação de organismos certificadores.

Os referidos autores, ainda relatam que, esse esforço conduziu a auditorias de teste em arquivos como o Consórcio Interuniversitário para Pesquisa Política e Social (ICPSR), a *Koninklijke Bibliotheek* e o Portico (arquivo de periódicos eletrônicos incubados na organização *Ithaka Harbors*, que apoia a comunidade acadêmica), com o objetivo de refinar as medidas de auditoria.

Seguindo esses esforços iniciais, Rocha (2015) complementa, ao argumentar que, a RLG e o NARA se associaram, conforme já mencionado, para estabelecer critérios de certificação alinhados com o relatório "Repositórios digitais confiáveis: atributos e responsabilidades" de 2002 do projeto RLG/OCLC, e com base no modelo OAIS. Em 2007, foi publicado o documento "*Trustworthy Repository Audit & Certification: Criteria and Checklist*" (TRAC), que serviu de base para a norma ISO 16363:2012, representando um esforço conjunto para a criação de um quadro de referência para a certificação de repositórios digitais confiáveis.

Ainda sobre esses esforços, Ambracher e Conrad (2021) apresentam detalhes sobre a elaboração da ISO 16363 ao descreverem que, o processo de normatização foi estabelecido pelo *Consultative Committee for Space Data Systems* (CCSDS) através de um grupo no setor *Mission Operations and Information Management Systems* (MOIMS), consistindo em uma área de interesse dentro do CCSDS, que incluiu especialistas que desenvolveram o OAIS. Esse grupo se dedicou a refinar e expandir as métricas de certificação, utilizando teleconferências semanais para revisar as métricas do TRAC, consolidando e clarificando-as. Dessa forma, a norma ISO 16363, "Auditoria e certificação de repositórios digitais confiáveis", foi o resultado desses esforços, alcançando *status* de norma ISO em 2012 e passando por uma revisão em 2021[2] (Ambracher; Conrad, 2021).

Este percurso reflete a busca contínua por práticas robustas e padrões

[2] Em consulta ao site da *International Organization for Standardization*, a norma será substituída pela ISO/DIS 16363, que ainda se encontra em desenvolvimento. Disponível em: https://www.iso.org/standard/56510.html. Acesso em 29 mar. 2024.

confiáveis na preservação digital. Contudo, Corrado (2019) e Donaldson (2020) abordam sobre críticas aos processos de certificação, apontando para possíveis percepções deles serem tecnocráticos e de não envolverem suficientemente os usuários dos repositórios. Apesar dessas críticas, reconhece-se a importância da certificação na demonstração de um compromisso sério com a preservação digital.

Dessa forma, essas discussões evidenciam o papel da auditoria e da certificação como indispensáveis para assegurar a confiabilidade, segurança e sustentabilidade de repositórios digitais. Estes processos implicam uma abordagem rigorosa e sistemática na gestão e preservação de conteúdos digitais, enquanto os desafios identificados sugerem a necessidade de adaptação das práticas de auditoria e certificação às demandas específicas dos repositórios e de seus usuários, promovendo a inclusão de todas as partes interessadas no processo.

3.4.1 Modelos de requisitos e norma para auditoria e certificação

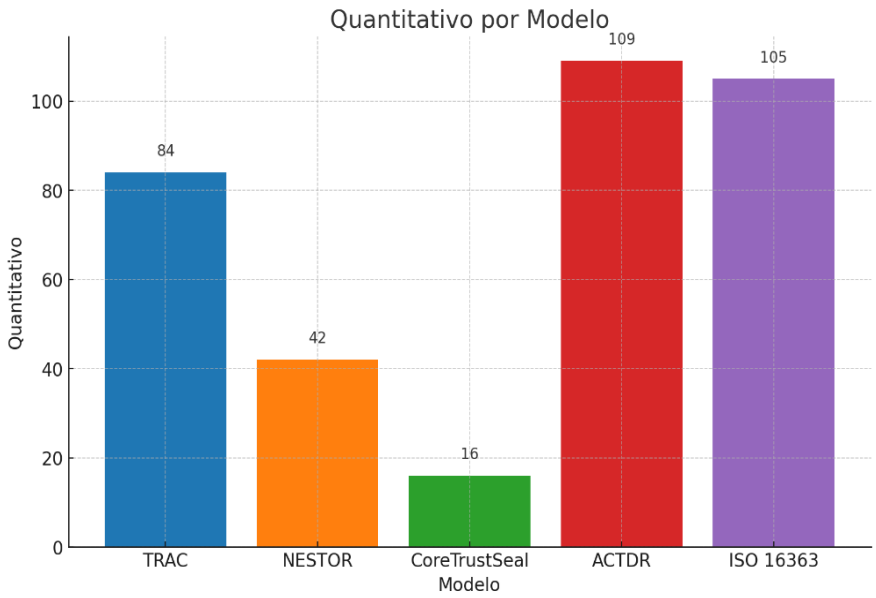
A seguir, serão descritos modelos de requisitos e a norma ISO 16363 para auditoria e certificação de repositórios digitais, focando na preservação segura e acessível do conteúdo digital.

Entre os modelos de requisitos estão o *Trustworthy Repository Audit & Certification* (TRAC), que oferece critérios para avaliar a confiabilidade dos repositórios; o selo alemão para padrões de qualidade em preservação digital, *Network of Expertise in long-term Storage* (NESTOR); o *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA), que propõe uma abordagem baseada em risco para auditoria de repositórios; o *CoreTrustSeal*, que define requisitos básicos para a confiança em repositórios; e o *Audit and Certification of Trustworthy Digital Repositories* (ACTDR), que harmoniza práticas internacionais para a certificação de repositórios digitais confiáveis.

Antes de explorar em profundidade cada modelo e a norma, é relevante a apresentação do Gráfico 1, que ilustra o número de requisitos dos mesmos, conforme levantado junto aos estudos da RSL, com exceção do DRAMBORA que não é prescritivo em termos de um número específico de requisitos que

devem ser seguidos, mas fornece um quadro conceitual e uma série de ferramentas que permitem aos repositórios realizarem uma auditoria abrangente de suas operações, políticas e procedimentos.

Gráfico 1 – Quantitativo de requisitos dos modelos e da ISO 16363 para auditoria e certificação de repositórios digitais confiáveis



Fonte: Elaborado pelos autores (2024).

Na imagem do Gráfico 1, verifica-se que, ACTDR e ISO 16363 têm os maiores números de requisitos, enquanto CoreTrustSeal tem o menor.

Nesse sentido, por meio da descrição desses modelos e da norma ISO 16363, busca-se compreender os objetivos e as estruturas empregadas na avaliação e certificação, visando a preservação do conteúdo digital ao longo do tempo.

3.4.1.1 Trustworthy Repository Audit & Certification (TRAC)

O *Trustworthy Repository Audit & Certification* (TRAC), desenvolvido em 2007 pelo *Online Computer Library Center* (OCLC) e *Research Libraries Group* (RLG), surgiu como resposta à necessidade de um processo formal de certificação para repositórios digitais confiáveis. Este esforço colaborativo, detalhado por Gomes e Autran (2020) e Frank (2022), envolveu organizações como *Research Libraries Group* (RLG), *National Archives and Records*

Administration (NARA), *Center for Research Libraries* (CRL), e *Consultative Committee for Space Data Systems* (CCSDS), culminando na criação de um conjunto de critérios e práticas para a auditoria e certificação de repositórios. O TRAC evoluiu para a norma ISO 16363:2012, conforme Welch e Phillips (2014 *apud* Andrade e Chagas, 2021), estabelecendo diretrizes rigorosas para a avaliação da confiabilidade de repositórios digitais.

Os critérios do TRAC, abordados por Rocha (2015) e Gava e Flores (2020), estão organizados em três seções principais, cobrindo a infraestrutura organizacional, o gerenciamento de objetos digitais e a infraestrutura técnica. Estes critérios são fundamentais para a certificação, oferecendo uma estrutura abrangente que inclui desde a admissão de documentos digitais até o gerenciamento de informação e acesso.

A implementação do TRAC e sua subsequente evolução refletem o trabalho conjunto de especialistas internacionais, promovendo a confiabilidade e sustentabilidade de longo prazo de repositórios digitais (RLG/NARA, 2007 *apud* Andrade e Chagas, 2021; Santos, 2019). Assim, o TRAC se estabelece como um marco na gestão de repositórios digitais, assegurando que estes atendam às necessidades contemporâneas e futuras de preservação e acesso à informação digital.

3.4.1.2 Network of Expertise in long-term STORage (NESTOR)

O *Network of Expertise in long-term STORage* (NESTOR), conforme descrito por Barros, Ferrer e Maia (2018), é um catálogo de critérios voltado para a preservação digital a longo prazo, destacando-se pela sua abordagem baseada na comunidade alemã. Esta iniciativa é corroborada pelo trabalho de Santos e Flores (2015), que enfatizam a relevância do NESTOR para organizações de memória, como arquivos, bibliotecas e museus, servindo como um guia essencial para a criação, planejamento e estabelecimento de Repositórios Digitais Confiáveis (RDCs). O catálogo é reconhecido por sua aplicabilidade tanto em instituições de administração de arquivos quanto em serviços comerciais e não comerciais, além de serviços de terceiros, evidenciando a sua abrangência e flexibilidade.

Santos (2019) acrescenta que, desde a sua concepção inicial em 2006 e a subsequente atualização em 2009, o NESTOR tem sido objeto de discussão internacional, ampliando seu escopo para além da Alemanha. Este aspecto internacional reforça a importância do catálogo em estabelecer padrões e diretrizes para a preservação digital em um contexto global. A estrutura do NESTOR, enriquecida com explicações detalhadas e exemplos práticos, é projetada para facilitar a implementação efetiva dos critérios por diversas organizações.

A origem do NESTOR, conforme detalhado por Andrade e Chagas (2023), reflete um esforço coletivo envolvendo o Ministério da Pesquisa e Educação da Alemanha, instituições culturais e fornecedores de tecnologia. Esta colaboração sublinha o compromisso com a promoção de um padrão de preservação digital, reconhecendo as complexidades e desafios associados à manutenção da informação digital a longo prazo.

3.4.1.3 Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)

O método *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA), fruto da colaboração entre o *Digital Curation Centre* (DCC) e o *Digital Preservation Europe* (DPE), é destacado por Santos e Flores (2015) e Santos (2019) como uma ferramenta crucial para a auditoria interna de repositórios digitais. Este método não apenas facilita a análise de capacidades, vulnerabilidades e forças dos repositórios, mas também prepara essas instituições para auditorias externas, contribuindo para sua certificação de confiabilidade. O processo inclui identificação do contexto organizacional, avaliação e gestão de riscos, bem como a interpretação dos resultados da auditoria.

Santos (2019) ressalta a importância do DRAMBORA na preparação de organizações para atender aos requisitos necessários de auditorias externas, permitindo uma gestão eficaz de riscos. Isso não apenas beneficia a organização internamente, mas também fornece evidências de comprometimento com a preservação digital de longo prazo.

3.4.1.4 CoreTrustSeal

O programa de certificação *CoreTrustSeal*, lançado em 2017 por meio da colaboração entre *o Data Seal of Approval* (DSA) e o ICSU *World Data System* (ICSU-WDS), surge como uma iniciativa voltada para a certificação básica de repositórios de dados. De acordo com Corrado (2019), o objetivo deste programa é fundamentar-se nos requisitos principais de repositórios de dados confiáveis, conforme estabelecido pelo catálogo DSA-WDS, visando proporcionar uma certificação baseada em critérios claros e objetivos. A mesma visão é compartilhada por Donaldson (2020), que destaca a importância da certificação para os repositórios de dados, ao fornecer um caminho para a demonstração de sua sustentabilidade e confiabilidade.

O processo de avaliação, segundo Corrado (2019), é meticuloso e se baseia na revisão de 16 requisitos essenciais, divididos em três categorias principais: infraestrutura organizacional, gerenciamento de objetos digitais e tecnologia. Este procedimento, apesar de não exigir visitas presenciais, demanda que os repositórios apresentem evidências públicas de sua conformidade com esses requisitos, salvo em situações que envolvam informações confidenciais. A abordagem para a certificação, conforme exposto por Donaldson (2020), também inclui uma autoavaliação interna dos repositórios, seguida de uma revisão por pares dentro da comunidade, sublinhando a importância da transparência e da melhoria contínua na gestão dos dados.

Além disso, Donaldson (2020) realça o papel da *CoreTrustSeal* como uma organização comunitária sem fins lucrativos, que não apenas promove infraestruturas de dados sustentáveis e confiáveis, mas também fomenta uma maior conscientização e aderência aos padrões estabelecidos. Essa perspectiva é complementada por Corrado (2019), que enxerga o *CoreTrustSeal* não como um padrão definitivo de certificação, mas como um primeiro passo em direção a um quadro global de certificação de repositórios, evidenciando um caminho para o avanço na qualidade e na confiabilidade dos dados armazenados.

3.4.1.5 Audit and Certification of Trustworthy Digital Repositories (ACTDR)

A discussão sobre a certificação de repositórios digitais se concentra no *Audit and Certification of Trustworthy Digital Repositories* (ACTDR), que evoluiu do TRAC para a norma ISO 16363:2012, marcando um esforço para estabelecer padrões reconhecidos internacionalmente para a confiabilidade de repositórios digitais. Corrado (2019) ressalta a importância e os desafios do processo de certificação, que, apesar de seu custo e complexidade, oferece um marco para a confiabilidade e sustentabilidade.

Santos e Flores (2015, 2020) e Andrade e Chagas (2023) enfatizam a relevância do ACTDR como ferramenta para avaliar a confiabilidade dos repositórios em infraestrutura organizacional, gestão de objetos digitais, e gestão de riscos de segurança. A evolução para a ISO 16363:2012 amplia o reconhecimento e adoção dos padrões, estabelecendo um símbolo de qualidade e confiabilidade para repositórios digitais (Carvalho, 2015 *apud* Santos, 2019; Andrade; Chagas, 2023).

Barbau *et al.* (2013, 2014) e Santos e Flores (2020) detalham os aspectos cobertos pelo ACTDR, sublinhando a importância da conformidade em diversas áreas. A certificação, embora desafiadora devido à sua complexidade e custo (Corrado, 2019), serve como um passo essencial para a melhoria da gestão de riscos e tomada de decisões informadas.

Santos (2019) destaca a necessidade de revisão contínua do ACTDR para manter sua pertinência e eficácia diante das mudanças tecnológicas. Este processo assegura que o ACTDR continue a ser o principal padrão para a auditoria externa de repositórios digitais, promovendo práticas de alta qualidade em gestão e preservação de conteúdos digitais.

3.4.1.6 Norma de Auditoria e Certificação de Repositórios Digitais Confiáveis (ISO 16363)

A norma ISO 16363:2012 é direcionada para a avaliação, auditoria e certificação de repositórios digitais, com o intuito de assegurar a confiabilidade e sustentabilidade dessas infraestruturas. Segundo Gomes e Autran (2020), o objetivo central da norma é facilitar processos de auditoria que permitam avaliar de forma eficaz a gestão dos objetos digitais nos repositórios, através de uma

estrutura de critérios bem definidos. Gonçalez (2017) reforça essa perspectiva ao salientar a importância da norma como ferramenta para a documentação necessária e a condução do processo de auditoria, incluindo a definição de requisitos para os auditores e a balização do processo de certificação.

A estrutura da ISO 16363:2012, conforme detalhado por Ambacher e Conrad (2021), é composta por 105 critérios agrupados em três categorias principais: Infraestrutura Organizacional, Gerenciamento de Objetos Digitais, e Infraestrutura e Gestão de Segurança. Gonçalez (2017) acrescenta que, apesar da abrangência dos critérios, a aplicabilidade não é universal, e a falta de detalhamento em algumas áreas pode levar a diferentes interpretações, exigindo adaptação conforme o contexto específico de cada repositório.

O processo de auditoria e certificação, como explicado por Ambacher e Conrad (2021), inicia-se com uma revisão da documentação do repositório, seguida de uma avaliação detalhada durante uma visita ao local. Este processo não só garante a conformidade com os critérios estabelecidos, mas também permite identificar e corrigir possíveis deficiências antes da certificação. Os repositórios que atendem aos requisitos recebem um certificado com validade de três anos, dependendo da realização de auditorias anuais de supervisão e da manutenção das condições que garantiram a certificação inicial.

Em termos de metodologia, a ISO 16363:2012 propõe uma abordagem que inclui ferramentas de autodiagnóstico e autoavaliação, destinadas a identificar omissões e falhas potenciais nos sistemas de preservação digital (Barros; Ferrer; Maia, 2018). Essas ferramentas são fundamentais para assegurar a aplicação efetiva dos critérios de avaliação e para promover a melhoria contínua das práticas de preservação digital.

Além disso, a norma passou por revisões regulares e foi submetida a testes práticos em repositórios reais antes da sua finalização, para assegurar a relevância e aplicabilidade dos critérios estabelecidos (Ambacher; Conrad, 2021). Essas iniciativas sublinham o compromisso com a adequação da norma à realidade operacional dos repositórios digitais, visando aprimorar continuamente os padrões de confiabilidade e sustentabilidade na preservação digital.

Nesse contexto, surge a ISO 16919:2014[3] como um complemento importante no âmbito da certificação de repositórios digitais confiáveis, delineando um conjunto de requisitos específicos para entidades certificadoras. Esta norma, conforme descrito por Flores, Pradebon e Cé (2017), apresenta critérios essenciais direcionados às entidades responsáveis pela certificação de repositórios digitais confiáveis, que tem como principal intuito estabelecer um padrão de práticas para as organizações encarregadas de avaliar a confiabilidade de tais repositórios, com base na ISO 16363, visando garantir uma certificação adequada.

Sendo assim, a ISO 16363:2012 emerge como um instrumento vital para a promoção de práticas confiáveis de preservação digital, oferecendo um guia abrangente para a avaliação e certificação de repositórios digitais. Através do estabelecimento de critérios claros e da condução de processos de auditoria rigorosos, a norma desempenha um papel crucial na garantia da integridade e acessibilidade de longo prazo dos objetos digitais armazenados nesses repositórios.

3.5 REPOSITÓRIO ARQUIVÍSTICO DIGITAL CONFIÁVEL (RDC-ARQ)

O termo e o conceito associado ao Repositório Arquivístico Digital Confiável (RDC-Arq) tem sua origem no âmbito do Conselho Nacional de Arquivos, quando foi definido no documento "*Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq*", instituído pela Resolução CONARQ n.º 43/2015 (Conselho Nacional de Arquivos, 2015), que alterou o termo "repositório digital confiável de documentos arquivísticos" estabelecido na Resolução CONARQ nº 39/2014 (Conselho Nacional de Arquivos, 2014) para o já referido "repositório arquivístico digital confiável" e acrônimo RDC-Arq, mantendo as seguintes definições:

> Um repositório arquivístico digital é um repositório digital que armazena e gerencia esses documentos, seja nas fases corrente e intermediária, seja na fase permanente. Como tal, esse

[3] Em consulta ao site da *International Organization for Standardization*, a norma será substituída pela ISO/DIS 16919, que ainda se encontra em desenvolvimento. Disponível em: https://www.iso.org/standard/57950.html. Acesso em 29 mar. 2024.

> repositório deve:
> - gerenciar os documentos e metadados de acordo com as práticas e normas da Arquivologia, especificamente relacionadas à gestão documental, descrição arquivística multinível e preservação; e
> - proteger as características do documento arquivístico, em especial a autenticidade (identidade e integridade) e a relação orgânica entre os documentos. (Conselho Nacional de Arquivos, 2015, p. 9).

Esta adjetivação que foi realizada nos RDCs, da Resolução CONARQ nº 39/2014 para a Resolução CONARQ nº 43/2015 e agora referendada pela atual Resolução CONARQ nº 51/2023, foi estratégica pela equipe elaboradora, quando especificou que não se trata somente de um RDC para documentos arquivísticos, mas sim, um RDC específico, com requisitos próprios para a gestão, a preservação e o acesso/difusão de documentos de arquivo, seja nas idades corrente, intermediária ou permanente.

“Um repositório arquivístico digital confiável deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável.” (Conselho Nacional de Arquivos, 2015, p. 10).

Dessa forma, as definições refletem uma compreensão profunda dos desafios associados à gestão de documentos arquivísticos digitais, sublinhando a necessidade de abordagens rigorosas e sistemáticas para garantir a preservação e o acesso dos documentos digitais ao longo do tempo e em uma cadeia de custódia digital. Isso envolve não apenas a aplicação de tecnologias avançadas, mas também a adesão a princípios arquivísticos estabelecidos que assegurem a proteção e a perpetuação do valor histórico e informativo dos documentos.

No que se refere a evolução das diretrizes do Conselho Nacional de Arquivos (CONARQ) para a implementação de um RDC-Arq é evidenciada por uma linha cronológica que começa, em 2014 com a Resolução CONARQ nº 39 (Conselho Nacional de Arquivos, 2014), estabelecendo as primeiras diretrizes para repositórios arquivísticos e orientando os órgãos e entidades do Sistema Nacional de Arquivos (SINAR) quanto à preservação e acesso em longo prazo.

Em 2015, a Resolução CONARQ nº 43 (Conselho Nacional de Arquivos, 2015) expande o escopo dessas diretrizes, introduzindo o termo Repositório Arquivístico Digital Confiável (RDC-Arq), enfatizando a importância da

conformidade com a norma ISO 16363:2012, e delineando requisitos para um repositório digital confiável.

No ano de 2023, a Resolução CONARQ nº 51 (Conselho Nacional de Arquivos, 2023) institui uma atualização significativa nas "*Diretrizes para implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq)*", mas, mantendo a essência do RDC-Arq criado originalmente. Essa atualização se caracteriza pelo aumento no número de requisitos, passando de 74, conforme identificado por Andrade e Chagas (2023), para 109 requisitos, coincidindo com o mesmo número de requisitos do ACTDR. Diante disso, a Tabela 1 detalha as alterações ocorridas no quantitativo de requisitos entre as diferentes versões do RDC-Arq, evidenciando as mudanças implementadas.

Tabela 1 - Organização e número de requisitos entre versões do RDC-Arq

Dimensões	RDC-Arq 2015	RDC-Arq 2023
Infraestrutura organizacional	17	25
Gerenciamento do documento digital	43	60
Tecnologia, infraestrutura técnica e segurança	14	24
Total	**74**	**109**

Fonte: Elaborado pelos autores (2024)

Além do aumento do número de requisitos, outra atualização foi em relação a organização da estrutura de apresentação dos requisitos, que ganharam mais detalhamentos, apresentando as seguintes especificações: Seção, Subseção, Requisito e Evidência. Ao aprimorar essas descrições, especialmente aquelas relacionadas à Evidência, os procedimentos de auditoria e certificação de um RDC-Arq são significativamente facilitados. Além disso, é importante ressaltar que o documento das diretrizes destaca uma seção que apresenta uma lista detalhada de tipos de documentos necessários para satisfazer determinados requisitos.

Dessa forma, essa trajetória das diretrizes do CONARQ reflete os esforços contínuos para estabelecer uma gestão eficaz e uma preservação duradoura dos documentos arquivísticos digitais no Brasil, demonstrando a crescente conscientização sobre os desafios da preservação digital e a

necessidade de estratégias específicas que assegurem a confiabilidade, autenticidade e acesso a longo prazo aos acervos digitais, sempre mantidos em uma cadeia de custódia digital, de forma a garantir a segurança jurídica dos cidadãos.

Segundo Gava e Flores (2020), a implementação e gestão de Repositórios Digitais Confiáveis Arquivísticos (RDC-Arq) emergem como desafios multidisciplinares que requerem a sinergia entre profissionais de diversas áreas, notavelmente entre arquivistas e especialistas em Tecnologia da Informação (TI). Esta colaboração multidisciplinar é vital para além da simples manutenção de *softwares* e *hardwares*, envolvendo a integração de pessoas, políticas, normas, padrões, modelos e requisitos necessários para a preservação digital eficaz dos documentos arquivísticos digitais.

Gava e Flores (2020, 2022) realçam que o RDC-Arq transcende a tecnologia, evidenciando a importância de uma abordagem organizacional que garanta a autenticidade e a preservação permanente dos documentos arquivísticos digitais, alinhando-se aos requisitos de um Repositório Digital Confiável (RDC) em um nível conceitual.

A aderência ao modelo *Open Archival Information System* (OAIS) é sublinhada por Santos (2019) como crucial para a realização de atividades de preservação digital, abrangendo a admissão, armazenamento, gerenciamento de dados, acesso e disseminação. A interoperabilidade entre Sistemas Informatizados de Gestão Arquivística de Documentos (SIGADs ou GestãoDoc) e RDC-Arq é destacada como essencial para manter uma cadeia de custódia digital confiável, ininterrupta, imaculada, enfatizando a necessidade de um ambiente de preservação confiável a longo prazo, mantendo assim, a fonte de prova dos documentos de arquivo e o princípio de não repúdio – jurídico - desses.

Os desafios inerentes à preservação digital incluem a necessidade de abordar a obsolescência tecnológica e garantir a segurança e confiabilidade dos documentos digitais. A auditoria periódica e a certificação são apresentadas como elementos críticos para assegurar a confiabilidade dos repositórios, com Barros, Ferrer e Maia (2018) apontando para a importância de mecanismos que

registrem alterações nos objetos digitais e garantam ambientes de armazenamento seguros. Andrade e Chagas (2021), bem como Braga, Holanda e Canelhas (2022), reforçam a necessidade de uma infraestrutura robusta, políticas claras e colaboração entre profissionais de diversas áreas para superar esses desafios.

Portanto, a partir da análise dos estudos a respeito dos repositórios arquivísticos digitais confiáveis, emerge um consenso sobre a complexidade dos mesmos, que abrange aspectos tecnológicos, organizacionais, normativos e disciplinares, enfatizando a importância de aderir a padrões internacionais, a necessidade de uma gestão colaborativa entre arquivistas e profissionais de TI, e a essencialidade de processos de auditoria e certificação na implementação e gestão eficaz de repositórios arquivísticos digitais confiáveis.

3.6 Plataformas para a Preservação Digital de documentos de arquivo

No contexto de um RDC-Arq, as plataformas para a preservação digital de documentos correspondem aos aspectos tecnológicos, constituídos de *software* específicos e infraestrutura de *hardware*. Sendo assim, no escopo desta revisão sistemática de literatura foram identificados e serão descritos os seguintes *softwares*: *Archivematica*, Repositório de Objetos Digitais Autênticos (RODA) e a solução brasileira Hipátia.

3.6.1 *Archivematica*

O *Archivematica* é amplamente reconhecido como um *software* livre e de código aberto, cujo propósito é a preservação digital de documentos digitais em longo prazo. Segundo Flores, Pradebon e Cé (2017), o *software* serve como um Repositório Arquivístico Digital Confiável (RDC-Arq), capaz de armazenar documentos conforme os padrões de preservação exigidos. Esse aspecto é reforçado por Schuc, Saad e Flores (2019), que enfatizam sua capacidade de processar objetos digitais desde a ingestão (ou admissão) até o acesso, em conformidade com o modelo funcional *Open Archival Information System* (OAIS).

A gestão e o desenvolvimento do *Archivematica* são atribuídos à

Artefactual Systems, uma empresa canadense, que trabalha em colaboração com instituições de renome como a *United Nations Educational, Scientific and Cultural Organization* (UNESCO) e diversas entidades acadêmicas e arquivísticas canadenses (Gomes; Autran, 2020). O projeto inicial foi motivado por um relatório ao Programa *Memory of the World* da UNESCO, destacando a necessidade de um sistema de preservação digital baseado em OAIS, o que culminou no desenvolvimento do *Archivematica* (Gava; Flores, 2021).

A interoperabilidade e o uso de padrões de metadados são aspectos cruciais do *Archivematica*, conforme destacado por vários autores durante esta RSL. A adesão a padrões reconhecidos como PREMIS, *Dublin Core*, e a conformidade com o modelo OAIS são essenciais para a geração de pacotes de informação para arquivamento (AIPs) confiáveis, autênticos e interoperáveis (Gomes; Autran, 2020). Essa interoperabilidade é vista como uma vantagem significativa, permitindo a comunicação com outros sistemas e dispositivos usados por arquivos, bibliotecas, museus e instituições de ensino.

O *Archivematica* é distribuído sob licenças que promovem a liberdade de copiar, distribuir e modificar o sistema, enfatizando seu compromisso com os princípios do *software* livre e de código aberto (Gomes; Autran, 2020). As funcionalidades do *software* são segmentadas em oito áreas projetadas por uma interface na *web*, direcionada à perspectiva do usuário final:

> Transferência (*Transfer*), Ingestão (*Ingest*), Armazenamento Arquivístico (*Archival Storage*), Planejamento de Preservação (*Preservation Planning*), Acesso (*Access*), Administração (*Administration*), Lista de pendências (*Backlog*) e Avaliação (*Appraisal*) (Gomes; Autran, 2020, p. 107).

No Brasil, a adoção do *Archivematica* enfrenta desafios específicos, principalmente devido à escassez de literatura brasileira sobre o tema. Contudo, é reconhecido como uma estratégia eficaz para preservação digital, com esforços sendo feitos para promover sua implementação e uso em instituições brasileiras (Gava; Flores, 2021).

Chaves (2023) destaca a pertinência do *Archivematica* para a realidade das instituições arquivísticas brasileiras, evidenciando as ações para sua adoção, incluindo a adaptação de guias pelo Conselho Nacional de Arquivos e a integração com a ferramenta AtoM (legado ICA-AtoM).

Dessa forma, o *Archivematica* é destacado na literatura consultada como uma solução robusta e confiável para a preservação digital sistêmica, suportado por uma comunidade ativa de desenvolvimento e uma base de usuários global. Seu desenvolvimento, características, e esforços de implementação refletem um compromisso contínuo com a preservação digital de longo prazo, demonstrando sua importância e adaptabilidade a diferentes contextos, incluindo o brasileiro.

3.6.2 Repositório de Objetos Digitais Autênticos (RODA)

De acordo com Chaves (2023), o Repositório de Objetos Digitais Autênticos (RODA), desenvolvido pela Direção-Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB) em Portugal, baseia-se em tecnologias *open source* e adota as normas OAIS, EAD, METS e PREMIS, configurando-se como um repositório certificado conforme a norma ISO 16363:2012.

Ainda, segundo a autora, o projeto contou com a colaboração da Direção de Arquivos de Portugal (DGARQ) e teve suporte técnico da Universidade do Minho, com desenvolvimento realizado pela empresa *Keep Solutions*. O RODA incorpora a funcionalidade obrigatória pelo OAIS, sendo um aplicativo que atende aos requisitos de um RDC-Arq, garantindo integração com outros sistemas e suporte para múltiplos formatos, além de ser auditável e exigir registro de usuários.

Por fim, Chaves (2023) relata que, através de tecnologia evolutiva por meio de *plugins*, o RODA oferece ações de preservação incorporadas, como reservas de formatos, verificações de integridade, diagnóstico e mitigação de riscos, produção de relatórios e verificação de vírus, o que o configura como um RDC-Arq utilizado para documentos arquivísticos.

3.6.3 Hipátia

O desenvolvimento e as características do Hipátia, conforme descrito por Shintaku, Braga e Oliveira (2021), evidenciam a contribuição significativa da instituição desenvolvedora dessa plataforma, o Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), que a partir dessa contribuição tecnológica

contribui com a automação do processo de preservação de documentos de arquivo.

Esse *software*, também nomeado como um modelo, serve como um elo integrador entre sistemas de informação e repositórios arquivísticos digitais confiáveis, respeitando a cadeia de custódia digital e eliminando a necessidade de intervenção manual. Essa característica é particularmente relevante na integração entre sistemas administrativos eletrônicos, como o Sistema Eletrônico de Informações (SEI), amplamente utilizado por órgãos do Poder Executivo Federal, e sistemas de preservação, como o *Archivematica*, garantindo a integridade e a autenticidade dos documentos transferidos.

Essa integração entre sistemas no Hipátia, só é possível por intermédio da funcionalidade do *crosswalk*, que é detalhada por Shintaku, Braga e Oliveira (2021), a partir dos estudos de Arora e Shah (2009) e Bountori e Gergatsoulis (2009), que explicam como essa técnica permite a conversão e compatibilidade entre diferentes padrões de metadados. O *crosswalk* facilita a adaptação de informações de variados sistemas de informação ao formato requerido para a preservação, de acordo com o modelo OAIS. Este processo de mapeamento de metadados é crucial para que o Hipátia possa integrar eficientemente dados de múltiplos sistemas, preservando a cadeia de custódia digital e garantindo a integridade dos documentos arquivísticos.

Além disso, a evolução e a implementação institucional do Hipátia são abordadas por Braga, Holanda e Canelhas (2022), que destacam a adaptabilidade e a evolução contínua do *software* para atender às diretrizes do CONARQ. Os autores relatam que, a parceria para implementação dessa plataforma estabelecida com o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) ilustra a aplicabilidade prática do Hipátia na melhoria da gestão documental e na preservação digital. Ainda, segundo os autores, essa abordagem reforça o papel do Hipátia como um modelo aberto, capaz de se adaptar e evoluir de acordo com as necessidades institucionais e os avanços informacionais, facilitando a implementação de repositórios arquivísticos digitais confiáveis em diversas organizações.

Sendo assim, o Hipátia representa uma inovação importante no campo da

Arquivologia digital, oferecendo soluções para a integração de sistemas de gestão eletrônica de documentos e repositórios arquivísticos de forma automatizada e confiável. Através da funcionalidade do *crosswalk* e da sua capacidade de evolução contínua, o Hipátia atende às demandas de preservação digital sistêmica, respeitando as normas e diretrizes estabelecidas para a gestão de documentos arquivísticos. A colaboração entre o IBICT e instituições como o TJDFT destaca a relevância do Hipátia para a preservação digital e a gestão documental, indicando seu potencial para contribuir significativamente para a Arquivologia moderna.

4 CONSIDERAÇÕES FINAIS

Neste trabalho, explorou-se amplamente o universo dos Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq), abordando-se desde os aspectos conceituais envolvidos até a prática de preservação digital sistêmica eficaz.

Inicialmente, discutiu-se a complexidade da preservação de documentos arquivísticos digitais, destacando que tal tarefa transcende os aspectos tecnológicos para envolver políticas, estratégias e uma visão integrada e sistêmica que abarca tanto os documentos nato-digitais (fruto de uma digitalização - reprodução de um processo de negócio analógico em ambiente digital, ou mesmo, de novos modelos de negócio, o que configura uma transformação digital, com inovação ou disrupção) quanto aqueles convertidos para o formato digital - os representantes digitais, fruto de uma digitização.

A metodologia adotada para o estudo consistiu em uma revisão sistemática da literatura, cujos resultados apontaram para a importância de uma abordagem multidisciplinar na gestão dos RDC-Arq. Estes repositórios emergiram como estruturas essenciais para garantir a autenticidade, cadeia de custódia digital, confiabilidade e acesso a longo prazo dos documentos digitais, demandando aderência a padrões internacionais, gestão colaborativa e processos de auditoria e certificação rigorosos.

Discutiu-se também o modelo OAIS como referencial para a preservação digital sistêmica, a relevância das auditorias e certificações para estabelecer a confiança nos RDC-Arq e a importância da evolução das diretrizes do CONARQ

na estruturação desses repositórios. Plataformas como *Archivematica*, RODA e Hipátia foram apresentadas como soluções tecnológicas adaptáveis que oferecem suporte à preservação digital de documentos de arquivo, demonstrando a aplicabilidade prática dos conceitos discutidos.

Para responder à questão central desta pesquisa sobre os aspectos relacionados aos Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) que garantem a autenticidade, cadeia de custódia digital, confiabilidade e acesso contínuo aos documentos de arquivo em formato digital ao longo do tempo, destaca-se a importância de uma série de práticas e conformidades estratégicas, com base nos estudos analisados.

Nesse sentido, os RDC-Arq devem:

1) Assegurar a conformidade com padrões internacionais reconhecidos, como o *Open Archival Information System* (OAIS) e a ISO 16363, assim como as atuais diretrizes da Resolução CONARQ nº 51/2023 (Conselho Nacional de Arquivos, 2023) que fornecem orientações detalhadas para a preservação digital confiável e a gestão de repositórios;

2) Estabelecer e manter políticas e procedimentos organizacionais robustos, criando uma estrutura sólida que abrange todos os aspectos da preservação e gestão de documentos digitais;

3) Submeter-se a auditorias regulares, que verificam a aderência aos padrões e práticas recomendadas, além de avaliar a eficácia dos processos de preservação digital implementados;

4) Obter certificações relevantes que validem sua confiabilidade, evidenciando não apenas a competência técnica, mas também o comprometimento com as melhores práticas de preservação digital.

Adicionalmente, embora a tecnologia desempenhe um papel crucial nesse contexto, ela representa apenas uma faceta dessa complexa estrutura. É imperativo também que haja um compromisso institucional profundo, colaboração interdisciplinar e uma gestão de documentos que compreenda todo o ciclo de vida dos documentos, desde sua gênese, produção, utilização e destinação, seja a guarda permanente ou o descarte, ancorada em cadeia de custódia digital e de preservação digital ininterruptas.

A preservação digital sistêmica efetiva em RDC-Arq, portanto, emerge como uma prática compreensiva que abrange aspectos técnicos, organizacionais, legais e sociais. Esses elementos são fundamentais não apenas para manter o acesso contínuo, mas também para assegurar a preservação de longo prazo dos documentos arquivísticos digitais, garantindo que estes possam ser herdados pelas futuras gerações.

REFERÊNCIAS

AMBACHER, B.; CONRAD, M. Computational Archival Science is a Two-Way Street. *In*: IEEE INTERNATIONAL CONFERENCE ON BIG DATA (BIG DATA), 2021. **Anais** [...]. [*S. l.*]: IEEE, 2021. Disponível em: https://ai-collaboratory.net/wp-content/uploads/2021/11/1_Ambacher.pdf. Acesso em: 20 ago. 2024.

ANDRADE, F. L. DE; CHAGAS, C. A. Proposta de aperfeiçoamento do modelo conceitual para Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) para auditoria e certificação a partir da comparação com o modelo de critérios Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC). **ÁGORA:** Arquivologia em debate, Florianópolis, v. 31, n. 63, p. 1–19, jul./dez. 2021. Disponível em: https://agora.emnuvens.com.br/ra/article/view/1016/975. Acesso em: 20 ago. 2024.

ANDRADE, F. L. DE; CHAGAS, C. A. Repositórios digitais confiáveis: a verificação de compatibilidade entre modelos internacionais de critérios de preservação digital no longo prazo e o RDC-Arq. **ÁGORA:** Arquivologia em debate, Florianópolis, v. 33, n. 66, p. 1–22, jan./jun. 2023. Disponível em: https://agora.emnuvens.com.br/ra/article/view/1177. Acesso em: 20 ago. 2024.

BARBAU, R.; LUBELL, J.; RACHURI, S.; FOUFOU, S. Toward a reference architecture for archival systems. *In:* IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY, 10., 2013, Nantes. **Anais** [...] Nantes: IFIP, 2013. p. 68-77. DOI: 10.1007/978-3-642-41501-2_8. Disponível em: https://dl.ifip.org/hal-01461922v1. Acesso em: 20 ago. 2024.

BARBAU, R.; LUBELL, J.; RACHURI, S.; FOUFOU, S. Towards a reference architecture for archival systems: Use case with product data. **Journal of Computing and Information Science in Engineering**, [*S. l.*], v. 14, n. 3, 2014. Disponível em: https://asmedigitalcollection.asme.org/computingengineering/article-abstract/14/3/031005/371528/Towards-a-Reference-Architecture-for-Archival?redirectedFrom=fulltext. Acesso em: 20 ago. 2024.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARROS, D. B. S.; FERRER, I. D.; MAIA, C. M. DE S. Auditoria de repositórios digitais preserváveis. **Revista Ibero-Americana de Ciência da Informação**, Brasília, v. 11, n. 1, p. 300–313, jan./abr. 2018. DOI: 10.26512/rici.v11.n1.2018.8572. Disponível em: https://doi.org/10.26512/rici.v11.n1.2018.8572. Acesso em: 20 ago. 2024.

BRAGA, T. E. N.; HOLANDA, A. P.; CANELHAS, T. Resolução RDC-Arq Conarq: uma análise dos novos requisitos informacionais propostos. **Revista Brasileira de Preservação Digital**, Brasília, v. 3, p. 1–10, jul. 2022. DOI: 10.20396/rebpred.v3i00.16583. Disponível em: https://hipatia.ibict.br/publicacoes/resolucao-rdc-arq-conarq-uma-analise-dos-novos-requisitos-informacionais-propostos/. Acesso em: 20 ago. 2024.

CHAVES, E. M. L. Preservação de documentos arquivísticos digitais a longo prazo em repositórios digitais confiáveis. **Revista Ibero-Americana de Ciência da Informação**, Brasília, v. 16, n. 1, p. 50–66, jan./abr. 2023. DOI: 10.26512/rici.v16.n1.2023.44023. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/44023. Acesso em: 20 ago. 2024.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 39, de 29 de abril de 2014. Estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. **Diário Oficial da União**, Brasília-DF, 30 abr. 2014.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 43, de 04 de setembro de 2015. Altera a redação da Resolução do CONARQ nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. **Diário Oficial da União**, Brasília-DF, 8 set. 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). Resolução nº 51, de 25 de agosto de 2023. Dispõe sobre as "Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis", Versão 2. **Diário Oficial da União**, Brasília-DF, 12 dez. 2023.

CORRADO, E. M. Repositories, Trust, and the CoreTrustSeal. **Technical Services Quarterly**, [*S. l.*], v. 36, n. 1, p. 61–72, Feb. 2019. DOI: 10.1080/07317131.2018.1532055. Disponível em: https://www.tandfonline.com/doi/full/10.1080/07317131.2018.1532055. Acesso em: 20 ago. 2024.

DONALDSON, D. R. Certification information on trustworthy digital repository websites: A content analysis. **PLOS ONE**, San Francisco, v. 15, n. 12, p. 1-14, Dec. 2020. DOI: 10.1371/journal.pone.0242525. Disponível em:

https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0242525&type=printable. Acesso em: 20 ago. 2024.

FLORES, D.; PRADEBON, D. S.; CÉ, G. Análise do conhecimento teórico-metodológico da preservação digital sob a ótica da OAIS, SAAI, ISO 14721 e NBR 15472. **Brazilian Journal of Information Science: research trends**, Marília, v. 11, n. 4, p. 72–80, dez. 2017. DOI: 10.36311/1981-1640.2017.v11n4.11.p73. Disponível em: https://revistas.marilia.unesp.br/index.php/bjis/article/view/7511. Acesso em: 20 ago. 2024.

FRANK, R. D. Risk in trustworthy digital repository audit and certification. **Archival Science**, [*S. l.*], v. 22, n. 1, p. 43–73, Jul. 2022. DOI: 10.1007/s10502-021-09366-z. Disponível em: https://link.springer.com/article/10.1007/s10502-021-09366-z. Acesso em: 20 ago. 2024.

GAVA, T. B. S.; FLORES, D. O papel do Archivematica no RDC-Arq e possíveis cenários de uso. **ÁGORA:** Arquivologia em debate, Florianópolis, v. 31, n. 63, p. 1–21, jul./dez. 2021. Disponível em: https://agora.emnuvens.com.br/ra/article/view/1018. Acesso em: 20 ago. 2024.

GAVA, T. B. S.; FLORES, D. Políticas de Preservação Digital: o caso do Brasil em relação à Colômbia e Austrália. **Em Questão**, Porto Alegre, p. 1–26, jul./ago. 2022. DOI: 10.19132/1808-5245283.117999. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/117999. Acesso em: 20 ago. 2024.

GAVA, T. B. S.; FLORES, D. Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. **Informação & Informação**, Londrina, v. 25, n. 2, p. 74–99, abr./jun. 2020. DOI: 10.5433/1981-8920.2020v25n2p74. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/38411/0. Acesso em: 20 ago. 2024.

GOMES, W. DA S.; AUTRAN, M. DE M. M. Análise dos aspectos de confiabilidade do Repositório Digital Arquivístico Archivematica à luz da Resolução nº 43 do Conselho Nacional de Arquivos. **Ciência da Informação em Revista**, Maceió, v. 7, n. 1, p. 105–120, maio 2020. DOI: 10.28998/cirev.2020v7n1g. Disponível em: https://www.seer.ufal.br/index.php/cir/article/view/9859. Acesso em: 20 ago. 2024.

GONÇALEZ, P. R. V. A. Recomendações para certificação ou medição de confiabilidade de Repositórios Arquivísticos Digitas com ênfase no acesso à informação. **Informação & Informação**, Londrina, v. 22, n. 1, p. 215–241, jan./abr. 2017. DOI: 10.5433/1981-8920.2017v22n1p215. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/28777. Acesso em: 20 ago. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721**: Space data and information transfer systems - Open archival information system (OAIS) - Reference model. Geneva: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363:** Space data and information transfer systems — Audit and certification of trustworthy digital repositories. Geneva: ISO, 2012.

JANTZ, R.; GIARLO, M. Digital archiving and preservation: technologies and processes for a trusted repository. **Journal of Archival Organization**, [*S. l.*], v. 4, n. 1-2, p. 193-213, 2007. DOI: https://doi.org/10.1300/J201v04n01_10. Disponível em: https://www.tandfonline.com/doi/abs/10.1300/J201v04n01_10. Acesso em: 20 ago. 2024.

PIGLIAPOCO, S. Digital preservation in Italy. Reflections on models, criteria and solutions. **JLIS.it**, [*S. l.*], v. 10, n. 1, p. 1–11, jan. 2019. DOI: https://doi.org/10.4403/jlis.it-12521. Disponível em: https://www.jlis.it/index.php/jlis/article/view/80. Acesso em: 20 ago. 2024.

ROCHA, C. L. Repositórios para a preservação de documentos arquivísticos digitais. **Acervo**, Rio de Janeiro, v. 28, n. 2, p. 180–191, 27 nov. 2015. Disponível em: https://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/608. Acesso em: 20 ago. 2024.

SANTOS, H. M.; FLORES, D. Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 20, n. 2, p. 198–218, jun. 2015. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/23001. Acesso em: 20 ago. 2024.

SANTOS, H. M. Auditoria de repositórios arquivísticos digitais confiáveis. **Informação em Pauta**, Fortaleza, v. 4, n. 2, p. 156–172, 27 dez. 2019. DOI: https://doi.org/10.32810/2525-3468.ip.v4i2.2019.41787.156-172. Disponível em: http://www.periodicos.ufc.br/informacaoempauta/article/view/41787/99880. Acesso em: 20 ago. 2024.

SANTOS, H. M.; FLORES, D. Gestão de objetos no Repositório Arquivístico Digital Confiável: um diálogo com a ISO 16.363. **Páginas a&b:** arquivos e bibliotecas, Porto, v. 3, n. 13, p. 67–99, ago. 2020. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/6462. Acesso em: 20 ago. 2024.

SANTOS, H. M.; FLORES, D. Responsabilidades de um Repositório Arquivístico Digital Confiável na perspectiva do Open Archival Information System. **Páginas a&b:** arquivos e bibliotecas, Porto, v. 3, n. 11, p. 116–132, jul. 2019. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/5459. Acesso em: 20 ago. 2024.

SANTOS, H. M. DOS; FLORES, D. Transformações dos Pacotes de Informação na Cadeia de Custódia Digital Arquivística. **Páginas a&b: arquivos e bibliotecas**, Porto, v. 3, n. 18, p. 18–35, 27 dez. 2022. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/12540. Acesso em: 20 ago. 2024.

SCHUCH C. D. O. S.; SAAD, D. S.; FLORES D. Preservação digital na gestão de processos administrativos de uma instituição de ensino superior: o caso dos PEAPDs da PROGEP da UFSM. **Em Questão**, Porto Alegre, v. 25, n. 2, p. 229–255, 2019. DOI: 10.19132/1808-5245252.229-255. Disponível em: https://seer.ufrgs.br/index.php/EmQuestao/article/view/82597. Acesso em: 20 ago. 2024.

SHINTAKU, M.; BRAGA, T. E. N.; OLIVEIRA, A. DE F. Hipátia: uma ferramenta livre no apoio à preservação digital. **Revista Brasileira de Preservação Digital**, Brasília, v. 2, p. 1–35, 30 dez. 2021. DOI: https://doi.org/10.20396/rebpred.v2i00.15987. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/15987. Acesso em: 20 ago. 2024.

VARDIGAN, M.; WHITEMAN, C. ICPSR meets OAIS: Applying the OAIS reference model to the social science archive context. **Archival Science**, [*S. l.*], v. 7, n. 1, p. 73–87, 2007. DOI: 10.1007/s10502-006-9037-z. Disponível em: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/60440/Vardigan.Whiteman.Applying%20OAIS.pdf. Acesso em: 20 ago. 2024.

TRUSTWORTHY DIGITAL ARCHIVAL REPOSITORIES: CONCEPTS, STANDARDS AND TECHNOLOGIES

ABSTRACT

Objective: this study was to analyze publications related to the trustworthy digital archival repository, including its fundamental concepts within the context of archival records management, and the requirement specifications for its operation and reliability assessment. **Methodology:** was realizad a bibliographical research based on a systematic literature review, being papers retrieved from the Brapci, Scopus and Web of Science databases were selected, and themes inherent to trustworthy digital archival repositories were categorized using content analysis. **Results:** themes were identified about the characteristics of digital repositories, relating to trust and archival principles. They also identified models of requirements and standards for auditing and certification, as well as digital platforms for preserving archival records over time. **Conclusions:** for effective digital preservation in a trustworthy digital archival repository, it is necessary to adhere to consolidated standards, establish solid organizational policies, carry out frequent audits and obtain certifications that attest to its reliability. The integration of technology, institutional commitment and comprehensive records management is essential to ensure the long-term preservation and access to digital records for future generations.

Descriptors: Digital preservation. Digital repositories. Information model. Certification.

REPOSITORIOS DE ARCHIVOS DIGITALES CONFIABLES: CONCEPTOS, ESTÁNDARES Y TECNOLOGÍAS.

RESUMEN
Objetivo: este estudio consistió en analizar investigaciones relacionadas con repositorios de archivos digitales confiables, explorar sus conceptos fundamentales en el contexto de la gestión de documentos de archivo y examinar las especificaciones de requisitos para su operación y evaluación de confiabilidad. **Metodología:** se realizó una investigación bibliográfica basada en una revisión sistemática de la literatura, seleccionando 40 trabajos recuperados de las bases de datos Brapci, Scopus y Web of Science, y mediante análisis de contenido se categorizaron temas inherentes a repositorios archivísticos digitales confiables. **Resultados:** se identificaron temas relacionados con las características de los repositorios digitales, relacionados con la confianza y los principios de archivo. Se identificaron modelos de requisitos y estándares para auditoría y certificación, así como plataformas digitales para la preservación de documentos de archivo en el tiempo. **Conclusiones:** Para una preservación digital efectiva en un repositorio de archivos digitales confiable, es necesario cumplir con estándares consolidados, establecer políticas organizacionales sólidas, realizar auditorías frecuentes y obtener certificaciones que acrediten su confiabilidad. La integración de la tecnología, el compromiso institucional y la gestión documental integral es esencial para garantizar la preservación a largo plazo y el acceso a los documentos digitales para las generaciones futuras.

Descriptores: Preservación digital. Repositorios digitales. Modelo de información. Certificación.

Recebido em: 02.05.2024
Aceito em: 14.07.2024