Inf. Pauta Fortaleza, CE v. 4 n. 2 jul./dez. 2019 ISSN 2525-3468

DOI: https://doi.org/10.32810/2525-3468.ip.v4i2.2019.41787.156-172

ARTIGO DE REVISÃO

AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

AUDIT OF TRUSTWORTHY DIGITAL ARCHIVAL REPOSITORIES

Henrique Machado dos Santos[1]

[1] Bacharel em Arquivologia e mestre em Patrimônio Cultural pela Universidade Federal de Santa Maria (UFSM). Arquivista da Coordenação de Arquivo Geral da Universidade Federal do Rio Grande (FURG).
E-mail: henrique.hms.br@gmail.com

Conflito de interesses: O autor declara que não há conflito de interesses.

Financiamento: Não há.

Declaração de Disponibilidade dos dados: Todos os dados relevantes estão disponíveis neste artigo.

Recebido em: 07/08/2019.
Aceito em: 28/09/2019.
Revisado em: 15/11/2019.

Como citar este artigo:
SANTOS, Henrique Machado dos. Auditoria de repositórios arquivísticos digitais confiáveis. **Informação em Pauta**, Fortaleza, v. 4, n. 2, p. 156-172, jul./dez. 2019. DOI: 10.32810/2525-3468.ip.v4i2.2019.41787.156-172.

RESUMO

Este estudo discute a implementação de repositórios arquivísticos em conformidade com o Sistema Aberto para Arquivamento de Informação e a necessidade de auditá-los para avaliar sua confiabilidade. Para tanto, realiza-se um levantamento bibliográfico de materiais previamente publicados, com seleção de: livros que abordam as perspectivas da Arquivística na era digital e o desafio da custódia documental confiável; publicações técnicas como as normas *International Organization for Standardization* e padrões de auditoria; e artigos científicos recuperados pela ferramenta de pesquisa *Google Scholar*, com busca temática relacionada à preservação de documentos arquivísticos digitais, repositórios digitais confiáveis, auditoria de informação e auditoria arquivística. O repositório arquivístico é o prisma da discussão, já a comparação entre os padrões de auditoria torna-se a categoria norteadora, logo, obtém-se um artigo de revisão assistemática. Dessa forma, são analisados os padrões de auditoria: *Trustworthy Repository Audit & Certification: Criteria and Checklist*, *Catalogue of Criteria for Trusted Digital Repositories* da *Network of Expertise in long-term STORage*, *Digital Repository Audit Method Based on Risk Assessment* e *Audit and Certification of Trustworthy Digital Repositories*. Por fim, o comparativo entre os padrões demonstra que o *Audit and Certification of Trustworthy Digital Repositories* é o mais indicado para auditar os repositórios arquivísticos digitais.

Palavras-chave: Preservação digital. Repositório digital. Arquivística. Documento digital. Confiabilidade. Autenticidade.

ABSTRACT

This study discusses the implementation of archival repositories that conform to the Open Archival Information System and the need to audit them to assess their reliability. To this end, a bibliographic survey of previously published materials is carried out, with selection of: books that approach the perspectives of Archival science in the digital age and the challenge of reliable documentary custody; technical publications such as International Organization for Standardization and auditing standards; and scientific articles retrieved by the Google Scholar search tool, with thematic search related to the preservation of digital archival records, reliable

digital repositories, information auditing and archival auditing. The archival repository is the prism of the discussion, since the comparison between the audit standards becomes the guiding category, thus, we obtain a no systematic review article. Thus, the audit standards are analyzed: Trustworthy Repository Audit & Certification: Criteria and Checklist, Catalog of Criteria for Trusted Digital Repositories from Network of Expertise in long-term STORage, Digital Repository Audit Method Based on Risk Assessment and Audit and Certification of Trustworthy Digital Repositories. Finally, a comparison of standards demonstrates that the Audit and Certification of Trustworthy Digital Repositories is best suited for auditing digital archival repositories.

Keywords: Digital preservation. Digital repository. Digital record. Reliability. Authenticity.

1 INTRODUÇÃO

O *corpus* teórico da preservação digital vem agregando novas práticas recomendadas. Parte disso se deve aos avanços na área das tecnologias da informação e às discussões realizadas no âmbito da comunidade de preservação. As atividades que antes eram orientadas exclusivamente às estratégias, como por exemplo, emulação, migração e refrescamento, agora são orientadas aos sistemas para gestão e preservação de documentos.

Tal mudança surge em torno da necessidade de agregar confiança ao custodiador. Dessa forma, os sistemas informatizados e as políticas de preservação digital tornaram-se peças-chave para garantir o acesso contínuo em longo prazo a documentos arquivísticos autênticos.

A literatura técnica de preservação digital define o modelo *Open Archival Information System* (OAIS) como o principal padrão para implementar Repositórios Digitais Confiáveis (RDC), tornando-se a norma *International Organization for Standardization* (ISO) 14721:2012. Por sua vez, a norma OAIS foi traduzida para a língua portuguesa do Brasil, e consiste na recomendação ABNT/NBR 15472:2007, Sistema Aberto para Arquivamento de Informação (SAAI).

O modelo OAIS/SAAI foi desenvolvido no âmbito do *Consulative Committee for Space Data Systems* (CCSDS) e apresenta-se como a principal norma no âmbito da preservação digital. Este é um estudo de fundamentação sólida, que envolve diversos profissionais com propriedade no tema. De tal modo, a conformidade com o modelo OAIS permite ao Repositório Arquivístico Digital Confiável (RDC-Arq) desenvolver um sistema robusto para preservação da informação digital em longo prazo.

Embora o OAIS não faça claras menções à Arquivística/Arquivologia, observa-se que demonstra elevada conformidade com os pressupostos teóricos tradicionais como, por exemplo, os princípios da proveniência, organicidade e autenticidade. Logo, o OAIS preenche lacunas teóricas, que notadamente foram criadas pelo advento do documento arquivístico digital.

Essas lacunas relacionam-se à complexidade do próprio ambiente digital, visto que os referenciais tradicionais da Arquivística eram orientados aos documentos em suportes analógicos. Assim, o modelo OAIS possibilita tratamento adequado aos documentos arquivísticos, por considerar a complexidade da informação registrada em ambiente digital. Igualmente, surge a necessidade de definir uma política de preservação em nível organizacional para elencar as normas a serem utilizadas, além de manter conformidade com as especificidades da Arquivística.

A implementação de um RDC-Arq em conformidade com o modelo OAIS compreende o primeiro passo para a preservação de documentos arquivísticos digitais autênticos em longo prazo. Quando inseridos no OAIS, tais documentos são transportados em pacotes de informação: Pacote de Informação para Submissão (*Submission Information Package* – SIP), Pacote de Informação para Arquivamento (*Archival Information Package* – AIP) e Pacote de Informação para Disseminação (*Dissemination Information Package* – DIP) juntamente com os seus respectivos componentes digitais. Esse transporte compreende o ciclo de vida dos documentos, ou seja, desde o produtor, perpassando pelo RDC-Arq até chegar ao consumidor.

No entanto, mesmo em conformidade com o OAIS, os RDC-Arq's precisam ser auditados e certificados para demonstrar que cumprem os requisitos preconizados, e consequentemente, possam agregar confiabilidade ao acervo custodiado. Logo, a implementação de um RDC-Arq requer ir além de sua conformidade com o modelo OAIS. Tal fato é sedimentado na rápida evolução da Tecnologia da Informação e Comunicação (TIC), que aliada ao surgimento de documentos complexos, trouxe significativos desafios ante a preservação digital.

Sendo assim, um RDC-Arq deve manter conformidade com o modelo OAIS, comportar as especificidades da Arquivística, ser auditado periodicamente, para que possa demonstrar que é confiável. Considerando o exposto, este estudo tem por objetivo discutir a adequação de possíveis padrões de auditoria a serem utilizados para mensurar o nível de confiabilidade dos RDC-Arq's.

A metodologia consiste no levantamento bibliográfico de materiais previamente publicados, que contempla a seleção de livros, publicações técnicas e artigos científicos recuperados por meio da ferramenta de pesquisa *Google Scholar*. Com relação aos livros utilizam-se obras que abordam questões como: as perspectivas da Arquivística na era digital e a custódia de documentos em ambiente digital publicadas nos últimos cinco anos. Dentre as publicações técnicas destacam-se: normas ISO e padrões para auditoria de repositórios. Já os artigos recuperados partem dos seguintes termos: "preservação de documentos arquivísticos digitais", "repositórios digitais confiáveis", "auditoria de informação", e "auditoria arquivística"; todas as buscas com a delimitação temporal de dez anos (2009-2019) e foram escolhidas a partir da análise dos respectivos resumos.

O RDC-Arq é utilizado como prisma da discussão, de modo que o estudo de possíveis padrões de auditoria para mensurar o seu nível de confiabilidade, torna-se a categoria norteadora desta pesquisa. Os dados coletados são analisados pelo método qualitativo e a discussão dos resultados segue a lógica dedutiva, de modo que se realiza uma triangulação entre a Arquivística, o modelo OAIS e os padrões de auditoria. Após tal reflexão, obtém-se um artigo de revisão com caráter assistemático (GIL, 2010; LUNA, 1997; SILVA; MENEZES, 2005; VOLPATO *et al*., 2013).

2 DA NECESSIDADE DE UM SISTEMA DE ARQUIVOS INTEROPERÁVEL

A literatura técnica da preservação digital perpassa questões essenciais como, por exemplo, as estratégias, os repositórios, a custódia confiável e a auditoria e certificação de repositórios digitais. Logo, existe a necessidade de aproximar essas abordagens da Arquivística, a qual está inserida em um contexto de reformulação epistemológica e pragmática.

A documentação em ambiente digital catalisa um processo de (re)definição dos princípios teórico-práticos, e assim, reforça a quebra do paradigma arquivístico, essencialmente analógico e custodial. As transformações sobre os registros contemporâneos se refletem diretamente na concepção de patrimônio, de modo a identificar e incorporar o patrimônio em ambiente digital. Desta forma, surge a necessidade de preservar documentos arquivísticos digitais para que possam ser utilizados como fontes de pesquisa e informação do futuro.

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

A fragilidade dos documentos arquivísticos em ambiente digital implica na necessidade de implementar um sistema de arquivos que contemplem desde a produção documental; perpassando a destinação final; a preservação de longo prazo; e promovendo o acesso contínuo aos conteúdos preservados. Dessa forma, os ambientes de gestão e preservação devem ser geridos por sistemas informatizados que contemplem as complexidades informáticas e as especificidades da Arquivística.

Inicialmente, a implementação de um sistema de arquivos irá envolver a conformidade com leis, decretos, portarias, resoluções do Conselho Nacional de Arquivos (Conarq), diretrizes do projeto *The International Research on Permanent Authentic Records in Electronic Systems* (InterPARES), normas ISO e a conformidade com padrões como o *Model Requirements for the Management of Electronic Records* (MoReq) (KANTORSKI; KROTH, 2015). No que tange ao ambiente de gestão documental, ressalta-se a pertinência de se implementar um Sistema Informatizado para Gestão Arquivística de Documentos (SIGAD).

Observa-se que o SIGAD consiste em um conjunto de procedimentos e operações técnicas, dotado de características arquivísticas e processado via computador. Portanto, poderá compreender um *software* exclusivo, um conjunto de *softwares* (integrados, adquiridos ou desenvolvidos) ou ser uma combinação de ambos. O êxito do SIGAD está relacionado à implementação *a priori* de uma política de gestão para documentos arquivísticos (BRASIL, 2011).

Com isso, o SIGAD pode ser desenvolvido nos moldes do MoReq ou do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq). Logo, o SIGAD será responsável pela tramitação, manutenção da autenticidade e destinação final dos documentos em fase corrente e intermediária, os quais serão armazenados em uma base de dados.

O e-ARQ Brasil enumera requisitos mínimos para um SIGAD, indiferente da plataforma tecnológica na qual for implementado. Desse modo, é possível especificar todas as atividades e operações técnicas envolvidas no processo de gestão documental,

incorporando assim, a produção, a tramitação, o uso e sua destinação final. Portanto, um SIGAD em conformidade com o e-Arq elevará o nível de confiabilidade e possibilitará acesso a documentos arquivísticos autênticos (BRASIL, 2011).

Já o MoReq fornece um conjunto de requisitos abrangente e simples, de fácil compreensão, voltado para um sistema de registros, de modo que seja adaptável e aplicável para atividades de negócios, setores industriais e diversos tipos de organizações. O MoReq define um conjunto comum de serviços básicos que são compartilhados por diferentes tipos de sistema de registros, que também são modulares e flexíveis, possibilitando a sua incorporação em aplicativos especializados e dedicados, os quais podem não ter sido previamente reconhecidos como sistemas de registros (DLM, 2010).

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

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

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

Após cumprir o respectivo prazo de guarda, os documentos armazenados nos sistemas de gestão serão submetidos ao processo de avaliação. Parte desses documentos será eliminada, com base nos prazos de guarda de uma tabela de temporalidade e destinação de documentos; e outra parte, dotada de valor permanente, será recolhida ao RDC-Arq.

O RDC-Arq será o ambiente confiável para preservação de longo prazo, no qual será realizada a maioria das atividades de preservação digital. No entanto, é preciso comprovar que o RDC-Arq cumpre os requisitos da Arquivística, bem como os relacionados à confiabilidade, que são enumerados pelo OAIS.

Ressalta-se que o modelo OAIS preconiza funções de preservação que incluem: admissão, armazenamento arquivístico, gerenciamento de dados, acesso e disseminação. Ademais, aborda a migração das informações digitais para novos suportes e formatos de arquivo, bem como, os modelos utilizados para representar a informação, a função do *software* na preservação de informação e a interoperabilidade entre os arquivos (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012).

Os documentos em ambiente digital necessitam de um conjunto de informações para representar corretamente o seu conteúdo, demonstrando a característica de recursividade. Assim, o modelo lógico da informação arquivada, proposto pelo OAIS, permite identificar e adicionar os componentes necessários para obter a correta representação/interpretação dos documentos. A informação adicional irá contribuir para a presunção de autenticidade, pois identifica o seu histórico de custódia e as modificações realizadas. Além disso, podem-se vincular informações que irão auxiliar na preservação dos documentos, identificar o seu armazenamento e descrever o seu conteúdo para facilitar o processo de busca e recuperação das informações.

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

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

Logo, é possível implementar um ambiente de preservação confiável, devendo-se estabelecer uma cadeia de custódia ininterrupta na relação interoperável entre o SIGAD e o RDC-Arq e considerar: os modelos e-Arq, MoReq e OAIS, os princípios arquivísticos (proveniência, autenticidade, naturalidade, organicidade e unicidade), a necessidade de auditoria, a legislação vigente, as diretrizes do Conarq, os estudos pertinentes sobre o tema e as demais normas ISO relacionadas à informação e documentação.

Posteriormente, a plataforma de acesso surge como complemento ao sistema de preservação, que irá fornecer meios para atingir os objetivos de um sistema de arquivos: preservar e garantir acesso contínuo em longo prazo.

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

3 ADICIONANDO CONFIANÇA POR INTERMÉDIO DA AUDITORIA

A auditoria consiste em um processo executado de forma independente, conforme uma sistemática, o qual é documentado para se obter evidências objetivas, ou seja, dados que sustentam a existência ou veracidade de determinado fato. Tais evidências podem ser avaliadas de forma objetiva para determinar o nível de conformidade com os critérios de auditoria (ABNT/NBR/ISO 19011:2018).

A partir desses critérios, podem-se identificar funções e atividades executadas em um determinado período com produção de resultados. Tradicionalmente, o conceito de auditoria está relacionado às funções de controle (OLIVEIRA; BATISTA, 2019). Ressalta-se que a auditoria tornou-se necessária em virtude da complexidade das organizações, de modo que ela busca evidenciar a conformidade das ações com um comportamento organizacional entendido como adequado.

Com relação ao termo “auditoria de informação” a literatura aponta que seu aspeto central consiste no estudo de todo o ciclo de vida da informação, de modo que comporta: produção, tramitação, necessidades e usos da informação; além do custo e do valor atribuído às informações de uma organização. Nesse contexto, a auditoria de informação está diretamente relacionada com a avaliação da qualidade dos serviços e ao planeamento estratégico da organização (PESTANA, 2014).

Já o termo "auditoria arquivística" abarca a avaliação dos procedimentos que são utilizados em todo o ciclo de vida dos documentos arquivísticos. Isso comporta desde a produção até a sua guarda permanente e acesso, em consonância com o embasamento legal e teórico da disciplina arquivística. Em caráter complementar, podem-se monitorar as ações, bem como fazer análises de cunho crítico e enumerar sugestões (OLIVEIRA; BATISTA, 2019).

Destaca-se que a auditoria, que tradicionalmente esteve relacionada às atividades de gestão, tem novas perspectivas, que podem ser observadas nos conceitos de "auditoria da informação" e "auditoria arquivística". O enfoque dado a todo o ciclo de vida documental reforça a implementação de RDC-Arq's capazes de salvaguardar a documentação em longo prazo e garantir o acesso.

A constante evolução das TIC's e a consequente demanda por documentos digitais estimula a implementação de repositórios digitais para garantir o acesso contínuo em longo prazo. Da mesma forma, ainda não há a confiança esperada pela comunidade designada e pelos usuários potenciais. Assim, estima-se que tal confiança seja atingida com procedimentos periódicos de auditoria e certificação, bem como por meio da divulgação dos métodos de preservação empregados pelo custodiador do acervo. Logo, a auditoria de RDC-Arq's se enquadra no escopo da auditoria arquivística.

O processo de auditoria torna-se essencial para demonstrar que um RDC-Arq está em conformidade com o modelo OAIS e que segue princípios da Arquivística. Por meio de auditorias periódicas, será possível verificar as vulnerabilidades dos repositórios e o cumprimento das políticas de preservação a fim de buscar soluções que elevem os níveis de confiabilidade. Posteriormente, as atividades de certificação constituem em um complemento frente à auditoria, para demonstrar que um determinado RDC-Arq atingiu os níveis de confiabilidade necessários, e poderá ser considerado "confiável".

Tendo em vista o exposto, observa-se que as atividades de auditoria e certificação são fundamentais para adicionar confiabilidade às organizações que fazem a custódia de documentos arquivísticos digitais. Ressalta-se a sua ligação com a gestão de documentos, assim como a necessidade de manter uma cadeia de custódia documental ininterrupta, entre o SIGAD e o RDC-Arq, a fim de gerar confiabilidade.

A questão da confiabilidade não se limita, tão somente, ao ambiente de preservação documental. Portanto, deve ser pensada desde o momento da produção documental, de modo a incluir metadados que corroborem com a presunção de

autenticidade. Além disso, o sistema responsável pelos documentos em fases corrente e intermediária, doravante SIGAD, deverá possuir os requisitos necessários para mantê-los autênticos até o momento da avaliação e consequente recolhimento ao RDC-Arq.

Após o recolhimento, compete ao RDC-Arq a responsabilidade de preservar documentos autênticos e mantê-los acessíveis no longo prazo. Para tanto, isso requer que o RDC-Arq demonstre o compromisso com a preservação tendo em vista que deverá atender as necessidades de sua comunidade designada. Com isso, o processo de auditoria e certificação torna-se essencial para reafirmar tal compromisso com a preservação.

4 PADRÕES PARA AUDITAR REPOSITÓRIOS DIGITAIS

No âmbito da auditoria de repositórios digitais, observa-se que há iniciativas pertinentes, dentre elas: *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC), *Catalogue of Criteria for Trusted Digital Repositories* da *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). Tais estudos visam orientar os preservadores em relação aos requisitos que um RDC deverá cumprir no processo de auditoria.

4.1 TRAC: o estudo pioneiro

Em 2003, o *Research Libraries Group* (RLG) e o *National Archives and Records Administration* (NARA) uniram esforços para criar uma força-tarefa, a RLG-NARA, com o objetivo de certificar repositórios digitais. Para tanto, tal parceria desenvolveu critérios para identificar os RDC capazes de fornecer acesso à informação digital no longo prazo. Dessa forma, os critérios produzidos visavam orientar o processo de certificação, com intuito de contemplar repositórios de arquivos, bibliotecas e outros serviços de armazenamento digital (RLG/NARA, 2007).

Esse padrão oferece ferramentas para auditoria, avaliação e certificação potencial dos repositórios. O TRAC estabelece a documentação que será exigida para realizar a auditoria, contemplando assim, questões como, por exemplo, os contratos, as licenças, as políticas de preservação, o planejamento e os planos de sucessão. Além disso, o TRAC

estabelece metodologias para determinar a perspectiva de sustentabilidade dos repositórios digitais (SAYÃO, 2010).

O TRAC tem o objetivo de identificar, em consonância com seus critérios, os repositórios digitais com capacidade de armazenamento, migração confiável e garantia de acesso aos documentos digitais. Seu principal desafio consistiu em produzir e esquematizar um processo genérico para auditar e certificar repositórios digitais (RLG/NARA, 2007). Os critérios do TRAC são divididos em três seções, que são: infraestrutura organizacional, gerenciamento de objetos digitais e tecnologias, infraestrutura técnica e segurança.

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

4.2 NESTOR: uma alternativa possível

A primeira versão do NESTOR foi publicada em dezembro de 2006 pelo *Working Group Trusted Repositories – Certification* com objetivo inicial de ser implementado na Alemanha. No entanto, o NESTOR já é discutido internacionalmente, e posteriormente, em novembro de 2009, teve sua segunda versão publicada.

O NESTOR consiste em um catálogo de critérios que são destinados, principalmente, para as organizações que tem o compromisso de preservar a memória, como, por exemplo, arquivos, bibliotecas e museus. Dessa forma, o NESTOR orienta a elaboração, o planejamento e a implementação de um RDC no longo prazo. Ademais, fornece orientações no que se refere à administração de arquivos, prestação de serviços comerciais e não comerciais, bem como, aos serviços de terceiros (NESTOR, 2009).

O objetivo deste catálogo é formular critérios que possam ser utilizados em uma ampla gama de repositórios digitais, além de manter-se válido por um longo período. Supõe-se a necessidade de optar por critérios relativamente abstratos (NESTOR, 2009).

Tais critérios acompanhados por explicações exaustivas e de exemplos em diferentes áreas.

O NESTOR oferece uma breve introdução que perpassa os problemas em torno da preservação da informação digital em longo prazo. Assim, descreve os principais conceitos e os princípios que sustentam seus critérios. Posteriormente, são apresentados os critérios em sua forma integral. Por fim, tem-se um *checklist*, que consiste em uma visão compacta do catálogo, além do glossário.

4.3 DRAMBORA: autoavaliação de riscos

O DRAMBORA surgiu a partir do trabalho conjunto realizado entre *Digital Curation Centre* (DCC) e *DigitalPreservationEurope* (DPE), formando assim, o grupo DCC/DPE. Inicialmente, o trabalho do grupo DCC/DPE teve como objetivo proporcionar uma abordagem complementar em associação com os esforços dos projetos TRAC e NESTOR.

Para tanto, o DRAMBORA apresenta um conjunto de ferramentas para auditar repositórios digitais, e se destina em facilitar a auditoria interna. Dessa forma, oferece aos administradores do repositório, a possibilidade de avaliá-los, e assim, identificar suas vulnerabilidades e potencialidades (DCC/DPE, 2007).

Dessa forma, em um primeiro momento, procede-se a auditoria interna com o DRAMBORA para identificar e mitigar os riscos; e posteriormente, executa-se a auditoria externa com, por exemplo, TRAC, NESTOR ou ACTDR, para então avaliar o repositório e certificá-lo como "confiável", caso atinja os níveis desejados.

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

Tal processo prepara as organizações para atenderem aos requisitos de avaliação subsequente, ou seja, a auditoria externa. Logo, realizar a auditoria interna com o DRAMBORA equivalente a um trabalho preparatório a fim de qualificar o repositório para a auditoria externa. Além disso, os resultados obtidos com o DRAMBORA podem

fornecer evidências aos auditores externos, demonstrando assim, compromisso com a preservação de longo prazo (DCC/DPE, 2007).

4.4 ACTDR: o surgimento de uma norma ISO

O ACTDR define um conjunto de práticas recomendadas orientadas ao modelo OAIS a fim de fundamentar o processo de auditoria e certificação. Sendo assim, é destinado, principalmente, aos administradores de repositórios e demais profissionais que prestam serviços de auditoria. Logo, o ACTDR visa mensurar os níveis de confiabilidade dos repositórios digitais (CCSDS, 2011; ISO 16363:2012).

Com o ACTDR é possível avaliar o repositório digital no que tange à sua infraestrutura organizacional, sustentabilidade financeira, gerenciamento dos objetos digitais e gestão de riscos. O padrão ACTDR segue essencialmente a base do TRAC, sendo composto por três seções primárias: infraestrutura organizacional, gestão de objetos digitais e infraestrutura de segurança da gestão de riscos.

Ademais, o ACTDR tem por objetivo realizar um processo contínuo de auditoria, julgando as áreas que necessitam ser melhoradas. O *status* de confiança não é atingido uma única vez, logo, será necessário manter um ciclo regular de auditoria e certificação, para que assim, possa ser demonstrada. Como consequência, a divulgação dos resultados da auditoria ao público geral irá elevar a confiança no repositório (CCSDS, 2011; ISO 16363:2012). Posteriormente, o ACTDR tornou-se a norma ISO 16363:2012, firmando-se como o principal padrão para auditoria de RDC's.

5 COMPARATIVO ENTRE OS PADRÕES DE AUDITORIA

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

O primeiro padrão a surgir foi TRAC o qual foi desenvolvido e revisado pela força-tarefa RLG-NARA até 2007, quando é publicada a sua versão final. Este estudo é continuado no ACTDR situado no âmbito do CCSDS. Dessa forma, o ACTDR torna-se o

sucessor/substituto dos critérios do TRAC em virtude de sua descontinuidade. Os avanços dos estudos em preservação digital farão com que o TRAC torne-se ultrapassado com os anos, visto que o conteúdo deste documento é definitivo.

O ACTDR é a continuidade do TRAC, e logo, em 2012 tornou-se a ISO 16363:2012. Ressalta-se que no âmbito do CCSDS, o ACTDR está inserido em um processo de constante revisão, o que reforça a sua pertinência. Além disso, enquanto norma ISO o documento também estará sujeito às revisões realizadas/solicitadas pelo comitê da ISO.

Já o NESTOR, traz uma proposta inicial para ser implementado na Alemanha, se limitando de certa forma, a um determinado contexto geopolítico. Posteriormente o projeto ganhou relevância sendo aplicado fora desse país, com uma tendência de assumir caráter genérico em seus requisitos, não se limitando, tão somente, à realidade alemã. O NESTOR é um estudo promissor que influenciou e foi influenciado por outros padrões como o TRAC e DRAMBORA, entretanto ainda carece de reconhecimento enquanto norma ISO.

Em um comparativo com os demais padrões para auditoria, o DRAMBORA diferencia-se por se tratar de um padrão indicado para auditoria interna. No entanto, isso não minimiza a sua pertinência, visto que apresenta uma série de requisitos pertinentes para mitigar riscos. Dessa forma, o DRAMBORA pode ser implementado objetivando uma auditoria posterior com ACTDR ou NESTOR.

6 CONSIDERAÇÕES FINAIS

Neste estudo, observou-se que a preservação de documentos arquivísticos em ambiente digital necessita de intervenção humana para mantê-los autênticos e acessíveis no longo prazo. Para tanto, recorre-se à implementação de políticas, estratégias e sistemas informatizados para gestão, preservação e acesso. Ou seja, um SIGAD para gerir os documentos nas fases corrente e intermediária e um RDC-Arq para gerir a fase permanente e promover o acesso.

Reitera-se que o SIGAD deve ser desenvolvido nos moldes de estudos sedimentados como, por exemplo, o MoReq e o e-Arq Brasil. Já o RDC-Arq, impreterivelmente, deverá seguir o modelo OAIS, ademais, precisa demonstrar que tem

capacidade de preservar documentos autênticos no longo prazo, obtendo assim, um *status* de confiável.

Para que um RDC-Arq seja de fato, certificado com "confiável", torna-se necessário realizar o processo de auditoria por meio de padrões como, por exemplo, TRAC, NESTOR, DRAMBORA e ACTDR. Estes padrões possuem uma série de procedimentos para mensurar os níveis de confiabilidade. Após o processo de auditoria, deve-se proceder a certificação por órgão competente, a fim de comprovar a confiabilidade do RDC-Arq.

Tendo em vista a descontinuidade do TRAC, a limitação (auditoria interna) do DRAMBORA e a incipiência (ausência de reconhecimento ISO) do NESTOR, pondera-se que o ACTDR consiste no principal padrão para auditoria externa, configurando-se, inclusive, como ISO 16363:2012. Com isso, preconiza-se a implementação de um RDC-Arq que siga o modelo OAIS, seja auditado periodicamente com o ACTDR. Além disso, o RDC-Arq deve respeitar os princípios da Arquivística.

Portanto, manter a confiabilidade de um RDC-Arq requer a manutenção de sistemas informatizados para gestão, preservação e acesso; envolvidos em uma linha de custódia ininterrupta. Tais sistemas serão responsáveis por assegurar os princípios da proveniência, autenticidade, naturalidade, organicidade e unicidade. Dessa forma, o ciclo de vida dos documentos deverá comportar as especificidades do documento arquivístico e as complexidades do ambiente digital.

Por fim, este estudo fornece subsídios teóricos aos profissionais de arquivo para facilitar a compreensão do processo de auditoria. Estima-se que assim seja possível incentivar o diálogo em torno dos RDC-Arq's, visto que há vasta literatura sobre "repositórios digitais" (sentido genérico do termo), ao passo que a especificidade "repositório arquivístico" ainda carece de literatura própria. Observa-se que tanto o OAIS, quanto os padrões de auditoria possuem uma linguagem direcionada aos profissionais da informática e administradores de RDC's. Logo, tornam-se necessárias adaptações para situar-lhes no âmbito da Arquivística.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 15472**: Sistemas espaciais de dados e informações – Modelo de referência para um sistema aberto de arquivamento de informação (SAAI). Rio de Janeiro: ABNT, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 19011**: Diretrizes para auditoria de sistemas de gestão. Rio de Janeiro: ABNT, 2018.

BARRETO, A. A. Os documentos de amanhã: a metáfora, a escrita e a leitura nas narrativas em formato digital. **DataGramaZero**, v. 10, n. 1, 2009, Rio de Janeiro. Disponível em: http://ridi.ibict.br/handle/123456789/159. Acesso em: 19 dez. 2017.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: http://www.siga.arquivonacional.gov.br/images/publicacoes/e-arq.pdf. Acesso em: 05 ago. 2014.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM. **Audit and Certification of Trustworthy Digital Repositories (ACTDR)**. Magenta Book. Washington, Sep. 2011. Disponível em: http://public.ccsds.org/publications/archive/652x0m1.pdf. Acesso em: 13 nov. 2018.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM. **Reference Model for an Open Archival Information System (OAIS)**. Magenta Book. Washington, Jun. 2012. Disponível em: https://public.ccsds.org/pubs/650x0m2.pdf. Acesso em: 13 maio 2014.

DIGITAL CURATION CENTRE; DIGITAL PRESERVATION EUROPE (DCC/DPE). **Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)**. v. 1.0, fev. 2007. Disponível em: http://www.repositoryaudit.eu/download. Acesso em: 13 nov. 2014.

DOCUMENT LIFECYCLE MANAGEMENT (DLM). Forum Foundation. **The European Commission**: 2010. Disponível em: http://moreq.info/files/moreq2010_vol1_v1_1_en.pdf. Acesso em: 27 mai. 2018.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2010.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721**: Space data and information transfer systems: open archival information system – Reference model. Genebra, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363**: Space data and information transfer systems: audit and certification of trustworthy digital. Genebra, 2012.

KANTORSKI, G.; KROTH, M. Proposta de informatização da gestão, preservação e acesso a documentos arquivísticos de uma instituição de ensino superior. *In*: COLÓQUIO INTERNACIONAL DE GESTÃO UNIVERSITÁRIA, 15., 2015, Argentina. **Anais eletrônicos** [...]. Argentina, 2015. Disponível em: https://repositorio.ufsc.br/xmlui/handle/123456789/136155. Acesso em: 20 fev. 2018.

LUNA, S. V. **Planejamento de pesquisa**: uma introdução. São Paulo: EDUC, 1997.

LUZ, C. **Primitivos digitais**: uma abordagem arquivística. Salvador: 9Bravos, 2015.

NETWORK OF EXPERTISE IN LONG-TERM STORAGE. Nestor Working Group on Trusted Repositories Certification: Catalogue of Criteria for Trusted Digital Repositories, Version 2. Frankfurt am Main: 2009. Nestor c/o Deutsche Nationalbibliothek. Disponível em: http://files.dnb.de/nestor/materialien/nestor_mat_08_eng.pdf. Acesso em: 20 jul. 2019.

OLIVEIRA, E. B.; BATISTA, D. A. Auditoria arquivística: uma proposta de requisitos. **Informação & Sociedade**: Estudos, v. 29, n. 1, 2019. Disponível em: http://dx.doi.org/10.22478/ufpb.1809-4783.2019v29n1.44006. Acesso em: 24 set. 2019.

PESTANA, O. Auditoria de informação: definição e evolução da atividade no contexto da gestão da informação e das

organizações. **Páginas A&B**: Arquivos e Bibliotecas, Portugal, n. 2, p. 49-64, 2014. Disponível em: http://ojs.letras.up.pt/index.php/paginasaeb/article/view/599/579. Acesso em: 25 set. 2019.

RESEARCH LIBRARIES GROUP; U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. **Trustworthy Repositories Audit & Certification**. RLG, OCLC, Feb. 2007. Disponível em: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf. Acesso em: 08 set. 2014.

SANTOS, H. M.; FLORES, D. Os impactos da obsolescência tecnológica frente à preservação de documentos digitais. **Brazilian Journal of Information Science**, Marília, v. 11, n. 2, p. 28-37, 2017. Disponível em: http://www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5550/4511. Acesso em: 25 maio 2018.

SILVA, M. **O arquivo e o lugar**: custódia arquivística e a responsabilidade pela proteção aos arquivos. Niterói: EdUFF, 2016. (Série Nova Biblioteca, 17).

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005. Disponível em: https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf. Acesso em: 13 jun. 2014.

SAYÃO, L. F. Repositórios digitais confiáveis para a preservação de periódicos eletrônicos científicos. **Ponto de Acesso**, Salvador, v. 4, n. 3, p. 68-94, dez. 2010. Disponível em: http://www.portalseer.ufba.br/index.php/revistaici/article/view/4709. Acesso em: 08 ago. 2014.

VOLPATO, G. L.; BARRETO, R. E.; UENO, H. M.; VOLPATO, E. D. S. N.; GIAQUINTO, P. C.; FREITAS, E. G. D. **Dicionário crítico para redação científica**. Botucatu: Best Writing, 2013.