

# REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS (RDC-ARQ) COMO PLATAFORMA DE PRESERVAÇÃO DIGITAL EM UM AMBIENTE DE GESTÃO ARQUIVÍSTICA

## TRUSTED DIGITAL ARCHIVAL REPOSITORIES (TDAR) AS DIGITAL PRESERVATION SYSTEM IN A ARCHIVAL MANAGEMENT ENVIRONMENT

Tânia Barbosa Salles Gava<sup>a</sup>

Daniel Flores<sup>b</sup>

### RESUMO

**Introdução:** Em um ambiente digital houve a necessidade de se repensar a garantia da cadeia de custódia ininterrupta, e como mantê-lo como um lugar de gestão arquivística, preservação permanente, custódia confiável, e como um arquivo permanente digital, motivado pela Lei 8159/91, que coloca como dever público a gestão dos documentos de arquivo, visando a sua eliminação ou recolhimento para guarda permanente. **Objetivo:** Apresentar os Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) como uma alternativa para a preservação digital em um ambiente de gestão arquivística, a fim de manter os documentos arquivísticos digitais autênticos e acessíveis a longo prazo. **Metodologia:** Pesquisa exploratória, bibliográfica e documental, tendo como principais fontes documentais e bibliográficas o material resultante das fases do Projeto InterPARES, as normativas do Conselho Nacional de Arquivos e artigos científicos de pesquisadores nacionais e internacionais. **Resultados:** Apresentação e Discussão dos principais conceitos relacionados aos Repositórios Arquivísticos Digitais Confiáveis tais como repositórios digitais, repositórios arquivísticos digitais, repositórios digitais confiáveis, cadeia de custódia digital arquivística e cadeia de preservação. **Conclusões:** É necessário olhar para o RDC-Arq, ou seja, para o Arquivo Permanente digital, como o lugar necessário e obrigatório perante a Lei 8159/91 para os documentos históricos/permanentes, e o lugar onde são implementados os referenciais consolidados e atuais de uma Preservação Digital Sistemática.

**Descritores:** Arquivologia. Repositórios Arquivísticos Digitais. Preservação Digital.

---

<sup>a</sup> Doutora em Engenharia Elétrica - Automação, na área de Inteligência Artificial Aplicada pelo PPGEE da Universidade Federal do Espírito Santo (UFES). Professora do Departamento de Arquivologia da Universidade Federal do Espírito Santo (UFES). E-mail: tania.gava@ufes.br

<sup>b</sup> Doutor em Ciência da Informação pela Universidade Federal do Rio de Janeiro (UFRJ). Professor do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal Fluminense (PPGCI-UFF). E-mail: danielflores.arquivologia@gmail.com

## 1 INTRODUÇÃO

A partir da década de 1990, principalmente pelo advento da Internet, começaram a ocorrer mudanças consideráveis na sociedade. Essa fantástica ferramenta começou a mudar de forma radical a forma das pessoas se comunicarem e compartilharem informações. Nesse sentido, toda a documentação gerada, no sentido arquivístico da palavra, considerando a documentação como um “conjunto de unidade de registro de informações, qualquer que seja o suporte ou formato” (ARQUIVO NACIONAL, 2005, p. 72), que antes era majoritariamente em suporte papel, começou a ser gerada em ou migrada para o formato eletrônico. Dessa forma, os documentos eletrônicos, que são todo “Gênero documental integrado por documentos em meio eletrônico ou somente acessíveis por equipamentos eletrônicos, como cartões perfurados, disquetes e documentos digitais” (ARQUIVO NACIONAL, 2005, p. 75) começaram a surgir com mais frequência.

Embora o documento digital seja um tipo de documento eletrônico, eles não são a mesma coisa. Um documento digital diz respeito a todo “documento codificado em dígitos binários, acessível por meio de sistema computacional” (ARQUIVO NACIONAL, 2005, p. 75). Por essa definição, pode-se entender porque os documentos digitais passaram a ser gerados de forma intensa após a década de 1990, que além da popularização da Internet, teve uma maior popularização dos sistemas computacionais. Consequentemente, os documentos arquivísticos digitais, que nada mais são do que documentos arquivísticos em formato digital, produzidos no decorrer de uma atividade prática como instrumento ou resultado dessa atividade, começaram a surgir cada vez com mais frequência. Neste período sua utilização estava relacionada ao uso de sistemas de informação digitais que registravam documentos e informação para a tomada de decisão. Esses documentos eram, então, impressos, assinados e preservados em suporte papel.

Embora os documentos digitais possuam uma grande facilidade em relação à sua criação, acesso e compartilhamento, eles trazem consigo muitas vulnerabilidades, ligadas principalmente a sua rápida degradação física,

obsolescência tecnológica, complexidade e alto custo relacionado à preservação a longo prazo (SANTOS; FLORES, 2015). Essas vulnerabilidades do documento digital, mais especificamente dos documentos arquivísticos digitais, trazem uma preocupação em relação a um tema complexo, e altamente custoso: a preservação digital. Além disso, em um ambiente digital houve a necessidade de se repensar a garantia da cadeia de custódia ininterrupta, e como mantê-lo como um lugar de gestão arquivística, preservação permanente, custódia confiável, e como um arquivo permanente digital, motivado pela Lei 8159/91 (BRASIL, 1991) que coloca como dever público a gestão dos documentos de arquivo, visando a sua eliminação ou recolhimento para guarda permanente.

Diante deste cenário, este artigo tem como objetivo apresentar os Repositórios Arquivísticos Digitais Confiáveis como uma plataforma de preservação digital em um ambiente de gestão arquivística, a fim de manter os documentos arquivísticos digitais autênticos e acessíveis a longo prazo. Mais do que isso, este artigo busca esclarecer muitos conceitos envolvidos nesse tema, ainda desconhecidos ou mal compreendidos.

Trata-se de uma pesquisa exploratória, uma vez que teve como objetivo proporcionar uma maior familiaridade com temas relacionados aos repositórios arquivísticos digitais confiáveis, com vistas a torná-los mais explícitos, como também o aprimoramento de conceitos. A pesquisa também se caracteriza como bibliográfica e documental. A pesquisa bibliográfica é “desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos” (GIL, 2002, p. 44). Já a pesquisa documental assemelha-se muito à pesquisa bibliográfica, no entanto suas fontes são muito mais diversificadas e dispersas. (GIL, 2002). Em relação aos procedimentos metodológicos, foi feita uma pesquisa tendo como principais fontes documentais e bibliográficas o material resultante das fases do Projeto InterPARES, as normativas do Conselho Nacional de Arquivos (Conarq) e artigos científicos de pesquisadores nacionais e internacionais, especialistas nos temas relativos a este trabalho.

## 2 REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Preocupados com o patrimônio arquivístico digital, crescente cada vez mais a partir da década de 1990, que já se encontrava em perigo de desaparecimento e de falta de confiabilidade por causa das fragilidades do formato digital, e com o fato de que sua preservação traria benefícios para gerações futuras, foi publicada em 2005, pelo Conarq, a Carta para a Preservação do Patrimônio Digital da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO). A Carta manifestava a necessidade dos Estados-membros, incluindo o Brasil, estabelecerem políticas e ações para a proteção do patrimônio digital (CONARQ, 2005). Essa preocupação refletia-se ao redor do mundo, no entanto no Brasil a Carta deu início a uma série de publicações técnicas do Conarq sobre o tema. A principal dessas publicações é a Resolução n.º 43 (CONARQ, 2015a), que altera a redação da Resolução do CONARQ n.º 39, de 29 de abril de 2014, e que 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, visando a preservação do Patrimônio Arquivístico Digital Brasileiro.

A Resolução n.º 43 apresenta requisitos, em nível conceitual, que devem ser cumpridos no desenvolvimento de um repositório digital confiável. Esses requisitos estão baseados na norma ISO 16363: 2012, que é a norma que permite a certificação de confiança, em nível internacional, para repositórios digitais de organizações públicas ou privadas, e amplamente usada na Ciência da Informação. Esses requisitos estão organizados em três conjuntos: infraestrutura organizacional; gerenciamento do documento digital; e tecnologia, infraestrutura técnica e segurança.

A Resolução n.º 43 também apresenta uma série de padrões e normas de referência para a construção de Repositórios Arquivísticos Digitais Confiáveis. São eles: Modelo de referência OAIS, Relatório da *Research Library Group* (RLG) e da *Online Computer Library Center* (OCLC), Certificação e auditoria de

repositórios confiáveis: critérios e *checklist* (TRAC), Requisitos técnicos para entidades de auditoria e certificação de organizações candidatas a serem repositórios digitais confiáveis - CCSDS, Metadados de preservação PREMIS, Norma Geral Internacional de Descrição Arquivística ISAD(G), Norma Brasileira de Descrição Arquivística NOBRADE, Metadados do e-ARQ Brasil, Protocolo para coleta de metadados OAI-PMH, Padrão de codificação e transmissão de metadados METS e a Descrição arquivística codificada EAD (CONARQ, 2015a, p. 19-25). Sendo assim, a Resolução n.º 43 surge como uma resposta do Conarq para a comunidade arquivística no Brasil, no sentido de orientar e chamar a atenção para a necessidade de se manter um ambiente autêntico para a preservação permanente de documentos arquivísticos digitais, considerando sua fragilidade, especificidade e complexidade. Principalmente porque era necessário garantir uma preservação permanente - 50 anos ou mais (GLADNEY, 2009), e não mais somente de longo prazo, considerada pelo Conselho Internacional de Arquivos como de cinco anos a partir da data de produção do documento digital. Vale ressaltar que a Norma Internacional ISO 16363:2012 possui prevalência sobre a Resolução n.º 43 do Conarq, o que não permite sua horizontalidade.

O termo RDC-Arq surgiu na Resolução n.º 43 do Conarq (CONARQ, 2015a), de 04 de setembro de 2015, que deu nova redação à Resolução n.º 39, de 29 de abril de 2014. A resolução n.º 39 os denominava de Repositórios Digitais Confiáveis de Documentos Arquivísticos. A mudança de nomenclatura da Resolução n.º 39 para a Resolução n.º 43 traz em si um significado muito importante, o de se ter um Repositório Digital Confiável (RDC) adjetivado, ou seja, um RDC Arquivístico, com características específicas. Ou seja, um Repositório Arquivístico deve incorporar em seu funcionamento princípios e normas arquivísticas, e não apenas ser um RDC para documentos arquivísticos, no sentido de gerenciar e preservar apenas um tipo específico de material digital, dentre tantos outros diferentes tipos de materiais digitais.

Embora no Brasil as iniciativas de implementação de um RDC-Arq sejam modestas, em países como os Estados Unidos, Reino Unido, Austrália, Nova Zelândia, Canadá, Portugal e Noruega os arquivos nacionais e outras

instituições arquivísticas públicas já possuem uma solução informatizada para atuarem como repositórios digitais confiáveis para os documentos em fase permanente, e em alguns casos até na fase intermediária (ROCHA, 2015).

O termo RDC-Arq embute em si três conceitos importantes e que precisam ser entendidos: os conceitos de Repositório Digital, Repositório Arquivístico Digital e Repositório Digital Confiável. Por Repositório Digital, a própria resolução n.º 43 define como:

[...] um ambiente de armazenamento e gerenciamento de materiais digitais. Esse ambiente constitui-se de uma solução informatizada em que os materiais são capturados, armazenados, preservados e acessados. Um repositório digital é, então, um complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, software e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos. (CONARQ, 2015a, p. 09).

Vale ressaltar que nesta definição os Repositórios Digitais (RD) são ambientes informatizados para a gestão de materiais digitais quaisquer, já com certa preocupação com a preservação digital. As iniciativas de desenvolvimento dos Repositórios Digitais pela comunidade internacional também tiveram início já na década de 1990, no sentido de orientar sua modelagem e implementação e de apontar requisitos para sua confiabilidade (CONARQ, 2015a). Atualmente, uma das classificações possíveis dos Repositórios Digitais é diferenciá-los como Repositórios Institucionais ou Repositórios Temáticos, que reúnem, respectivamente, a produção científica de uma instituição e de uma determinada área (WEITZEL, 2006). Os Repositórios Digitais são empregados em diversas outras situações, tais como: biblioteca digital, acervo de obras de arte digitais, depósito legal de material digital e curadoria de dados digitais de pesquisa, o que, porém, não consegue atender aos requisitos específicos da área arquivística para a garantia de autenticidade e de preservação dos documentos de arquivo.

Já os Repositórios Arquivísticos Digitais são Repositórios Digitais que armazenam e gerenciam documentos arquivísticos digitais em todo o seu ciclo de vida, seja nas fases corrente e intermediária, seja na fase permanente. Para isso, esses repositórios devem gerenciar os documentos e metadados de acordo

com as práticas e normas da Arquivologia, além de proteger as características desse tipo de documento, principalmente em relação à autenticidade e relação orgânica (CONARQ, 2015a). Por autenticidade, entende-se “Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e de que está livre de adulteração ou qualquer outro tipo de corrupção.” (CONARQ, 2016, p. 10). Já a relação orgânica diz respeito aos “Vínculos que os documentos arquivísticos guardam entre si e que expressam as funções e atividades da pessoa ou organização que os produziu.” (CONARQ, 2016, p. 36).

Os Repositórios Digitais Confiáveis (RDC), por sua vez, referem-se a Repositórios Digitais que devem ser capazes de manter os materiais digitais autênticos e de garantir sua preservação e acesso pelo tempo que for necessário. A preocupação dos RDC com a Preservação Digital apresenta um nível de rigor muito superior se comparado com a proposta dos Repositórios Digitais. Os requisitos de um RDC, em nível conceitual, devem se basear na ISO 16363:2012, e estão organizados em três principais conjuntos de requisitos: infraestrutura organizacional; gerenciamento do documento digital; e tecnologia, infraestrutura técnica e segurança. Em relação à infraestrutura organizacional, o RDC deve cumprir requisitos relacionados à: governança e viabilidade organizacional; estrutura organizacional e de pessoal; transparência de procedimentos e arcabouço político; sustentabilidade financeira; e contratos, licenças e passivos. Em relação ao gerenciamento do documento digital, o RDC deve estar de acordo com o modelo de referência OAIS, que estabelece a formação de pacotes de informação envolvendo os documentos digitais (informação de conteúdo) e seus metadados (informação de representação). Já os requisitos de tecnologia, infraestrutura técnica e segurança descrevem as melhores práticas das áreas de gestão de dados e segurança, que devem ser atendidas por um RDC em relação à infraestrutura de sistema; tecnologias apropriadas; e segurança. (CONARQ, 2015a).

A partir do entendimento desses três conceitos, pode-se conceituar melhor um RDC-Arq. Segundo Luz e Flores (2016), esses conceitos são tão recentes que o Dicionário Brasileiro de Terminologia Arquivística - DIBRATE (ARQUIVO NACIONAL, 2005) não possui verbetes para “repositórios digitais” e

“repositórios digitais confiáveis”. Isso acontece no contexto arquivístico, uma vez que para as bibliotecas o seu uso já é uma realidade. Sendo assim, pode-se definir um RDC-Arq como um Repositório Digital que é “capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável.” (CONARQ, 2015a, p. 10).

Além disso, é muito importante entender que um RDC-Arq não é somente uma solução de *software* e *hardware*. Ele também contempla pessoas, políticas, normas, padrões, modelos, requisitos, e que sua gestão deve envolver pelo menos dois tipos de profissionais: arquivistas e profissionais da Tecnologia da Informação (TI). O arquivista deve ser responsável pela gestão arquivística e *dashboard*<sup>1</sup> da plataforma de preservação, atendendo às normativas da área, e o profissional de TI deve se responsabilizar pela administração do *Storage Service*<sup>2</sup>. Por exemplo, cabe ao Arquivista ou Arquivo solicitar a exclusão de documentos no RDC-Arq, armazenados no *Storage Server*, e cabe ao profissional de TI aprová-la ou não, e executar a exclusão, se for o caso. Esses profissionais devem ser nomeados por documento, com suplentes (para casos de impedimento do titular), por portaria ou o ato administrativo comumente adotado pelo órgão, previstos na política arquivística do órgão do RDC-Arq em questão. Essa multidisciplinaridade entre a Arquivística e a TI, e sua adaptação ao Modelo OAIS, é apenas uma das relações interdisciplinares possíveis. Caso seja aplicada a Bibliotecas e Museus, ou alguma outra instituição de Preservação Digital, a relação precisa ser adequada às respectivas especificidades de cada área.

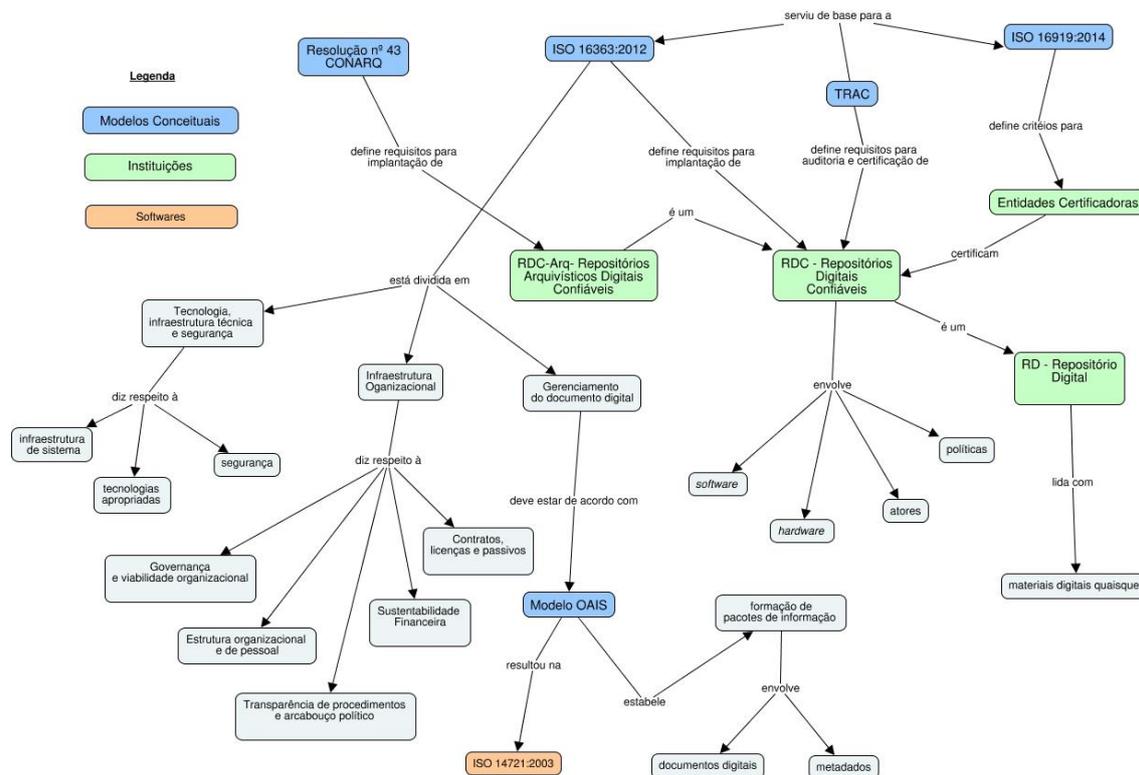
A Figura 1 apresenta um mapa conceitual dos principais conceitos relacionados a esta seção.

---

<sup>1</sup> Um *dashboard* é a interface gráfica de um software que apresenta de forma visual as informações mais importantes e necessárias, reunidas em uma única tela para que a informação possa ser monitorada de forma adequada.

<sup>2</sup> O *Storage Service* é uma interface onde é possível fazer a gerência da área de armazenamento no servidor onde a plataforma de preservação encontra-se instalada e oferece ferramentas para a TI administrar o armazenamento, *backup* em cadeia de custódia e gerenciamento de pacotes.

**Figura 1 – Mapa Conceitual sobre os conceitos relacionados a um RDC-Arq**



Fonte: Autoria própria.

### 3 O GERENCIAMENTO DO DOCUMENTO DIGITAL NO CONTEXTO DE UM RDC-ARQ

Como dito anteriormente, é muito importante entender o RDC-Arq como uma Estrutura Organizacional. Ou seja, ele possui muito mais aspectos do que simplesmente lidar com *softwares* e *hardwares* que farão a gestão do documento arquivístico digital no sentido de manter sua autenticidade e preservação permanente. O gerenciamento do documento digital é apenas um dos conjuntos de requisitos de um RDC-Arq, talvez o mais importante, mas não o único. Uma vez que o gerenciamento do documento digital no RDC-Arq lida com a gestão dos documentos digitais, é comum associá-lo simplesmente a uma solução informatizada para implementar um repositório digital confiável. No entanto, é importante perceber que o RDC-Arq é muito mais do que isso. Sendo assim, neste conjunto de requisitos é necessário se trabalhar com alguma plataforma arquivística de preservação, ou seja, com *softwares* para fazer a gestão e

preservação dos documentos digitais. Um exemplo desse tipo de *software* é o *Archivematica*<sup>3</sup>. Neste contexto, a partir de agora será usado o termo plataforma de preservação para se referir ao componente de *software/hardware* que faz a gestão e preservação dos documentos digitais, para se evitar qualquer tipo de confusão conceitual.

O gerenciamento do documento digital deve estar de acordo com o modelo de referência OAIS, que estabelece a formação de pacotes de informação envolvendo os documentos digitais e seus metadados. (CONARQ, 2015). São três os tipos de pacotes de informação:

- Pacote de informação para submissão (*submission information package – SIP*) – refere-se à admissão dos documentos digitais e seus metadados associados.
- Pacote de informação para arquivamento (*archival information package – AIP*) – refere-se ao acondicionamento e armazenamento dos documentos digitais e seus metadados associados.
- Pacote de informação para disseminação (*dissemination information package – DIP*) – refere-se ao acesso aos documentos digitais e seus metadados associados.

A TRAC (*Trustworthy Repository Audit & Certification: Criteria and Checklist*), que define requisitos para a auditoria e certificação de um RDC, apresenta requisitos para o gerenciamento do documento digital caracterizados em seis grupos, a saber: admissão: captação de documentos digitais; admissão, criação do pacote de arquivamento; planejamento da preservação; armazenamento e preservação/manutenção do AIP; gerenciamento de informação; e gerenciamento de acesso.

O modelo OAIS visa identificar os componentes funcionais que deverão fazer parte de um sistema de informação dedicado à preservação digital. O modelo também descreve as interfaces internas e externas do sistema e os

---

<sup>3</sup> O *Archivematica* é um *software* de preservação digital de código aberto adotado pelo Arquivo Nacional, de ampla utilização ao redor do mundo, desenvolvido pela empresa canadense Artefactual (<https://www.artefactual.com>).

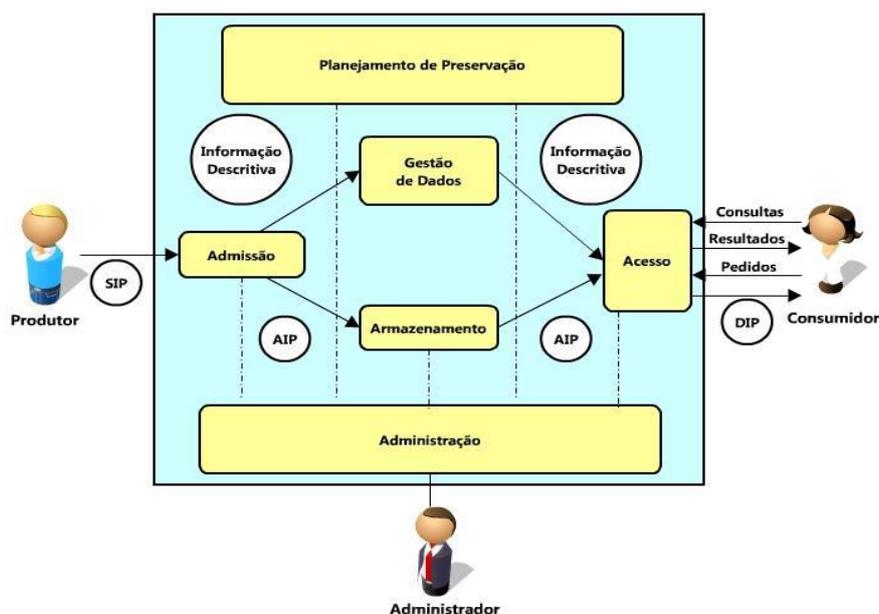
objetos de informação que são manipulados no seu interior. (FERREIRA, 2006).

O ambiente do modelo define três entidades externas:

- Produtor – é o papel desempenhado por pessoas ou sistemas que fornecem a informação a ser preservada.
- Administrador – é o papel desempenhado por aqueles que estabelecem as políticas gerais que governam o repositório.
- Consumidor – é o papel desempenhado por pessoas ou sistemas que interagem com os serviços *OAIS* para acessar a informação preservada desejada.

O modelo *OAIS* se desmembra em dois modelos: o modelo funcional e o modelo de informação. O modelo funcional delinea as funções que precisam ser desempenhadas por um repositório *OAIS*. Já o modelo de informação diz respeito ao conceito de pacote de informação, formado pela informação de conteúdo e pela informação de descrição de preservação, encapsuladas e identificadas pela informação de empacotamento. A Figura 2 apresenta os componentes funcionais, os pacotes de informação e as entidades externas de uma plataforma de preservação compatível com o Modelo *OAIS*. (CONARQ, 2015a).

**Figura 2 – O Modelo de Referência *OAIS***



Fonte: (CONARQ, 2015a).

Observando a Figura 2 pode-se ver que o “Produtor” é a entidade externa à plataforma de preservação, que se responsabiliza pela submissão de material digital. No caso de um RDC-Arq, esse material digital diz respeito aos documentos arquivísticos digitais. O material submetido é representado na Figura 2 pelo Pacote de Informação de Submissão (SIP - *Submission Information Package*). Durante o processo de submissão, representado na Figura 2 por “Admissão” (também chamado Ingestão), a plataforma de preservação é responsável por garantir a integridade da informação recebida. Ainda nesta fase é produzida toda a “Informação Descritiva” que dá suporte à localização e recuperação do material depositado. Essa informação descritiva (ou metainformação) é armazenada e gerida pelo componente “Gestão de Dados”. O material digital a ser preservado, ou seja, o Pacote de Informação de Arquivo (AIP – *Archival Information Package*) será preservado no Repositório de Dados, representando na Figura 2 como “Armazenamento”. O componente “Planejamento de Preservação” encarrega-se da definição de políticas de preservação. Este serviço é responsável pelo monitoramento do ambiente externo à plataforma de preservação e por desencadear eventos de preservação, sempre que necessário. É, por exemplo, da responsabilidade deste componente definir as estratégias de preservação a serem utilizadas no interior da plataforma de preservação, monitorar as tendências comportamentais da sua comunidade de interesse e/ou identificar formatos que se encontram na iminência de se tornar obsoletos. Esta parte da plataforma de preservação diz respeito à entidade “Administrador”. Já o componente “Acesso” estabelece a ponte entre a plataforma de preservação e sua comunidade de interesse, ou seja, o conjunto de potenciais consumidores do material custodiado (entidade “Consumidor”). Esse componente é responsável por facilitar a localização e recuperação do material digital preservado, bem como prepará-lo para entrega ao consumidor. Os pacotes entregues ao consumidor assumem a forma de Pacotes de Informação de Disseminação (DIP - *Dissemination Information Package*) (FERREIRA, 2006).

É importante notar que os pacotes DIP podem ser diferentes dos pacotes AIP. Ou seja, a informação que é entregue ao consumidor pode ser apenas um

subconjunto da informação arquivada ou até uma versão transformada da mesma. Além disso, os formatos dos materiais digitais dos pacotes SIP, DIP e AIP em geral são diferentes entre si, relativos ao mesmo material digital que se quer preservar. Esses formatos são definidos pela política de preservação digital do RDC-Arq. No Brasil, a política de preservação digital adotada no âmbito da AN Digital - Programa Permanente de Preservação e Acesso a Documentos Arquivísticos Digitais, do Arquivo Nacional, define que para um material digital original (pacote SIP) nos formatos .DOC ou .DOCX, por exemplo, o formato de preservação (pacote AIP) deve ser o .PDF/A, e o formato de acesso (pacote DIP) o .PDF. Assim, a escolha do formato de preservação é “um ponto fundamental, pois qualquer falha no conversor utilizado, na conversão para um formato com compactação ou na conversão para formato com tendência obsoleta, pode gerar perdas de informação ou retrabalho em conversões futuras”. (SANTOS; HEDLUND; FLORES, 2015, p. 159). Recomenda-se também o uso de formatos de arquivo de código aberto para possibilitar a reconstrução do formato em caso de obsolescência. Já para o formato de acesso, a preocupação é com a disponibilização do material digital por meio de um sistema de informação. Sendo assim, deve-se optar por formatos mais “leves”.

Também é importante destacar que o pacote SIP possui os objetos originais e seus respectivos metadados, e o pacote AIP é a conversão desses objetos originais em um formato aberto para preservação (caso necessário, quando o formato de origem não é de preservação), juntamente com todos os metadados, incluindo os metadados de gestão (no Brasil, o e-ARQ Brasil, pg. 93, nos EUA, o DoD 5015.2 e na União Européia, o Moreq, entre outros), e o pacote DIP, acessado por meio de uma plataforma de acesso, possui os objetos digitais derivados, e suas miniaturas, chamadas de *thumbnail*, além dos metadados de Representação, ou seja, de Descrição Arquivística, baseados na norma internacional de descrição arquivística ISAD(G) ou correspondente. Sendo assim, pode-se notar que os pacotes SIP, AIP e DIP, em geral, diferem entre si, sendo que o foco da preservação digital está no pacote AIP. Assim, caso haja algum tipo de corrupção ou adulteração no pacote DIP, ele sempre poderá ser gerado novamente, desde que o AIP esteja preservado.

#### **4 O RDC-ARQ COMO O ARQUIVO PERMANENTE DIGITAL**

O Arquivo é definido pela terminologia arquivística como "Instituição ou serviço que tem por finalidade a custódia, o processamento técnico, a conservação e o acesso a documento arquivístico". (CONARQ, 2016, p. 9). Com o advento das tecnologias, os documentos arquivísticos em suporte papel começaram a ser migrados e produzidos como documentos eletrônicos e, atualmente, como documentos digitais. A produção de documentos em formato digital foi um movimento que se intensificou a partir da década de 1990 e continua até hoje. Na verdade, cada vez mais os documentos arquivísticos são nato digitais, sendo um caminho sem volta. Com este novo cenário, a ideia de Arquivo precisou ser ampliada, uma vez que a natureza de um documento eletrônico, em especial dos documentos digitais, difere, e muito, do documento em suporte papel. No Brasil, a Carta de Preservação Digital trouxe à tona a preocupação com este novo tipo de legado, o patrimônio arquivístico digital, diante do desafio da sua preservação para acesso contínuo, por meio de recursos tecnológicos disponíveis à época em que ocorrer a sua utilização. A Carta traz a preocupação com os seguintes problemas: dependência social da informação digital, rápida obsolescência da tecnologia digital, incapacidade dos atuais sistemas eletrônicos de informação em assegurar a preservação de longo prazo, fragilidade intrínseca do armazenamento digital, complexidade e custos da preservação digital e multiplicidade de atores envolvidos. (CONARQ, 2005).

Assim, houve a necessidade de se ressignificar o conceito de Arquivo Permanente, que agora deve lidar também com o patrimônio arquivístico digital, e suas peculiaridades. Neste novo cenário o documento arquivístico digital tem que estar confinado em sistemas informatizados com requisitos arquivísticos, para manter sua autenticidade e preservação permanente. E não apenas isso, há uma separação da gestão arquivística nas fases corrente e intermediária, da administração na fase permanente. Nas fases corrente e intermediária temos a figura dos Sistemas informatizados de Gestão Arquivística de Documentos (SIGAD), que são definidos pelo e-Arq Brasil. (CONARQ, 2011). Já na fase permanente torna-se também necessário o aparecimento de uma nova figura de

sistema informatizado com requisitos arquivísticos, o RDC-Arq, ou seja, o Arquivo Permanente Digital. Luz e Flores (2016) nos alertam para a importância da manutenção de uma linha de custódia ininterrupta entre estes dois sistemas, contemplando todo o ciclo de vida dos documentos arquivísticos digitais.

Falar de Arquivo Permanente Digital nos remete invariavelmente a discutir temas como cadeia de custódia, que é um “Documento ou trilha que demonstra a sucessão de entidades coletivas ou pessoas que tiveram posse, custódia e controle sobre os documentos.” (INTERNATIONAL COUNCIL ON ARCHIVES, *Multilingual Archival Terminology*). A cadeia de custódia documental pode ser entendida como o ambiente no qual perpassa o ciclo de vida dos documentos, sendo necessário que os princípios e funções arquivísticas sejam aplicados de forma adequada à documentação custodiada. É importante destacar que embora se cite o ciclo de vida, a cadeia de custódia não é o ciclo de vida, ou seja, eles são conceitos distintos, mas que se entrelaçam, já que a cadeia de custódia é um conceito jurídico, uma necessidade de cotejar, em uma linha ininterrupta, os documentos de arquivo.

A cadeia de custódia de documentos arquivísticos tradicionais, para ser confiável, deve ser mantida por meio de uma linha ininterrupta, compreendendo as três idades do arquivo: fases corrente, intermediária e permanente. Dessa forma, a confiabilidade ocorre por intermédio da própria instituição que tem a responsabilidade sobre a produção, gestão, preservação e acesso aos documentos arquivísticos. (FLORES; ROCCO; SANTOS, 2016).

Vale destacar que todo esse processo deve ser executado por uma instituição arquivística que deve manter uma linha de custódia ininterrupta a fim de garantir a confiabilidade dos materiais custodiados. No entanto, isso não significa que não possa haver mudança de custodiadores. Ou seja, há a necessidade de acompanhar a cadeia de custódia de maneira que ela se mantenha ininterrupta entre as três idades documentais, inclusive considerando a mudança de custódia documental. (FLORES; ROCCO; SANTOS, 2016). Além disso, caso haja alteração na cadeia de custódia, é necessário aplicar os princípios e normas arquivísticas “a fim de exercer uma sequência de custódia sem interrupção, sem que estes documentos se percam, sejam desviados tanto

de instituição como de um sistema que não tenha todos os requisitos arquivísticos e assim comprometa a autenticidade e confiabilidade” (LUZ; FLORES, 2016, p. 7). Isso é muito importante neste novo contexto digital, uma vez que a proposta de uso do RDC-Arq na gestão arquivística dos documentos digitais passa por essa nova concepção, como será visto adiante. No entanto, há de se considerar ainda o conceito de cadeia de preservação, em comparação ao conceito de cadeia de custódia, que é definida como um “Sistema de controles que se estende por todo o ciclo de vida dos documentos, a fim de assegurar sua autenticidade ao longo do tempo.” (ICA, *Multilingual Archival Terminology*). Embora esses dois conceitos sejam diferentes, eles se complementam. A cadeia de preservação, como o próprio nome diz, tem como objetivo garantir a preservação dos documentos arquivísticos digitais a longo prazo. O projeto InterPARES 2<sup>4</sup> apresenta um modelo de Cadeia de Preservação – *Chain of Preservation* (CoP) como uma sequência de passos para a produção, manutenção, avaliação e preservação digital de documentos autênticos. Essa cadeia de preservação deve ser observada em todo o ciclo de vida dos documentos, tal como a cadeia de custódia – *Chain of Custody* (CoC). Ou seja, são dois processos que devem ocorrer concomitantemente, ambos buscando a manutenção da autenticidade dos documentos.

Nesta compreensão, é possível vislumbrar que a CoP se apresenta de forma muito mais computacional, já que está focada em registrar, por meio de metadados e modelos computacionais, a sua implementação. Trata-se de uma abordagem mais técnica e tecnológica e diferente da abordagem da CoC, que por sua vez, não está focada num modelo computacional, e sim na ideia de um princípio arquivístico, de cuidado, de um querer, de um manter a linha ininterrupta, apresentando a necessidade de cotejar o documento arquivístico digital. A CoP, por sua vez, é a implementação tecnológica da CoC que, agora, precisa ser ressignificada em um ambiente digital, já que a CoP não substitui a CoC enquanto princípio.

---

<sup>4</sup> Disponível em: [http://www.interpares.org/ip2/display\\_file.cfm?doc=ip2\\_book\\_appendix\\_14.pdf](http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_appendix_14.pdf)

Vale destacar que a presunção de autenticidade do documento arquivístico digital tem suas peculiaridades. No Brasil, a resolução n.º 37, de 19 de dezembro de 2012, aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais. Segundo a Resolução:

Os documentos arquivísticos digitais apresentam dificuldades adicionais para presunção de autenticidade em razão de serem facilmente duplicados, distribuídos, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes. Assim, a presunção de autenticidade do documento arquivístico digital é realizada por meio da análise da sua forma e do seu conteúdo, bem como do ambiente de produção, manutenção/uso e preservação desse documento, e não apenas com base em suas características físicas ou em soluções tecnológicas. (CONARQ, 2012, p. 1).

A Resolução também nos chama a atenção para a diferenciação de dois conceitos muito importantes, mas sutilmente distintos: o de autenticidade e autenticação. A autenticidade refere-se à “qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração. A autenticidade é composta de identidade e integridade”. (CONARQ, 2012, p. 2). Já a autenticação refere-se à “declaração de autenticidade de um documento arquivístico, num determinado momento, resultante do acréscimo de um elemento ou da afirmação por parte de uma pessoa investida de autoridade para tal”. (CONARQ, 2012, p. 2). Portanto, a presunção de autenticidade é a inferência da autenticidade de um documento arquivístico feita a partir da análise de como esse documento foi produzido e mantido. Além disso, “Enquanto declaração, a autenticação não garante necessariamente a autenticidade do documento, na medida em que se pode declarar como autêntico algo que não é”. (CONARQ, 2012, p. 5). Também é correto afirmar que um documento pode ser considerado autêntico sem que nele conste necessariamente uma autenticação. Vale ressaltar que no ambiente digital as técnicas de autenticação são dependentes da tecnologia, como é o caso da assinatura digital.

## 5 A CADEIA DE CUSTÓDIA ARQUIVÍSTICA DIGITAL

A orientação técnica n.º 3 do Conarq (CONARQ, 2015b) apresenta cenários que representam algumas possibilidades de implantação de um Repositório Arquivístico Digital Confiável – RDC-Arq (CONARQ, 2015a) integrado a um Sistema Informatizado de Gestão Arquivística de Documentos (CONARQ, 2011), tomando como base a Resolução n.º 43 do CONARQ e o e-ARQ Brasil, respectivamente. O documento ressalta que o uso do RDC-Arq em interação com o SIGAD pode, e deve, se dar nas três idades dos documentos, e de maneiras distintas, em três possíveis cenários diferentes: no ciclo de vida completo, nas idades corrente e intermediária e na idade permanente.

**Cenário 1)** o primeiro cenário, que engloba todo o ciclo de vida do documento, apresenta o uso de um RDC-Arq para as idades corrente e intermediária, e outro para a idade permanente. Ou seja, há a mudança dos documentos de um ambiente de gestão para um ambiente de preservação permanente e acesso. O RDC-Arq da idade permanente pode ser o de uma instituição arquivística, como o Arquivo Nacional, por exemplo, ou da própria instituição produtora. Sendo assim, este cenário envolve mudança de custódia (sem interrupção) dos documentos arquivísticos digitais, das fases corrente e intermediária, para a fase permanente. Para manter a autenticidade dos documentos, criados num ambiente seguro e protegido pelo SIGAD, essa mudança deve ser monitorada, e mantida como uma Cadeia de Custódia Digital Arquivística (CCDA), de forma ininterrupta. A definição de cadeia de custódia no ambiente analógico é definida como “Documento ou trilha que demonstra a sucessão de entidades coletivas ou pessoas que tiveram posse, custódia e controle sobre os documentos.” (INTERNATIONAL COUNCIL ON ARCHIVES, *Multilingual Archival Terminology*). Hirtle (2001, tradução nossa) corrobora com a ideia de que “em um ambiente analógico, a transferência física e legal dos documentos de uma instituição para uma Instituição Arquivística assegura uma cadeia de custódia ininterrupta”, o que não é verdade para o ambiente digital, pela especificidade e complexidade do documento digital e vulnerabilidade do registro digital. Sendo assim, no ambiente digital, faz-se

necessária uma nova proposta de definição de Cadeia de Custódia Digital Arquivística, seja pela ressignificação da Cadeia de Custódia ou da Cadeia de Preservação. Neste sentido, já se pode observar em eventos ou na literatura internacional da área, incidências como a apresentada por Luciana Duranti em uma palestra na Conferência anual do ICA-ALA, ocorrida na cidade do México em novembro de 2017, onde a pesquisadora e coordenadora do InterPARES conceitua a Digital Chain of Custody (Cadeia de Custódia Digital) como sendo “A informação preservada sobre os documentos e sobre suas mudanças que mostrem que um dado específico estava em um determinado estado em uma data e hora específica”. (DURANTI, 2017, tradução nossa).

Assim, uma definição de Cadeia de Custódia Digital Arquivística (CCDA) deve trazer a ideia de que a cadeia de custódia digital não pode ser interrompida, e deve ser auditada pela cadeia de preservação ou outro procedimento capaz dessa garantia no ambiente digital. Além disso, que a presunção de autenticidade deve ser mantida quando acontece a mudança de custódia de um ambiente digital, que por si só é extremamente vulnerável, para outro, como, por exemplo, de um SIGAD, SIGAD de Negócio ou qualquer outro sistema de informação digital para um RDC-Arq, independentemente da fase. Essa presunção de autenticidade deve vir apoiada pela evidência de que os documentos não foram modificados ou corrompidos em seus aspectos essenciais durante a sua transmissão de um ambiente digital para outro.

**Cenário 2)** o segundo cenário apresenta o uso de um RDC-Arq nas idades corrente e intermediária, associado ao uso de um SIGAD, a fim de garantir o controle do ciclo de vida, o cumprimento da destinação prevista e a manutenção da autenticidade e da relação orgânica dos documentos. Segundo a orientação técnica, “nessas idades, os produtores já precisam tomar cuidados especiais, previstos em um plano de preservação digital, com relação aos documentos digitais que serão mantidos por médio e longo prazo”. (CONARQ, 2015b).

São três as possibilidades (cenários) de uso de um SIGAD nas idades corrente e intermediária:

**Possibilidade 1:** Um SIGAD pode gerenciar documentos digitais nas idades corrente e intermediária, armazenando determinados documentos em sistemas de *storage*, e encaminhando outros documentos para um RDC-Arq, de acordo com a política arquivística adotada. Esses documentos arquivísticos podem ser, por exemplo, documentos sensíveis, sigilosos e/ou de temporalidade maior do que cinco anos.

**Possibilidade 2:** Um sistema informatizado de processos de negócios, no ambiente do produtor, pode interoperar com um SIGAD, e este com um RDC-Arq e/ou um sistema de *storage*. São exemplos de sistemas de negócio: sistemas de controle acadêmico em instituições de ensino, sistemas de prontuários médicos, sistemas de controle de ponto etc. Neste caso, o sistema de negócios produz os documentos arquivísticos, que são captados e geridos pelo SIGAD, que faz toda a gestão arquivística, armazenando, por exemplo, os documentos de curta temporalidade no sistema de *storage* e encaminhando os de longa temporalidade para o RDC-Arq.

**Possibilidade 3:** Um sistema informatizado de processos de negócio no ambiente do produtor que incorpora as funcionalidades de um SIGAD interopera com um RDC-Arq e/ou com um sistema de *storage*. Neste caso, o sistema informatizado (sistema de negócios + SIGAD) armazena, por exemplo, os documentos arquivísticos de curta temporalidade no sistema de *storage* e encaminha os de longa temporalidade para o RDC-Arq.

**Cenário 3)** um terceiro cenário apresenta o uso de um RDC-Arq na idade permanente, que é o cenário mais aceito, aliás, obrigatório. Neste cenário os documentos digitais destinados à fase permanente devem ser mantidos e preservados por um RDC-Arq, de maneira a apoiar o tratamento técnico adequado, incluindo arranjo, descrição e acesso, para assegurar a manutenção da autenticidade e da relação orgânica desses documentos. Um exemplo desse cenário é considerar o ambiente de preservação e acesso como o Arquivo Nacional, ou seja, como o Arquivo Permanente Digital, recebendo os documentos arquivísticos de SIGAD dos diversos órgãos e entidades da Administração Pública Federal.

Vale ressaltar que todas as decisões específicas de cada cenário devem estar respaldadas por uma política de preservação digital do RDC-Arq. Além disso, podem-se usar múltiplas abordagens, ou seja, o uso simultâneo de vários cenários.

A Figura 3 apresenta a proposta do uso do RDC-Arq juntamente com um SIGAD, considerando os conceitos de ciclo de vida dos documentos, cadeia de custódia digital arquivística e cadeia de preservação.

**Figura 3 – Interoperabilidade do SIGAD com o RDC-Arq.**



Fonte: Autoria Própria.

## 6 CONSIDERAÇÕES FINAIS

Este artigo teve como objetivo principal apresentar os Repositórios Arquivísticos Digitais Confiáveis como uma necessidade para a preservação digital sistêmica em um ambiente de gestão arquivística, a fim de manter os documentos arquivísticos digitais autênticos e acessíveis a longo prazo. Mas mais do que isso, apresentá-lo como o Arquivo Permanente Digital ante a

realidade digital, afinal, os documentos digitais são complexos e específicos, necessitam estar confinados em um sistema de informação digital, durante toda a sua vida, mantendo uma CCDA. Assim, o RDC-Arq é mais que necessário, é obrigatório para a garantia da autenticidade e confiabilidade dos documentos arquivísticos digitais. Para isso foi necessário discutir e ressignificar conceitos tais como: repositórios digitais, repositórios arquivísticos digitais, repositórios digitais confiáveis, repositórios arquivísticos digitais confiáveis, cadeia de custódia digital arquivística, cadeia de preservação, entre outros.

O artigo também discutiu sobre a Cadeia de Custódia Digital Arquivística (CCDA), onde se apresentou um rascunho de conceito discutindo-o como princípio e sobre os cuidados que se deve ter neste processo para manter a presunção de autenticidade e preservação a longo prazo dos documentos arquivísticos digitais durante todo o seu ciclo de vida, porém com uma abordagem arquivística de princípios, e não de procedimentos tecnológicos, como os apresentados na Cadeia de Preservação. Assim, uma definição de Cadeia de Custódia Digital Arquivística (CCDA) deve trazer a ideia de que a cadeia de custódia digital não pode ser interrompida, e deve ser auditada pela cadeia de preservação ou outro procedimento capaz dessa garantia no ambiente digital. Além disso, que a presunção de autenticidade deve ser mantida quando acontece a mudança de custódia de um ambiente digital, que por si só é extremamente vulnerável, para outro, como, por exemplo, de um SIGAD, SIGAD de Negócio ou qualquer outro sistema de informação digital para um RDC-Arq, independentemente da fase. Essa presunção de autenticidade deve vir apoiada pela evidência de que os documentos não foram modificados ou corrompidos em seus aspectos essenciais durante a sua transmissão de um ambiente digital para outro.

Considerando os princípios da especificidade e complexidade do documento digital, e que ele deve estar confinado em um sistema informatizado com requisitos arquivísticos, é importante destacar que a CCDA deve ser implementada dentro de um SIGAD, ou SIGAD de Negócio, garantindo que estes sistemas e o(s) RDC-Arq não entrem em colapso, que o documento não saia desses sistemas sem supervisão adequada (auditoria e certificação), e que não

haja brecha ou janela de insegurança que permita alterações de corrupção.

Por fim, é importante olhar para o RDC-Arq, ou seja, para o Arquivo Permanente digital, como o lugar necessário e obrigatório perante a Lei 8159/91 para os documentos históricos/permanentes, e o lugar onde são implementados, hoje, os referenciais consolidados e atuais de uma Preservação Digital Sistêmica. Uma vez que a Lei 8159/91 considera como permanentes os conjuntos de documentos de valor histórico, probatório e informativo, que devem ser definitivamente preservados (são inalienáveis segundo a Lei), vale reforçar que, perante a Lei, fica sujeito à responsabilidade penal, civil e administrativa, na forma da legislação em vigor, todos os que vierem a desfigurar ou destruir documentos de valor permanente ou considerados de interesse público e social.

## REFERÊNCIAS

ARQUIVO NACIONAL. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro, 2005. 231 p. Disponível em: [http://conarq.arquivonacional.gov.br/images/publicacoes\\_textos/dicionario\\_de\\_terminologia\\_arquivistica.pdf](http://conarq.arquivonacional.gov.br/images/publicacoes_textos/dicionario_de_terminologia_arquivistica.pdf). Acesso em: 28 jul. 2019.

BRASIL. Lei n.º 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, 9 jan. 1991. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/L8159.htm](http://www.planalto.gov.br/ccivil_03/leis/L8159.htm). Acesso em: 04 jul. 2016.

CONSELHO NACIONAL DE ARQUIVOS. **Carta para preservação do patrimônio arquivístico digital**. Rio de Janeiro, 2005, 24 p. Disponível em: [http://conarq.arquivonacional.gov.br/images/publicacoes\\_textos/Carta\\_preservacao.pdf](http://conarq.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf). Acesso em: 14 ago. 2019.

CONSELHO NACIONAL DE ARQUIVOS. **E-ARQ BRASIL: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos**. Rio de Janeiro, 2011. 139 p. Disponível em: [http://conarq.gov.br/images/publicacoes\\_textos/earqbrasil\\_model\\_requisitos\\_2009.pdf](http://conarq.gov.br/images/publicacoes_textos/earqbrasil_model_requisitos_2009.pdf). Acesso em: 01 jan. 2009.

CONSELHO NACIONAL DE ARQUIVOS. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro, 2012. 10 p. Disponível em: [http://conarq.arquivonacional.gov.br/images/publicacoes\\_textos/conarq\\_presuncao\\_autenticidade\\_completa.pdf](http://conarq.arquivonacional.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_completa.pdf). Acesso em: 21 mar. 2018.

CONSELHO NACIONAL DE ARQUIVOS. **Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq**. Rio de Janeiro: Arquivo Nacional, 2015a. 31 p. Disponível em: [http://conarq.gov.br/images/publicacoes\\_textos/diretrizes\\_rdc\\_arq.pdf](http://conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf). Acesso em: 04 nov. 2019.

CONSELHO NACIONAL DE ARQUIVOS. **Orientação Técnica n.º 3: Cenários de uso de RDC-Arq em conjunto com o SIGAD**. Rio de Janeiro: Arquivo Nacional, 2015b. 8 p. Disponível em: [http://conarq.arquivonacional.gov.br/images/ctde/Orientacoes/Orientacao\\_tecnica\\_rdc\\_arq\\_2015\\_v8\\_pub.pdf](http://conarq.arquivonacional.gov.br/images/ctde/Orientacoes/Orientacao_tecnica_rdc_arq_2015_v8_pub.pdf). Acesso em: 04 nov. 2019.

CONSELHO NACIONAL DE ARQUIVOS. **Glossário: Documentos Arquivísticos Digitais. Versão 7.0**. Rio de Janeiro: Arquivo Nacional, 2016. 54 p. Disponível em: [http://conarq.arquivonacional.gov.br/images/ctde/Glossario/2016-CTDE-Glossario\\_V7\\_public.pdf](http://conarq.arquivonacional.gov.br/images/ctde/Glossario/2016-CTDE-Glossario_V7_public.pdf). Acesso em: 21 mar. 2018.

DURANTI, Luciana. An Infrastructure for TruthEntrusting Digital Facts to Archival Theory. *In: ALA-ICA CONFERENCE*, México, nov. 2017. Disponível em: <http://www.alaarchivos.org/wp-content/uploads/2017/12/Magistral-Luciana-Duranti.pdf>. Acesso em: 5 jun. 2019.

FERREIRA, Miguel. **Introdução à preservação digital: Conceitos, estratégias e actuais consensos**. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. 88 p.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. Cadeia de custódia para documentos arquivísticos digitais. **Acervo - Revista do Arquivo Nacional**, v. 29, n. 2, p. 117-132, 2016. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/40511>. Acesso em: 24 out. 2019.

GLADNEY, Henry. Long-Term Preservation of Digital Records: Trustworthy Digital Objects. **The American Archivist**, v. 72, n. 2, p. 401-435, 2009. Disponível em: <https://americanarchivist.org/doi/pdf/10.17723/aarc.72.2.g513766100731832>. Acesso em: 01 out. 2019.

GIL, Antônio Carlos. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo: Atlas, 2002. 175 p.

HIRTLE, P. B. Archival Authenticity in a Digital Age. **Páginas A&B, Arquivos e Bibliotecas**, Portugal, n. 6, p. 73-90, 2001. Disponível em: <https://ojs.letras.up.pt/index.php/paginasueb/article/view/136/128>. Acesso em: 04 ago. 2019.

INTERNATIONAL COUNCIL ON ARCHIVES. **Multilingual Archival Terminology**. Disponível em: <https://www.ica.org>. Acesso em: 14 ago. 2019.

LUZ, Charley; FLORES, Daniel. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivístico. *In: SEMINÁRIO SERVIÇOS DE INFORMAÇÃO EM MUSEUS*, 4., 2016, São Paulo. **Anais eletrônicos** [...] São Paulo: Pinateca de São Paulo, 2016. Disponível em: <http://biblioteca.pinacoteca.org.br:9090/publicacoes/index.php/sim/article/view/105/110>. Acesso em: 17 jul. 2019.

ROCHA, C. L. Repositórios para a preservação de documentos arquivísticos digitais. **Acervo - Revista do Arquivo Nacional**, Rio de Janeiro, v. 28, n. 2, p. 180-191, 2015. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/608/66>. Acesso em: 04 nov. 2019.

SANTOS, H. M.; FLORES, D. As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital. **Biblios - Revista de Bibliotecología y Ciencias de la Información**, n. 59, p. 45-54, 2015. Disponível em: <http://biblios.pitt.edu/ojs/index.php/biblios/article/view/215>. Acesso em: 26 jun. 2019.

SANTOS, H. M.; HEDLUND, D. C.; FLORES, D. Padronização dos formatos de arquivo: um caminho para preservar os documentos arquivísticos digitais. **Biblionline**, João Pessoa, v. 11, n. 1, p. 158-172, 2015. Disponível em: <https://periodicos.ufpb.br/ojs2/index.php/biblio/article/view/25157>. Acesso em: 04 nov. 2019.

WEITZEL, S. R. O papel dos repositórios institucionais e temáticos na estrutura da produção científica. **Em Questão**, Porto Alegre, v. 12, n. 1, p. 51-71, 2006. Disponível em: <https://seer.ufrgs.br/EmQuestao/article/view/19>. Acesso em: 20 out. 2019.

## **TRUSTED DIGITAL ARCHIVAL REPOSITORIES (TDAR) AS DIGITAL PRESERVATION SYSTEM IN A ARCHIVAL MANAGEMENT ENVIRONMENT**

### **ABSTRACT**

**Introduction:** In a digital environmen it was necessary to rethink the assurance of uninterrupted custody chain, and how to maintain it as a place of records management, permanent preservation, reliable custody, and a digital permanent archive, through the Law 8159/91, which considers archival records management as a public duty, aiming their elimination or recall for permanent custody. **Objective:** Introduce Trusted Digital Archival Repositories (TDAR) as a digital preservation system in a records management environment, to keep authentic and long-term digital archival documents. **Methodology:** Exploratory, bibliographic and documentary research, with InterPARES Project documentation, National Archives Council standards, and scientific

papers as main documentary and bibliographic references. **Results:** Presentation and discussion of concepts related to TDAR such as digital repositories, digital records repositories, trusted digital repositories, the digital archival custody chain, and preservation chain. **Conclusions:** It is essential to see a TDAR, in other words, a Digital Permanent Archive, as the fundamental and obligatory spot of historical and permanent documents under Law 8159/91, furthermore the place where it is implemented the current and consolidated aspects of a Systemic Digital Preservation.

**Descriptors:** Archival Science. Digital Archival Repositories. Digital Preservation.

## REPOSITARIOS DE ARCHIVOS DIGITALES CONFIABLES (RADC) COMO UNA PLATAFORMA DE PRESERVACIÓN DIGITAL EN UN ENTORNO DE GESTIÓN DE ARCHIVOS

### RESUMEN

**Introducción:** en un entorno digital ha sido necesario repensar la garantía de una cadena de custodia ininterrumpida y cómo mantenerla como un lugar de gestión de archivos, preservación permanente, custodia confiable y como un archivo permanente digital, motivado por la Ley 8159/91, que coloca la gestión de los documentos de archivo como un deber público, con miras a su eliminación o revocación para la custodia permanente. **Objetivo:** presentar Repositorios de Archivos Digitales Confiables (RADC) como una plataforma de preservación digital en un entorno de gestión de archivos con el fin de mantener los documentos de archivo digitales auténticos accesibles y a largo plazo. **Metodología:** Investigación exploratoria, bibliográfica y documental, teniendo como principales fuentes documentales y bibliográficas el material resultante de las fases del Proyecto InterPARES, las normas del Consejo Nacional de Archivos y artículos científicos de investigadores nacionales e internacionales. **Resultados:** Presentación y discusión de conceptos clave relacionados con los repositorios de archivo digital de confianza, tales como repositorios digitales, repositorios de archivo digital, repositorios digitales de confianza, cadena de custodia digital de archivo y cadena de preservación. **Conclusiones:** Es necesario mirar el RDCA, es decir, el archivo digital permanente, como el lugar donde se implementan las referencias consolidadas y actuales de una preservación digital sistémica.

**Descriptores:** Archivística. Repositorios de archivo digital. Preservación digital.

**Recebido em:** 07.11.2019

**Aceito em:** 31.05.2020