

Resumo: Este estudo sintetiza conhecimentos sobre as transformações do pacote de informação do modelo Open Archival Information System (OAIS), no âmbito de uma Cadeia de Custódia Digital Arquivística (CCDA). Assim, discute-se a importância de o sistema de arquivos ser composto por plataformas de gestão, preservação e acesso. A metodologia parte do levantamento de materiais previamente publicados, contemplando: livros, publicações técnicas e artigos de periódicos científicos. A análise dos dados coletados consiste em uma triangulação entre a Arquivística, o modelo OAIS e a CCDA. A discussão utiliza a lógica dedutiva, que resulta em um artigo de revisão assistemática. Por fim, defende-se que estabelecer uma CCDA permitirá que as transformações do pacote de informação do OAIS sejam realizadas por um custodiante confiável capaz de assegurar a manutenção da autenticidade e a preservação dos documentos arquivísticos digitais no longo prazo.

Palavras-chave: Custodiante confiável; Documento digital; Preservação digital; Repositório Digital Confiável.

Abstract: This study synthesizes knowledge about the transformations of the information package of the Open Archival Information System (OAIS) model, within the scope of a Chain of Custody for Digital Archives (CCDA). Thus, the importance of the file system being composed of management, preservation and access platforms is discussed. The methodology is based on a survey of previously published materials, including: books, technical publications and articles from scientific journals. The analysis of the collected data consists of a triangulation between Archival Science, the OAIS model and the CCDA. The discussion uses deductive logics, which results in an unsystematic review article. Finally, it is argued that establishing a CCDA will allow the transformations of the OAIS information package to be carried out by a reliable custodian capable of ensuring the maintenance of the authenticity and the preservation of digital archival records in the long term.

Keywords: Trusted custodian; Digital record; Digital preservation; Trustworthy Digital Repository.

1. Introdução

A constante evolução das tecnologias de informação proporciona um momento de reformulação das bases teóricas da Arquivística. Com o advento dos documentos digitais, surge a necessidade de adaptar e desenvolver teorias para comportar os universos “analógico” e “digital”. Observa-se que esse processo de reformulação atinge tanto a teoria, quanto a prática, e consequentemente, surgem diversas discussões e questionamentos em relação à abordagem dos documentos arquivísticos em ambiente digital.

Nesse sentido, as práticas de gestão e de preservação do patrimônio digital ganham relevância devido ao crescente volume de documentos digitais produzidos. Ressalta-se que a preservação digital ainda não possui um *corpus* teórico demarcado, logo, os profissionais da área devem propor respostas, mesmo que estas sejam provisórias, com o propósito de salvaguardar tais documentos.

A preservação digital se configura como um dos principais desafios da Arquivística contemporânea. Cada vez mais documentos digitais são produzidos e essa produção acelerada é inversamente proporcional às práticas de preservação em longo prazo. Tal fato se caracteriza como uma ameaça à memória digital das sociedades contemporâneas, que dependem das tecnologias e dos documentos digitais para evoluir e disponibilizar conhecimentos para as futuras gerações.

No cenário atual, já existem metodologias para minimizar os efeitos da obsolescência tecnológica, como por exemplo, as estratégias de preservação, os padrões de metadados e os repositórios digitais. Tais ações têm o objetivo de preservar e garantir acesso em longo prazo aos documentos arquivísticos digitais. Em resumo, as estratégias mantêm as condições de acesso à informação, os metadados registram elementos de autenticidade, e o repositório digital gerencia de forma sistemática as ações proferidas sobre a documentação; isso inclui gerir estratégias e metadados.

Tal responsabilidade deve ser pautada em um Repositório Digital Confiável (RDC), capaz de garantir a preservação e o acesso em longo prazo a documentos autênticos. Para atingir tal expectativa é necessário manter a conformidade com padrões amplamente aceitos pela comunidade de preservação, especialmente com o modelo Open Archival Information System (OAIS). O modelo OAIS é considerado o principal padrão de referência em preservação digital, e tornou-se a Norma ISO 14.721:2012.

No âmbito da Arquivística será necessário um RDC com capacidade para registrar e garantir requisitos essenciais como: autenticidade, organicidade, proveniência, custódia e unicidade. Logo, deve-se implementar um Repositório Arquivístico Digital Confiável (RDC-Arq), que corresponde a um RDC que contempla as especificidades da disciplina arquivística.

Portanto, o RDC-Arq será responsável por reunir os documentos e suas informações relacionadas por meio de pacotes de informação, que são sistematicamente transformados conforme as necessidades de aquisição, armazenamento e disseminação. Para fins deste estudo, são discutidas as transformações dos pacotes de informação no âmbito de uma Cadeia de Custódia Digital Arquivística (CCDA). Assim, tem-se por objetivo sintetizar conhecimentos do OAIS e da Arquivística, visando uma convergência na implementação do RDC-Arq.

A definição de CCDA parte de uma linha de custódia ininterrupta em ambiente digital, então auditada por uma cadeia de preservação ou procedimento com garantia equivalente. Em caso de um evento crítico, como é a alteração da custódia, será preciso garantir a presunção de autenticidade. Portanto, é preciso que sejam geradas evidências para apoiar a presunção de autenticidade, e assim, comprovar que não ocorreram modificações ou corrupções em aspectos essenciais dos documentos (GAVA e FLORES, 2020).

A metodologia consiste no levantamento bibliográfico de materiais previamente publicados, contemplando: livros, publicações técnicas e artigos de periódicos científicos recuperados pela ferramenta de busca Google Scholar. Os dados coletados são analisados por meio da triangulação dos temas (Arquivística, OAIS e CCDA) e a discussão segue a lógica dedutiva. Consequentemente, obtém-se um artigo de revisão assistemática, com a finalidade de proporcionar reflexão sobre o tema, e ponderar sobre o ponto de vista dos autores (GIL, 2010; LUNA, 1997; SILVA e MENEZES, 2005; VOLPATO *et al.*, 2013).

Inicialmente, descrevem-se brevemente as responsabilidades de um repositório digital em conformidade com o modelo OAIS. Posteriormente, são perpassadas as transformações proferidas sobre o pacote de informação. E por fim, ocorre uma reflexão sobre a confiabilidade desse processo no contexto de uma CCDA visando garantir a autenticidade dos documentos arquivísticos digitais. Logo, adotam-se os seguintes elementos para a discussão: presunção da autenticidade dos documentos; e a confiabilidade dos métodos e dos sistemas informatizados para a custódia documental.

2. Modelo OAIS e Arquivística

A responsabilidade pela documentação compete ao preservador formalmente declarado. Logo, recai sobre ele a necessidade de implementar os requisitos para tal, de modo que julga-se necessário um RDC-Arq em conformidade com o modelo OAIS para preservar e garantir acesso contínuo em longo prazo a documentos arquivísticos autênticos.

O modelo OAIS consiste em um esquema conceitual que determina e sistematiza um RDC genérico, que tem por objetivo preservar e garantir o acesso em longo prazo à informação¹ digital (BAGGIO e FLORES, 2013; THOMAZ e SOARES, 2004). No âmbito da Arquivística, o OAIS consiste em um arquivo permanente digital e, para tornar-se um RDC-Arq, deverá abarcar requisitos considerados essenciais, como, por exemplo, organicidade e proveniência.

Há uma série de responsabilidades obrigatórias determinadas pelo modelo OAIS (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012). Desta forma, um RDC-Arq deverá contemplar os seguintes requisitos:

- Negociar e aceitar informações adequadas junto ao produtor;
- Obter o controle das informações fornecidas para garantir a preservação em longo prazo;
- Participar da definição da comunidade designada², e estabelecer sua base de conhecimento para compreender as informações fornecidas;

¹ O modelo OAIS utiliza o termo “informação” comum em diversas áreas, como, por exemplo, Administração, Arquivologia, Biblioteconomia, Ciência da Computação e Museologia. Portanto, este estudo utiliza os termos “documento” e “informação” como sinônimos, para assim, diminuir barreiras terminológicas entre as áreas. Tal escolha se justifica, pois, no OAIS a “informação” é qualquer conhecimento intercambiável. Logo, o RDC-Arq em conformidade com o OAIS será responsável por preservar “documentos arquivísticos digitais” (informações registradas em um suporte) que foram produzidos ou recebidos no decorrer das atividades administrativas de uma organização, pessoa ou família; e que são considerados de guarda permanente, por uma razão informacional, probatória ou histórica.

² Conjunto identificado de usuários potenciais capazes de entender um conjunto específico de informações. A comunidade designada pode ser composta por várias comunidades de usuários. Logo, o arquivo definirá a comunidade designada, mesmo que essa definição possa mudar com o tempo (CCSDS, 2012; ISO 14.721:2012). No entanto, no âmbito da Arquivística, essa distinção de público não ocorre de forma rígida. O acesso à informação preservada é oferecido para quaisquer usuários

- Garantir que a comunidade designada é capaz de compreender as informações preservadas sem necessidade de recursos especiais ou do auxílio dos produtores;
- Seguir políticas e procedimentos previamente documentados demonstrando confiabilidade na preservação da informação, além de restringir a exclusão de *itens*, exceto que permitido como parte de uma estratégia aprovada;
- Disponibilizar a informação preservada à comunidade designada, permitindo disseminá-la como cópia ou rastreável³.

Tais responsabilidades enfatizam a aquisição, o acesso e a confiabilidade da informação digital. Dessa forma, é possível obter direitos para realizar as atividades de preservação em longo prazo e disseminar as informações para as partes interessadas, as comunidades designadas. Assim, estima-se que essas comunidades sejam capazes de interpretar as informações preservadas sem a necessidade de se recorrer a métodos complexos e específicos.

As responsabilidades irão definir o que será preservado e o respectivo direito para tal. Além de manter procedimentos para preservar e definir quem poderá usufruir desse material. Assim, o modelo OAIS subentende a necessidade de assegurar a posse legal da informação digital, bem como conhecer previamente a existência de uma comunidade potencialmente interessada na preservação, e garantia de acesso ininterrupto à informação.

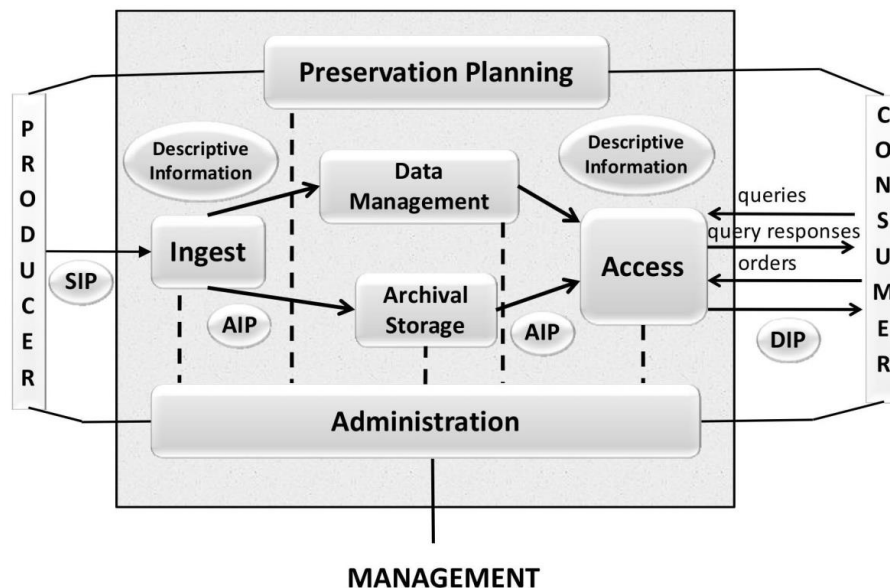
Com relação ao ambiente OAIS há seis entidades funcionais internas, que são: admissão (*ingest*), armazenamento arquivístico (*archival storage*), gestão de dados (*data management*), administração (*administration*), planejamento de preservação (*preservation planning*) e acesso (*access*). E três entidades externas, que são: produtor (*producer*), administrador (*management*) e consumidor (*consumer*).

Nesse ambiente, perpassam respectivamente, os pacotes de informação para submissão, armazenamento e disseminação (*Submission Information Package – SIP*, *Archival Information Package – AIP* e *Dissemination Information Package – DIP*), nos quais são inseridas as informações descritivas (*descriptive information*) referentes às suas respectivas informações de conteúdo. A seguir, a Fig. 1 apresenta uma esquematização simplificada da relação entre indivíduos, entidades funcionais e pacotes de informação.

que tenham interesse na informação de conteúdo. A visão arquivística da comunidade designada corresponde ao arquivo e seus usuários potenciais, ou seja, não há restrição de público. O objetivo é atender os usuários interessados, de modo que estes sejam capazes de interpretar corretamente as informações preservadas.

³ Capacidade de apontar para o objeto de dados originalmente submetido junto com os demais elementos que comprovam a sua autenticidade.

Fig. 1 – Entidades funcionais do OAIS



Fonte: CCSDS, 2012:4-1).

Observa-se que o produtor (*producer*) se refere às pessoas ou sistemas que fornecem a informação que será preservada por meio da submissão de SIP. O administrador (*management*) se refere àqueles que estabelecem as políticas gerais que governam o repositório via entidade interna administração (*administrator*).

Dessa forma, os SIP são transformados em AIP para serem arquivados. Já o consumidor (*consumer*) se refere às pessoas ou sistemas que interagem com os serviços oferecidos pelo OAIS para acessar a informação preservada por meio da entidade de acesso (*access*). Logo, para atender as demandas de acesso, o repositório irá gerar pacotes DIP, os quais são compostos por formatos de arquivos mais “simples e leves”, ideais para disseminação via Internet.

Após o produtor (*producer*) submeter o SIP, a entidade de admissão (*ingest*) irá verificar a conformidade do pacote com os modelos previamente definidos nas políticas de preservação junto à entidade planejamento da preservação (*preservation planning*). Em caso de não conformidade, o SIP será rejeitado. Caso o SIP esteja de acordo com estas políticas, a entidade de administração (*administrator*) irá realizar a admissão dos seus conteúdos.

Posteriormente, a informação descritiva (*descriptive information*) será inserida, com objetivo de registrar o histórico de custódia dos objetos digitais. Isso possibilita relatar quaisquer alterações realizadas juntamente com as informações adicionais utilizadas para preservação e garantia de acesso. Assim, o SIP é transformado em AIP e encaminhado à entidade de armazenamento arquivístico (*archival storage*).

Neste estágio, a entidade de armazenamento arquivístico (*archival storage*) torna-se responsável por preservar os AIP, enquanto a entidade gestão de dados (*data management*) irá gerenciar as informações descritivas dos objetos digitais. Assim, a gestão

de dados (*data management*) manterá um banco de dados atualizado sobre as informações relativas aos AIP, corroborando com a manutenção da autenticidade, preservação e garantia de acesso contínuo no longo prazo.

A entidade de acesso (*access*) é a meio de comunicação entre o consumidor (*consumer*) e o OAIS, e pode ser contatada via plataforma de acesso. Neste ponto, ressalta-se que o consumidor (*consumer*) não tem acesso direto aos AIP armazenados na entidade armazenamento arquivístico (*archival storage*). A interação é limitada à plataforma de acesso, comunicando-se indiretamente por intermédio da entidade de acesso (*access*). Tal procedimento configura-se como um fluxo de informação pertinente do OAIS, visto que adiciona maior controle às ações e minimiza os riscos de invasão.

Dessa forma, o consumidor solicita acesso a determinado conteúdo e, assim, a entidade de acesso (*access*) encaminha a solicitação. O resultado da solicitação é enviado ao consumidor (*consumer*) pela entidade de acesso (*access*) via DIP; que segue as políticas de preservação e acesso, definidas respectivamente, pelas entidades do plano de preservação (*preservation planning*) e de administração (*administrator*).

Em resumo, as responsabilidades do OAIS estão relacionadas às políticas de preservação digital, já o fluxo de informação, por meio das entidades, está relacionado ao gerenciamento dos objetos digitais admitidos, custodiados e disseminados. Após esta breve explanação do OAIS, procede-se a contextualização das transformações dos pacotes de informação, visando salvaguardar documentos arquivísticos em um RDC-Arq.

3. Transformações do pacote de informação em um RDC-Arq

Durante o ciclo de vida documental (relação entre produtor, OAIS e consumidor) ocorrerão transformações lógicas e/ou físicas nos pacotes de informação e em seus respectivos objetos associados. Sendo assim, a seguir, discutem-se as transformações nas entidades: produtor (*producer*), admissão (*ingest*), armazenamento arquivístico (*archival storage*), gestão de dados (*data management*) e acesso (*access*); e no próprio fluxo de dados.

3.1. Transformações de dados na entidade produtor

Os dados sob custódia na entidade do produtor são, por natureza, dados privados, e podem estar em qualquer formato que seja desejado (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012). Dessa forma, há possibilidade de uma variada gama de formatos de arquivos, originados de diversos *softwares*, e por vezes, sem a conformidade com os padrões recomendados para preservação de longo prazo.

No entanto, quando se decide armazenar esses dados no OAIS, o produtor deve reunir-se com os arquivistas a fim de negociar um acordo de submissão que defina questões como o conteúdo, o formato e as datas programadas para receber os SIP. Posteriormente, o repositório procede a execução das atividades de preservação definidas em sua política.

Observa-se que a preservação digital representa um desafio técnico e organizacional que necessita de um envolvimento contínuo, visto que a informação digital não poderá sobreviver de forma inerte (SAYÃO, 2010). Sendo assim, após perpassar as fases corrente e intermediária, por vezes, será preciso converter o formato dos documentos que

necessitam de guarda permanente ou preservação de longo prazo, para que assim seja possível assegurar a sua compatibilidade com os sistemas informatizados (SANTOS, 2005). Portanto, cabe ao RDC-Arq realizar as migrações/conversões adequadas para garantir a preservação dos documentos.

3.2. Transformações de dados na entidade admissão

O processo de admissão (*ingest*) transforma os SIP recebidos em um conjunto de AIP e descrições de pacote que podem ser aceitos, e consequentemente, armazenados pelas entidades armazenamento arquivístico (*archival storage*) e gestão de dados (*data management*). Observa-se que a complexidade do processo de admissão pode variar consideravelmente, conforme as peculiaridades do OAIS e do produtor.

A entidade de admissão (*ingest*) irá classificar os objetos de informação recebidos em categorias; posteriormente, determinar em quais coleções existentes cada objeto se enquadra; e, por fim, armazenar o AIP na entidade armazenamento arquivístico (*archival storage*). Tão logo, a entidade de admissão (*ingest*) emitirá mensagens solicitando a atualização das respectivas descrições das coleções (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012).

Espera-se que a entidade de admissão (*ingest*) coordene atualizações entre as entidades armazenamento arquivístico e gestão de dados. Portanto, será possível fornecer o gerenciamento e a recuperação de erros de forma adequada.

Desta forma, o AIP deverá, inicialmente, ser armazenado na entidade armazenamento arquivístico; em seguida, como confirmação dessa operação, deve ser incluída uma identificação única para recuperar esse AIP e, por fim, este identificador será incorporado pela descrição do pacote antes de ser inserido na descrição de coleções na entidade de gestão de dados (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012).

Ao associar informações contextuais aos documentos digitais é possível registrar a proveniência, assim como, demais anotações explicativas que podem ser compreendidas por meio de normas e padrões de metadados que tornam a informação facilmente legível (ROTHENBERG, 1999). Os metadados atuam como descritores, contribuindo para contextualização e verificação da autenticidade dos documentos digitais.

Os metadados de preservação devem ser identificados e/ou criados no momento da captura dos documentos digitais. Tal procedimento agrega confiabilidade e demarca o contexto a fim de permitir o gerenciamento dos documentos no longo prazo. Sendo assim, tais metadados devem fornecer informações sobre o conteúdo, a estrutura e o contexto no qual os documentos foram criados (CASTRO, CASTRO e GASPARIAN, 2007).

O estágio de admissão é fundamental para registrar informações pertinentes à alteração de custódia, caso existam. Esse é o momento em que os documentos arquivísticos são transferidos/recolhidos formalmente dos sistemas informatizados de gestão para o RDC-Arq, o qual se tornará seu ambiente de preservação e custódia.

3.3. Transformações de dados nas entidades armazenamento arquivístico e gestão de dados

A entidade armazenamento arquivístico recebe os AIP gerados no processo de admissão, que são acrescentados aos conteúdos permanentes do OAIS. Já a entidade gestão de dados recebe as descrições de pacotes gerados no processo de admissão e amplia as descrições de coleções existentes, para então, incluir seu conteúdo.

Tais descrições são fundamentais para manter a autenticidade, pois visam assegurar o acesso e a utilização dos documentos, a fim de permitir a recuperação eficiente. Além disso, mantém o elo entre os documentos e o seu contexto de produção por meio de ligações estruturadas e facilmente compreensíveis. Igualmente, os metadados podem fornecer informações sobre possíveis dependências tecnológicas, tendo em vista a minimização desses entraves à preservação de longo prazo (CASTRO, CASTRO e GASPARIAN, 2007).

A visão interna do OAIS consiste na representação permanente dos dados armazenados, de modo que todas as codificações e mapeamentos devem ser devidamente registrados e compreendidos. A transferência dos objetos admitidos normalmente é realizada por um *software*, logo, o OAIS tem a responsabilidade de manter uma cópia desse *software* ou a documentação criteriosa dos formatos de arquivos que possuir. Dessa forma, será possível realizar transferências para outros sistemas no futuro, sem perda de informação, mesmo que ocorram erros com o *software* que realiza as transferências (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012).

Observa-se que a preservação em um RDC-Arq que segue o OAIS deve ter um caráter sistemático, ou seja, seguir normas e definir claramente os *softwares* utilizados no decorrer das atividades. A questão central concentra-se em desenvolver alternativas para os problemas decorrentes da obsolescência tecnológica que podem ocorrer.

Caso ocorra algum problema com os *softwares* utilizados para conversão, transferência ou monitoramento, o RDC-Arq deve ser capaz de substituí-los e retomar o processo de preservação sem maiores danos aos documentos custodiados. Logo, o RDC-Arq deve ser suscetível a mudanças em sua própria estruturada técnica e operacional.

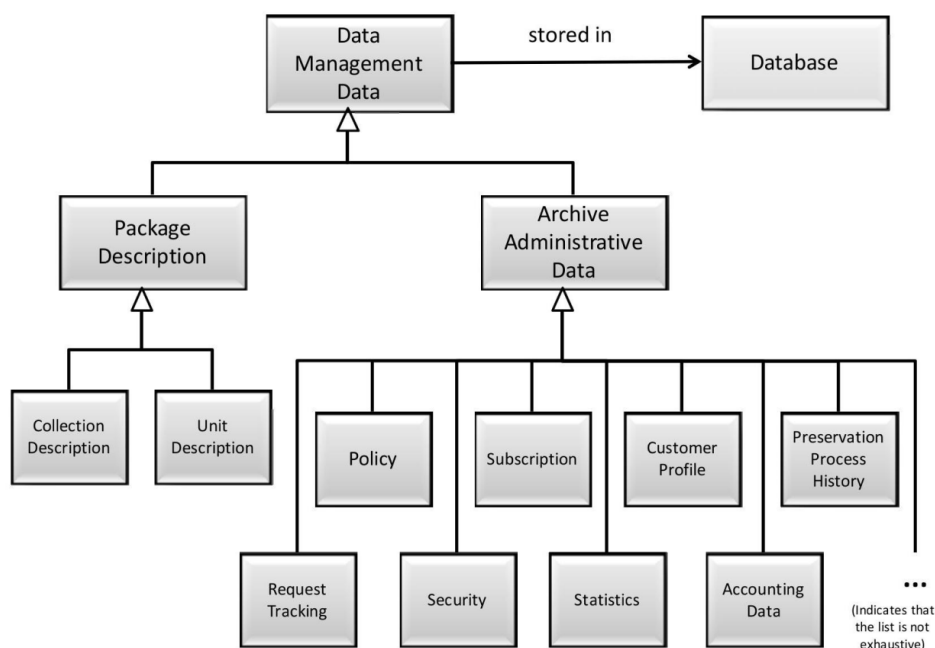
3.3.1. Informações para gestão de dados

As descrições de pacotes são armazenadas em uma área permanente, que pode ser comparada aos sistemas gerenciadores de banco de dados que facilitam o acesso e a atualização das descrições associadas. Observa-se que além das descrições de pacotes, todas as informações necessárias à operação do OAIS podem ser armazenadas em bancos de dados com classes de dados permanentes (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012).

Desta forma, um RDC-Arq em conformidade com o OAIS poderá utilizar a infraestrutura da gestão de dados para armazenar informações referentes ao seu próprio funcionamento. Ou seja, armazenar informações sobre suas configurações como, por exemplo, políticas, registros de usuários, estatísticas e informações contábeis.

Os dados administrativos do arquivo representam o conjunto de informações necessárias para operação rotineira do OAIS. A seguir, a Fig. 2 ilustra os vários tipos desta informação de gerenciamento no OAIS.

Fig. 2 – Informação para gestão de dados



Fonte: (CCSDS, 2012:4-50).

Conforme a figura, os dados para gestão de dados (*data management data*) são armazenados em uma base de dados (*database*); além disso, subdividem-se em descrição do pacote (*package description*) e dados administrativos do arquivo (*archive administrative data*). Por sua vez, os dados administrativos do arquivo podem-se subdividir em diversas categorias conforme as necessidades da entidade gestão de dados, dentre elas:

- a) Políticas (*policy*):** os custos, a disponibilidade e as restrições para solicitar informações arquivadas;
- b) Acompanhamento das requisições (*request tracking*):** usuários e registro do progresso de cada transação;
- c) Segurança (*security*):** inclui nomes de usuário, senhas e demais mecanismos de autenticação;
- d) Solicitações programadas (*subscription*):** fornecem suporte para repetir os pedidos futuros;
- e) Estatística (*statistics*):** fornece dados quantitativos para entidade de administração com a finalidade de determinar futuras políticas e ajustar o desempenho do OAIS com objetivo de melhorar a eficiência das operações;
- f) Histórico do processo de preservação (*preservation process history*):** rastreia as migrações, alteração de suporte e demais transformações no AIP;
- g) Perfil do consumidor (*customer profile*):** armazena informações básicas do consumidor que não necessitam ser informadas em solicitações futuras;

- h) Contábil** (*accounting data*): inclui os dados necessários ao funcionamento do OAIS enquanto parte de um sistema de negócio.

Observa-se que além de assegurar a preservação dos documentos arquivísticos digitais autênticos no longo prazo, o RDC-Arq necessita armazenar os dados relativos ao seu funcionamento de forma segura. Para isso, utiliza a entidade gestão de dados, a qual irá gerenciar as informações necessárias à administração do sistema e armazená-las em uma base de dados.

Tais informações possuem uma estreita relação com a administração, visto que se referem a questões gerenciais, como: políticas, segurança, estatísticas, desempenho da preservação e atendimento ao usuário. Portanto, compete ao RDC-Arq preservar os documentos e as suas próprias configurações.

3.4. Sub-título

Um instrumento de busca poderá ser usado quando o consumidor deseja localizar informações de interesse no OAIS. Logo, se estabelece uma relação de pesquisa com a entidade de acesso. Esses instrumentos permitem que os consumidores possam selecionar o AIP de interesse e proceder à solicitação.

O uso de taxonomia pode otimizar a busca, por sua capacidade de representar conceitos, agilizar a comunicação entre produtores e consumidores da informação. Além disso, controla a diversidade de expressões, de modo a evitar ambiguidades (LUZ, 2010). O arquivo terá por objetivo, possibilitar que o consumidor tenha acesso pleno à informação para usufruí-la, de modo que possa consultar os documentos e realizar uma cópia (BERTOLETTI, 2002). Logo, um AIP pode ser precisamente localizado por meio da taxonomia, e a sua cópia pode ser disponibilizada pelo RDC-Arq na forma de DIP.

Dessa forma, o consumidor obtém uma visão lógica dos AIP desejados e de suas respectivas descrições de pacote associadas que devem ser incluídas no DIP. Além disso, o consumidor pode especificar detalhes desejados, como o tipo de mídia e o formato do objeto digital (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012).

Para melhorar a eficiência do acesso, os arquivistas precisam compreender o que os consumidores/pesquisadores desejam, de modo que possam ajudar a responder dúvidas relacionadas a pesquisa (CASTRO, 2008). Sendo assim, é pertinente que haja um serviço de suporte, para auxiliar os consumidores a utilizarem a plataforma de acesso do RDC-Arq. Após compreender o funcionamento da ferramenta, os consumidores vão confiar mais no sistema de preservação, e consequentemente, melhorar a precisão dos resultados de suas buscas.

A entidade de acesso irá registrar a solicitação na entidade gestão de dados e, posteriormente, coordenar a resposta assim que a solicitação puder ser plenamente atendida. A maioria dessas solicitações será atendida plenamente, caso contrário, a entidade de administração irá notificar a entidade de acesso quando os conteúdos estiverem disponíveis para entrega. Dessa forma, a entidade de acesso irá contatar as entidades armazenamento arquivístico e gestão de dados, e solicitar os AIP e as descrições de pacotes associadas para gerar o DIP e entregar a solicitação ao consumidor. Para isso, as entidades armazenamento arquivístico e gestão de dados criam cópias dos objetos

solicitados na área de armazenamento temporário (ABNT/NBR 15.472:2007; CCSDS, 2012; ISO 14.721:2012).

O RDC-Arq é isolado de interação direta com usuários e sistemas externos, para minimizar possíveis invasões. Isso é possível ao utilizar uma plataforma de acesso pela qual os usuários podem solicitar acesso aos documentos. Esse procedimento eleva os níveis de segurança, pois, o RDC-Arq será monitorado constantemente e os usuários não terão acesso direto aos conteúdos originais nele custodiados.

A entidade de acesso transforma os AIP e as respectivas descrições de pacote associadas em um conjunto de DIP. Salienta-se que a complexidade desse processo de transformação pode variar consideravelmente em virtude do nível dos serviços de processamento oferecidos pelo OAIS e solicitados pelo consumidor. Conforme observado, há um duplo objetivo nas transformações dos pacotes de informação: a preservação e a garantia de acesso.

Ao atender demandas de acesso, o RDC-Arq apenas envia uma cópia autêntica das informações solicitadas à plataforma de acesso e difusão. Portanto, o público geral irá interagir somente com a plataforma de acesso, na qual solicitam os AIP de interesse. As solicitações serão analisadas e, em caso de deferimento, o RDC-Arq entrega o DIP correspondente ao AIP solicitado. Já nos casos de indeferimento da solicitação, o RDC-Arq encaminha a justificativa com base em suas políticas de preservação definidas *a priori*.

Caso a plataforma de acesso seja invadida não ocorrerão danos às informações custodiadas pelo RDC-Arq em virtude do seu armazenamento *offsite*⁴. Dessa forma, a plataforma de acesso pode ser recuperada, com as versões mais recentes dos DIP, seja em caso de desastres, erros acidentais, invasões ou falhas do sistema. Consequentemente, o armazenamento *offsite* irá proteger o RDC-Arq contra tais invasões. No entanto, para agregar confiança sobre esses métodos, será preciso desenvolver uma CCDA para garantir a autenticidade dos documentos arquivísticos e das informações gerenciais.

4. Cadeia de Custódia Digital Arquivística

Os documentos arquivísticos, em sua trajetória administrativa e histórica, perpassam por três fases, que são: corrente, intermediária e permanente. Dessa forma, têm-se ambientes distintos: o de gestão documental, o de preservação e o acesso. Nos ambientes de gestão e de preservação são realizadas as ações necessárias para o correto tratamento dos documentos arquivísticos, já o ambiente de preservação é o meio de interação entre o Arquivo e o público geral.

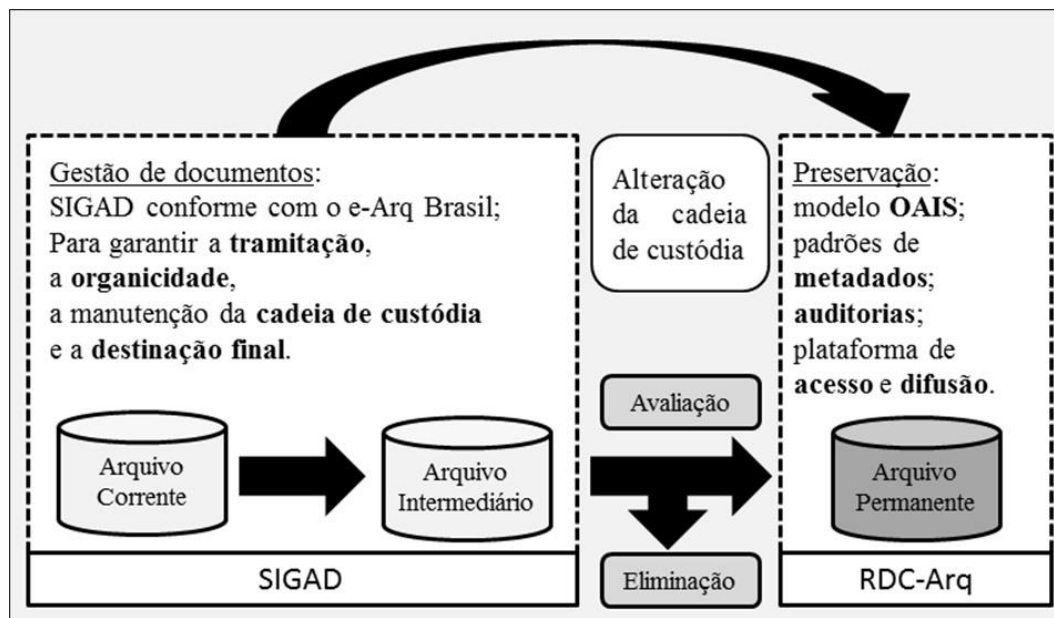
Dessa forma, torna-se necessário constituir a plataforma de gestão, a plataforma de preservação e a plataforma de acesso. Consequentemente faz-se necessário implementar o Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e o RDC-Arq,

⁴ Estratégia de envio de dados críticos para fora do local principal, frequentemente utilizada como parte de um plano de recuperação de desastres. Consiste em transportar os dados para fora do local usando mídia de armazenamento removível ou serviço de *backup* remoto.

ambos envolvidos em uma CCDA. Logo, o SIGAD será responsável pelas fases corrente e intermediária, e o RDC-Arq será responsável pela fase permanente, além de interagir com a plataforma de acesso e difusão.

Inicialmente, ressalta-se que o processo de preservação digital começa antes mesmo da submissão dos documentos arquivísticos ao RDC-Arq. Isso requer a pré-existência de um SIGAD capaz de garantir a manutenção da autenticidade dos documentos. Assim, o SIGAD deverá seguir padrões recomendados pela comunidade arquivística em sua implementação, como por exemplo, o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil)⁵. Logo, a interoperabilidade entre o SIGAD e o RDC-Arq permite constituir uma CCDA na qual há um relacionamento entre os padrões e-Arq Brasil e OAIS. A seguir, a relação entre os sistemas informatizados é esquematizada na Fig. 3.

Fig. 3 – Custódia dos Documentos Arquivísticos Digitais



Fonte: Adaptado de Flores, Rocco e Santos, 2016:128.

No sistema de arquivos, o SIGAD será responsável pela tramitação dos documentos, e deverá manter questões como proveniência, classificação e organicidade. Além disso, o SIGAD deve implementar rotinas para presunção de autenticidade a fim de garantir que não ocorreram alterações “não autorizadas” ou “não registradas” sobre os documentos. Logo, o SIGAD deverá armazenar os documentos em uma base de dados constantemente monitorada a fim de agregar confiança.

⁵ Equivalente a ISO 15.489.

Depois de encerrado o valor primário dos documentos nas fases corrente e intermediária, esses serão avaliados pelo SIGAD com base nos prazos estabelecidos por uma Tabela de Temporalidade de Documentos (TTD). Dessa forma, a TTD irá estabelecer os prazos de guarda e a destinação a serem seguidos.

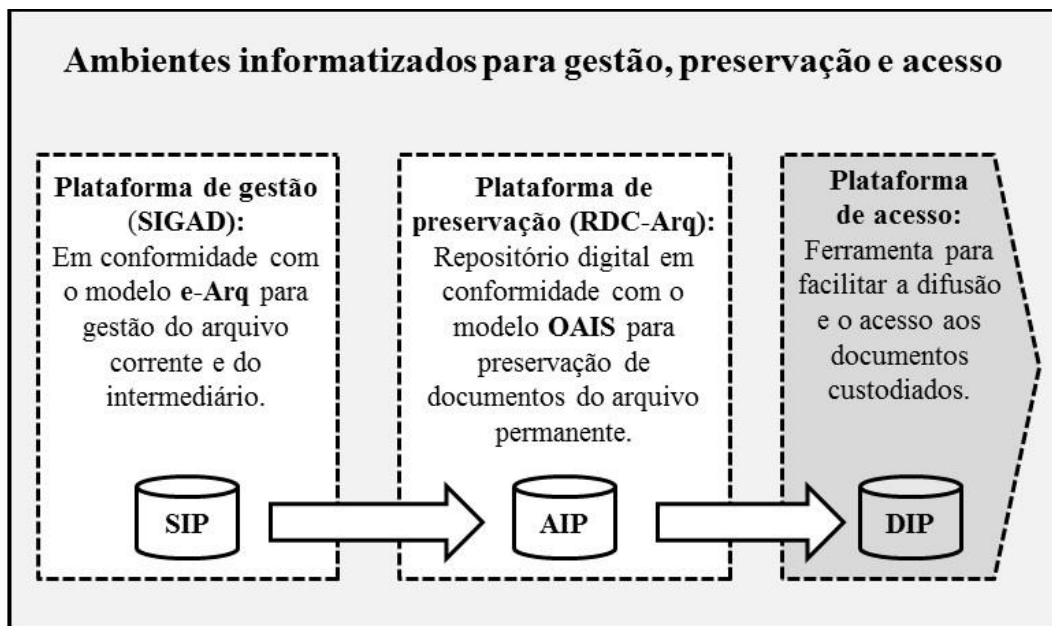
Com a TTD é possível eliminar o “lixo digital”, então considerado um empecilho significativo à preservação de documentos digitais em virtude do espaço lógico de armazenamento ocupado. Portanto, a eliminação de documentos digitais, conforme a tabela de temporalidade deve ocorrer mediada pelo arquivista, logo, as eliminações automáticas devem ser evitadas (INNARELLI, 2012).

Consequentemente, os documentos que possuírem um valor secundário (valor histórico, social, probatório ou informativo) serão recolhidos ao RDC-Arq. Portanto, os demais os documentos, que já cumpriram seu valor imediato, e que não possuem valor secundário, serão eliminados pelo SIGAD conforme a TTD. Assim, o RDC-Arq, em conformidade com o OAIIS e os princípios arquivísticos, será entendido como o responsável por preservar e garantir o acesso contínuo no longo prazo.

A interoperabilidade entre SIGAD e RDC-Arq necessita de automatização, tanto para evitar possíveis manipulações não autorizadas, quanto para evitar inserções indevidas de documentos ou de pacotes de informação. O objetivo dessa automatização é assegurar que o RDC-Arq só admitirá materiais que estejam contemplados pela CCDA, reduzindo a margem para adulterações ou inserções de conteúdos inautênticos. Ressalta-se que tal interoperabilidade consiste em usar padrões compatíveis que permitem a comunicação entre os sistemas como, por exemplo, os padrões de metadados e os padrões de empacotamento (FLORES, ROCCO e SANTOS, 2016).

Deve haver compatibilidade entre os padrões de metadados e os pacotes de informação utilizados no SIGAD, no RDC-Arq e na plataforma de acesso. Dessa forma, será possível automatizar a comunicação entre os sistemas informatizados dos produtores, preservadores e consumidores, aumentando os níveis de confiabilidade dos sistemas. A seguir a Fig. 4 esquematiza a relação interoperável entre SIGAD, RDC-Arq e plataforma de acesso.

Fig. 4 – Ambientes informatizados para gestão, preservação e acesso



Fonte: Flores, Rocco e Santos, 2016:129.

A relação interoperável apresentada entre os pacotes de informação (SIP, AIP e DIP) requer a compatibilidade normativa entre o e-Arq Brasil e o OAIS. Tal compatibilidade irá se refletir no SIGAD, no RDC-Arq e na plataforma de acesso. Para tanto, o padrão de metadados utilizado deve contemplar elementos pertinentes à administração, preservação, descrição e acesso. Logo, um padrão de metadados compatível adiciona confiabilidade tanto ao processo de recolhimento, quanto na perspectiva de acesso; além disso, evita o retrabalho.

No entanto, a transferência/recolhimento é um ponto crítico para a autenticidade dos documentos em ambiente digital. Tal fato se justifica, pois os documentos digitais são vulneráveis de modo que podem ser facilmente alterados sem deixar vestígios aparentes.

Dessa forma, é preciso implementar rotinas de monitoramento, que incluem trilhas de auditoria, a fim de verificar a integridade dos documentos que são transferidos/recolhidos da base de dados do SIGAD para o RDC-Arq. Tal monitoramento gera confiança no processo de preservação e deve estar implícito nas rotinas do sistema de arquivos. Com isso, pode-se elevar a confiança dos métodos empregados, além de fortalecer as evidências da CCDA.

A custódia, portanto, diz respeito à transmissão dos arquivos ao longo do tempo, de produtores para outros produtores, de acordo com as mudanças administrativas, até o arquivista. O arquivista faz parte da transmissão da custódia e, portanto, ao receber os documentos, que serão preservados sob sua guarda, ele mantém essa linha idônea de responsabilidades, porque é um dos seus legítimos sucessores (SILVA, 2017:179).

Ressalta-se que o arquivista executa um julgamento imparcial no que se refere a preservação da prova. Limita seu interesse a guarda de documentos que representam um

testemunho pertinente. Portanto, não há interesse de tomar ações em caráter favorável ou desfavorável à administração (SCHELLENBERG, 2006). O arquivista não compartilha dos mesmos interesses que as partes envolvidas no conteúdo dos documentos. Logo, pode ser considerado próximo da neutralidade, capaz de realizar um julgamento imparcial, embora tal afirmação seja temerária.

As visões de Silva (2017) e Schellenberg (2006) permitem ponderar que o arquivista é o legítimo sucessor dos documentos. Durante a fase de avaliação, sua responsabilidade consiste em discernir entre os documentos passíveis de eliminação e os que devem ser preservados em caráter permanente. Para os documentos em ambiente digital, chama-se atenção para a transferência/recolhimento que será realizada do SIGAD ao RDC-Arq. Esse é o principal ponto crítico da custódia, pois quaisquer ausências de monitoramento, por menor que seja o intervalo de tempo, serão suficientes para “pôr em xeque” a autenticidade.

Sendo assim, a CCDA para documentos em ambiente digital precisa contemplar o SIGAD e o RDC-Arq. Essa dimensão inicia-se com a captura dos documentos pelo SIGAD e se estende até o recolhimento ao RDC-Arq. Mesmo que ocorra alteração do custodiante/custodiador, devem-se implementar ferramentas de monitoramento que assegurem a confiabilidade desse processo. Portanto, a interoperabilidade entre os sistemas de gestão e preservação é fundamental para a manutenção da idoneidade da custódia.

Observa-se que a CCDA contribui para que as responsabilidades obrigatórias propostas pelo OAIS sejam cumpridas, sem que ocorra negligência em algum estágio. Da mesma forma, pode-se assegurar a confiabilidade durante as transformações do pacote de informação. Visto que haverá monitoramento contínuo, por alguém responsável, dotado de competência técnica e jurídica para exercer a função de custodiante confiável. Assim, as transformações do pacote de informação serão realizadas em um ambiente confiável, contribuindo com a presunção de autenticidade dos documentos.

Além disso, torna-se pertinente que o Arquivo disponibilize publicamente suas normas e políticas de gestão e preservação para despertar a confiança do público geral (comunidade designada, consumidores, usuários e pesquisadores). Trata-se de informar como funciona o sistema de arquivos, quais sistemas são implementados nos ambientes de gestão, preservação e acesso. No caso do RDC-Arq, por exemplo, este será um meio para que o público reconheça a confiabilidade dos métodos adotados no que tange a preservação e garantia de acesso no longo prazo.

5. Considerações finais

Este estudo concentrou-se na relação entre as transformações proferidas sobre os pacotes de informação (SIP, AIP e DIP) e a CCDA no âmbito da Arquivística. De modo que foram destacados os principais requisitos e padrões arquivísticos pertinentes a serem considerados na implementação de um sistema de arquivos confiável, capaz de contemplar os ambientes para gestão de documentos, preservação de longo prazo e acesso contínuo.

Com relação ao OAIS, foram brevemente perpassadas as responsabilidades, as entidades funcionais e as transformações dos pacotes de informação. Observou-se que a definição de um conjunto de responsabilidades obrigatórias circunscreve os requisitos mínimos que o

ambiente de preservação deve atender. Com isso, o administrador do OAIS pode definir as questões mais urgentes no desenvolvimento do RDC-Arq.

As entidades funcionais do OAIS permitem vislumbrar a sistemática de admissão, armazenamento arquivístico, gerenciamento de dados, administração do sistema, planejamento da preservação e acesso. Dessa forma, compreende-se a importância de um RDC-Arq em conformidade com o OAIS, para assim, desenvolver um ambiente confiável para realizar as transformações dos pacotes de informação, e consequentemente, garantir a autenticidade dos documentos arquivísticos digitais.

O modelo OAIS irá armazenar os próprios dados gerenciais e administrativos. Logo, será responsável por garantir a segurança de informações relativas a perfis de usuários, políticas internas, estatísticas operacionais e informações contábeis (caso seja um sistema de negócio).

Além disso, com o RDC-Arq é possível por garantir a correta interpretação/representação das informações digitais por suas respectivas comunidades designadas. Sua implementação deve considerar aspectos tecnológicos e políticos, de modo a abranger fluxos de informação, requisitos obrigatórios e entidades funcionais do OAIS. Ademais, deverá seguir princípios da Arquivística, como, por exemplo, proveniência, organicidade, custódia, unicidade e autenticidade.

Os sistemas informatizados são essenciais para garantir a confiabilidade. De modo que a implementação do SIGAD e do RDC-Arq, de forma interoperável, contribuem para manter a CCDA, capaz de contemplar o ciclo de vida dos documentos arquivísticos digitais. A confiança será adquirida mediante demonstração de conformidade com normas e padrões amplamente aceitos, tanto pela comunidade científica, quanto pelo público geral. Da mesma forma, o responsável pela custódia documental, no SIGAD e no RDC-Arq, deve ter capacidade técnica e jurídica para tal, para que seja considerado um custodiante confiável.

Entretanto, é preciso ressaltar que a custódia não consiste, em uma relação de poder sobre a documentação, mas sim em uma atribuição de responsabilidades pela sua preservação, autenticidade e garantia de acesso. Logo, a custódia em ambiente digital requer o constante monitoramento das ações, em virtude das vulnerabilidades dos documentos. Isso implica em rotinas de segurança que contemplem os pontos críticos da documentação, dentre eles: a captura dos documentos pelo SIGAD; a transferência/recolhimento do SIGAD para o RDC-Arq; e a possível alteração do responsável pela custódia.

A alteração da cadeia de custódia pode ocorrer no ato do recolhimento (do SIGAD para o RDC-Arq), ou mesmo como parte do plano de sucessão, caso o atual custodiante encerre suas atividades. Deve-se ressaltar que a alteração da custódia consiste em um meio para prolongá-la, pois visa a garantir a preservação e o acesso aos documentos, delegando a responsabilidade para alguém capaz de cumpri-la plenamente.

A manutenção da CCDA permite que as transformações dos pacotes de informação sejam realizadas em um ambiente confiável, capaz de assegurar sua idoneidade. Tal questão é comprovada pelos sistemas informatizados que monitoram e registram as alterações com auxílio de trilhas de auditoria e metadados. Esse comprometimento com a preservação digital poderá ser atestado por meio de auditorias periódicas, com objetivo de receber certificação de órgão competente, a fim de comprovar a confiabilidade dos componentes do sistema de arquivos.

Por fim, estima-se que este estudo incentive o diálogo em torno dos repositórios digitais, além de proporcionar uma aproximação entre RDC-Arq, OAIS e CCDA. Da mesma forma, fornece subsídio teórico para pesquisadores recém-iniciados e ressalta a importância de considerar a confiabilidade dos componentes do sistema de arquivos. Sua principal limitação consiste em sua natureza puramente teórica, tão logo, recomenda-se o desenvolvimento de estudos de caso a fim de retratar os possíveis descompassos entre teoria e prática.

Referências bibliográficas

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

2007 *NBR 15.472:2007: Sistemas espaciais de dados e informações: modelo de referência para um sistema aberto de arquivamento de informação (SAAI)*. Rio de Janeiro: ABNT, 2007.

BAGGIO, C. C.; FLORES, D.

2013 Documentos digitais: preservação e estratégias. *Biblos: revista do Instituto de Ciências Humanas e da Informação*. [Em linha]. 27:1 (2013) 11-24. [Consult. 13 out. 2022]. Disponível em: <https://periodicos.furg.br/biblos/article/view/2654/2395>.

BERTOLETTI, E. C.

2002 *Como fazer programas de reprodução de documentos de arquivo*. São Paulo: Arquivo Público do Estado de São Paulo, 2002.

CASTRO, A. M.; CASTRO, A. M.; GASPARIAN, D. M. C.

2007 *Arquivos: físicos e digitais*. Brasília: Thesaurus, 2007.

CASTRO, C.

2008 *Pesquisando em arquivos*. Rio de Janeiro: Zahar, 2008.

CCSDS - CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM

2012 *Reference model for an Open Archival Information System (OAIS)*. [Em linha]. Washington: CCSDS, 2012. [Consult. 13 out. 2022]. Disponível em: <http://public.ccsds.org/publications/archive/650xom2.pdf>.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M.

2016 Cadeia de custódia para documentos arquivísticos digitais. *Acervo*. [Em linha]. 29:2 (2016) 117-132. [Consult. 13 out. 2022]. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/download/717/732/>.

GAVA, T. B. S.; FLORES, D.

2020 Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. *Informação & Informação*. [Em linha]. 25:2 (2020) 74-99 [Consult. 13 out. 2022]. Disponível em: <https://brapci.inf.br/index.php/res/v/142084>.

GIL, A. C.

2010 *Como elaborar projetos de pesquisa*. 4^a ed. São Paulo: Atlas, 2010.

INNARELLI, H. C.

2012 *Instrumenta 2: Preservação de Documentos Digitais*. São Paulo: Associação dos Arquivistas de São Paulo, 2012.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

2012 *ISO 14.721:2012: space data and information transfer systems: open archival information system: reference model*. Genève: ISO, 2012.

LUNA, S. V.

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

LUZ, C.

2010 *Arquivologia 2.0: a informação digital humana*. Florianópolis: Bookess, 2010.

ROTHENBERG, J.

1999 *Ensuring the longevity of digital information*. [Em linha]. Santa Monica: [s.n.], 1999. [Consult. 13 out. 2022]. Disponível em: <https://www.clir.org/wp-content/uploads/sites/6/ensuring.pdf>.

SANTOS, V. B.

2005 *Gestão de documentos eletrônicos: uma visão arquivística*. 2ª ed. rev. aum. Brasília: ABARQ, 2005.

SAYÃO, L. F.

2010 Repositórios digitais confiáveis para a preservação de periódicos eletrônicos científicos. *Ponto de Acesso*. [Em linha]. 4:3 (2010) 68-94. [Consult. 13 out. 2022]. Disponível em: <https://portalseer.ufba.br/index.php/revistaici/article/view/4709/3565>.

SCHELLENBERG, T. R.

2006 *Arquivos modernos: princípios e técnicas*. 6ª ed. Rio de Janeiro: Fundação Getúlio Vargas, 2006.
Tít. orig.: *Modern archives: principles and techniques* Chicago: The University of Chicago Press, 1956.

SILVA, E. L.; MENEZES, E. M.

2005 *Metodologia da pesquisa e elaboração de dissertação*. [Em linha]. Florianópolis: UFSC, 2005. [Consult. 13 out. 2022]. Disponível em: <https://www.researchgate.net/publication/312125489>.

SILVA, M.

2017 *O Arquivo e o lugar: custódia arquivística e a responsabilidade pela proteção aos arquivos*. Niterói: Eduff, 2017.

THOMAZ, K. P.; SOARES, A. J.

2004 A Preservação digital e o modelo de referência Open Archival Information System (OAIS). *DataGramaZero*. [Em linha]. 5:1 (2004). [Consult. 13 out. 2022]. Disponível em: <http://www.brapci.inf.br/index.php/article/download/7616>.

VOLPATO, G. L. [et al.]

2013 *Dicionário crítico para redação científica*. Botucatu: Best Writing, 2013.

Henrique Machado dos Santos | henrique.hms.br@gmail.com

Universidade Federal do Rio Grande (FURG), Brasil

Daniel Flores | dfloresbr@gmail.com

Universidade Federal Fluminense (UFF), Brasil