

Resumo: Este estudo descreve os requisitos para auditoria da gestão de objetos digitais com base no *Audit and Certification of Trustworthy Digital Repositories*. Para tanto perpassa questões relacionadas à aquisição de conteúdo, criação do pacote de informação para armazenamento, planejamento, manutenção dos objetos digitais, gestão da informação e gestão de acesso. A discussão segue a lógica dedutiva, de modo que se realiza uma triangulação para analisar a gestão de objetos digitais, contextualizá-la no âmbito da Arquivística, e identificar os pressupostos essenciais para um repositório arquivístico digital confiável. Dentre os principais elementos a serem observados, destacam-se a identificação e manutenção das propriedades significativas para fortalecer a presunção de autenticidade, e o registro de todas as ações proferidas sobre a documentação por meio de metadados. Por fim, se reforça a necessidade da Arquivística se apropriar de temáticas relacionadas à preservação sistêmica.

Palavras-chave: Documento digital; Preservação digital; Preservação sistêmica; Repositório digital.

Abstract: This study describes the requirements for auditing digital object management based on the *Audit and Certification of Trustworthy Digital Repositories*. For this, it deals with questions related to content acquisition, creation of the archival information package, planning, maintenance of digital objects, information management and access management. The discussion follows the deductive logic, so that triangulation is performed to analyze the management of digital objects, contextualize it in the field of Archival Science, and to identify the essential assumptions for a trustworthy digital archival repository. Among the main elements to be observed are the identification and maintenance of significant properties to strengthen the presumption of authenticity, and the recording of all actions taken on the documentation through metadata. Finally, it reinforces the need for Archival Science to appropriate itself of themes related to systemic preservation.

Keywords: Digital record; Digital preservation; Systemic preservation; Digital repository.

1. Introdução

O advento dos documentos digitais e a sua conseqüente demanda pela sociedade tornou-se um dos principais desafios da Arquivística/Arquivologia contemporânea (THOMAZ, 2006). O ambiente digital apresenta uma série de complexidades derivadas do aparato tecnológico composto por *hardware*, *software* e suportes, necessários para interpretar/representar os documentos.

Observa-se que esse aparato tecnológico está em constante mudança, fato que ocasiona a obsolescência tecnológica, logo, isso tem motivado a implementação de políticas e estratégias de preservação digital. Com tais ações estima-se contornar as complexidades do ambiente digital, além de manter as especificidades do documento arquivístico. Assim, a preservação de documentos digitais requer a manutenção de princípios arquivísticos da

proveniência, organicidade, naturalidade, unicidade e indivisibilidade. Para tanto, devem ser inseridos em um sistema de arquivos confiável, que será o responsável por sua tramitação, custódia, manutenção da autenticidade e acesso.

Nessa perspectiva, a preservação de documentos deve ser orientada por meio de um Repositório Digital Confiável (RDC) que seja desenvolvido em conformidade com o modelo *Open Archival Information System* (OAIS). Esse é o principal padrão de preservação, e tornou-se a norma da *International Organization for Standardization* (INTERNATIONAL...) 14.721:2012, que orienta os requisitos de um RDC.

No âmbito da Arquivística, surge a necessidade de se implementar um Repositório Arquivístico Digital Confiável (RDC-Arq), que contempla os requisitos de um RDC e comporta as especificidades do documento de arquivo. Logo, o RDC-Arq consiste no “Arquivo Permanente Digital”, responsável pela preservação, custódia confiável e garantia de acesso a documentos autênticos em longo prazo.

Observa-se que para atingirem o *status* de confiável, tanto o RDC, quanto o RDC-Arq necessitam comprovar que seguem os requisitos preconizados pelo modelo OAIS. Logo, podem ser auditados com o *Audit and Certification of Trustworthy Digital Repositories* (ACTDR), padrão que se tornou a norma ISO 16.363:2012.

Em geral, o processo de auditoria consiste em uma atividade de controle dos procedimentos de gestão que proporciona transparência e confiabilidade aos utilizadores (OLIVEIRA e BATISTA, 2019). Logo, há uma persistente relação entre a auditoria de informação, a avaliação da qualidade dos serviços e o planejamento estratégico organizacional (PESTANA, 2014). Nesse sentido, a auditoria arquivística busca avaliar os procedimentos de todo o ciclo de vida dos documentos, e verificar a sua conformidade com leis, normas e bases teóricas da disciplina (OLIVEIRA e BATISTA, 2019). Portanto, além de respeitar os fundamentos da Arquivística, a auditoria de um RDC-Arq deve verificar sua conformidade com o modelo OAIS, tendo em vista o uso de um padrão como, por exemplo, o ACTDR.

Observa-se que os requisitos de auditoria do ACTDR – ISO 16.363:2012 estão divididos em três seções: infraestrutura organizacional (*organizational infrastructure*), gestão de objetos digitais (*digital object management*) e infraestrutura e segurança da gestão de riscos (*infrastructure and security risk management*). Para fins deste estudo será abordada somente a “gestão de objetos digitais” tendo por objetivo descrever os requisitos para preservação da informação de conteúdo/documento arquivístico, e contextualizá-los no âmbito da Arquivística.

A infraestrutura organizacional compreende as políticas do RDC, enquanto que a infraestrutura de segurança para gestão de risco se refere às rotinas de segurança da informação necessárias para mitigar vulnerabilidades. Já a gestão de objetos digitais compreende aspectos relacionados à aquisição de conteúdo, criação do Pacote de Informação para Armazenamento (*Archival Information Package* – AIP), planejamento da preservação, preservação do AIP, gestão da informação, e gestão de acesso.

O processo de auditoria permite realizar um estudo de todo o ciclo de vida da informação, e assim, identificar necessidades em relação à sua produção, uso/fluxo, indivíduos envolvidos e demais aspectos capazes de determinar o valor das informações na organização. Para tanto, preconiza-se a fiscalização das práticas arquivísticas desde a gestão, perpassando a preservação, até o acesso (OLIVEIRA e BATISTA, 2019). Nessa

perspectiva, delimita-se o presente estudo para os fluxos de informação em fase permanente, de modo que a ênfase da discussão é depositada no processo de preservação digital e garantia de acesso contínuo em longo prazo.

2. Metodologia

Classifica-se o presente estudo como natureza aplicada, pois tem por objetivo gerar conhecimentos para aplicação prática, vislumbrando a solução de problemas específicos identificados. Com isso, contribui para ampliar o conhecimento científico e gerar novos questionamentos para investigação (GIL, 2010; SILVA e MENEZES, 2005).

A seleção de materiais parte do levantamento bibliográfico de livros, publicações técnicas e artigos científicos. Os artigos são recuperados na Base de Dados em Ciência da Informação (BRAPCI) por meio de palavras-chave como: "preservação digital", "documentos arquivísticos digitais" e "repositórios digitais confiáveis". Para isso, utiliza-se a delimitação temporal que comporta o período entre 2004 e 2019, posteriormente, os artigos são escolhidos após análise dos seus respectivos resumos; e outras obras foram selecionadas a partir de suas referências.

Este estudo assume um caráter descritivo, pois objetiva discorrer sobre as características do objeto de investigação (GONÇALVES, 2011). Os requisitos para auditoria de RDC's preconizados pelo ACTDR são a base da discussão, que segue a lógica dedutiva. Dessa forma, realiza-se a seguinte triangulação: analisa-se a seção "gestão de objetos digitais" para contextualizá-la no âmbito da Arquivística, de modo que o RDC-Arq torna-se a categoria norteadora (GIL, 2010; LUNA, 1997; SILVA e MENEZES, 2005; VOLPATO *et al.*, 2013).

Com isso, obtém-se um artigo de revisão assistemática/narrativa que parte de uma temática aberta, pautada nos referenciais da preservação digital. Com tal abordagem é possível compreender os requisitos para gestão de objetos digitais preconizados pelo ACTDR, e assim, contextualizá-los na preservação de documentos arquivísticos digitais (CORDEIRO *et al.*, 2007).

Ressalta-se que não há pretensão de abordar a temática de forma exaustiva, logo, este estudo limita-se em compreender e expor os pressupostos básicos para gestão de objetos digitais do ACTDR, bem como, a sua pertinência para auditar um RDC-Arq. Sendo assim, com esta reflexão sobre o tema pretende-se ressaltar o ponto de vista dos autores frente a problemática da preservação de documentos arquivísticos digitais autênticos em longo prazo.

3. Aquisição de conteúdo

Durante o processo de aquisição de objetos digitais, o RDC-Arq deve identificar as propriedades significativas que serão preservadas, para isso, adicionam-se às informações necessárias ao Pacote de Informação para Submissão (*Submission Information Package* – SIP). As fontes de proveniência dos objetos admitidos devem ser autenticadas, bem como, executar as correções necessárias a cada SIP submetido. Ademais, é

precINTERNATIONAL... obter controle físico dos objetos digitais para preservá-los, de modo a fornecer respostas adequadas ao produtor durante o processo de submissão/aquisição.

3.1. Identificar os objetos para preservação

O processo de admissão preconizado pelo OAIS requer a identificação das informações de conteúdo, bem como das respectivas propriedades significativas que serão preservadas. Logo, o RDC-Arq define quais aspectos da informação de conteúdo são pertinentes à preservação e informa aos seus colaboradores.

Para tanto, apresentam-se aos financiadores, depositantes e consumidores, quais responsabilidades são assumidas e quais aspectos são excluídos. Além disso, devem-se informar aos produtores/depositantes quais informações são necessárias. Isso pode ser formalizado por meio de: declaração de missão; acordos de submissão; contratos de depósito; documentação das propriedades que devem ser preservadas; fluxo de trabalho; e políticas de preservação (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Cabe o RDC-Arq deve estabelecer, junto com depositantes, financiadores, e comunidade designada, um meio para determinar e verificar as características e propriedades significativas da informação que serão preservadas em longo prazo. Esses procedimentos irão confirmar ou refutar a autenticidade dos documentos preservados, de modo que podem ser demonstrados por meio de: acordos de submissão; contratos de depósito; políticas de preservação; documentação de fluxo de trabalho; e definição clara das propriedades que devem ser preservadas (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Ressalta-se que preservar e custodiar documentos digitais requer a implementação de processos contínuos de migração e *backup* tendo em vista a manutenção de sua autenticidade. Tais processos são motivados em virtude da fragilidade dos suportes de informação e da obsolescência tecnológica das plataformas de *hardware/software* (RONDINELLI, 2005).

Logo, a preservação digital presume a necessidade de alterar as informações para que se mantenham acessíveis e inteligíveis à comunidade designada. Portanto, RDC-Arq e produtor devem definir um conjunto de propriedades significativas, que corresponde às características essenciais dos objetos digitais que precisam ser preservadas para manter a autenticidade (SANTOS e FLORES, 2019b).

Sendo assim, o RDC-Arq estabelece métodos para determinar as propriedades significativas dos diferentes tipos de informação de conteúdo, para os quais assumiu a responsabilidade de preservação junto à comunidade designada. Tais características são essenciais para a presunção de autenticidade, bem como para a correta interpretação/representação da informação de conteúdo.

Posteriormente, o RDC-Arq manterá um registro das propriedades significativas que irá preservar. Para tanto, deve identificar e documentar as informações de conteúdo e as respectivas propriedades da informação que irá preservar. Tal requisito pode ser evidenciado por meio de: políticas de preservação; manuais de processamento; registros dos tipos de informação de conteúdo; estratégias de preservação adquiridos; e planos de ação. Logo, o RDC-Arq demonstra que compreende as suas coleções digitais, de forma

suficiente, para garantir a preservação das propriedades a que se comprometeu. Essa informação poderá ser utilizada para determinar a eficácia das suas atividades de preservação no longo prazo (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

As ações de preservação digital compreendem procedimentos para garantir as características dos documentos arquivísticos digitais, das quais se destaca a autenticidade (ROCHA e SILVA, 2007). Com isso, ressalta-se a pertinência de definir e implementar os “requisitos fundamentais”, seja na orientação para desenvolvimento/aquisição de sistemas informatizados, seja na avaliação dos sistemas que estão em uso. Consequentemente, será possível manter conformidade com a legislação e com as especificidades de gestão da informação (PINTO, 2009).

Dessa forma, o RDC-Arq define o que será preservado, e assim, firma o compromisso com tais tipos de informação definidos *a priori*. O cumprimento desse requisito é essencial para demonstrar a capacidade de preservar documentos de forma confiável, visto que as propriedades significativas impactam diretamente na presunção de autenticidade dos documentos arquivísticos digitais.

3.2. Reunir os objetos digitais necessários

Cabe ao RDC-Arq especificar claramente, no momento do depósito, quais informações precisam ser respectivamente associadas à informação de conteúdo, de modo a buscá-las junto ao produtor. Tal requisito pode ser evidenciado por meio de: exigência de transferência; acordos entre o produtor e o RDC-Arq; e fluxo de trabalho para produzir o AIP. Logo, é preciso especificar exatamente quais são os objetos digitais transferidos, qual a documentação que está associada, e se existem restrições de acesso (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

O nível de precisão dessas especificações irá variar conforme as políticas de cobrança em relação aos produtores. Logo, o RDC-Arq deverá buscar junto ao produtor toda a informação necessária para representar corretamente as informações de conteúdo. Reunir todos os objetos digitais necessários garante que a comunidade designada possa acessar a informação de conteúdo de forma autêntica.

Observa-se que a autenticidade dos documentos está relacionada à confiabilidade da custódia documental nos sistemas de gestão e preservação. Entende-se que a manutenção da autenticidade não se limita aos arquivos permanentes, portanto, devem-se empregar métodos confiáveis desde a gênese dos documentos, perpassando todo o seu ciclo de vida (SANTOS e FLORES, 2019a).

Com isso, o RDC-Arq deve buscar todos os objetos digitais necessários à autenticidade e correta representação das informações de conteúdo. Igualmente, se desperta atenção para que o produtor empregue métodos de produção, armazenamento e tramitação confiáveis.

Por vezes uma simples migração não será suficiente, portanto é preciso vislumbrar o acesso ininterrupto aos objetos digitais, de modo a preservar seus diversos recursos informacionais. Ademais, devem-se estabelecer políticas para admissão, tratamento, representação e descrição dos objetos digitais. Com isso, estima-se desenvolver um sistema confiável que manterá informações autênticas (BOERES e CUNHA, 2012).

Há ainda a possibilidade dos objetos digitais sofrerem variações no conteúdo durante o seu ciclo de vida. Soma-se a isso a necessidade de alterar a informação digital para que possa ser preservada. Logo, tal fato reforça a necessidade de adaptação dos conceitos de autenticidade e fixidez, permitindo assim, uma variabilidade limitada para os documentos arquivísticos em ambiente digital.

A variabilidade limitada consiste na variação de forma e do conteúdo dos documentos. No entanto não poderá comprometer o seu caráter arquivístico, pois deverá ser implementada a partir de regras fixas (RONDINELLI, 2013). Logo, a variabilidade limitada equivale a variação de forma e apresentação intencionais criadas e já previstas pelo autor (SANTOS, 2012).

Ressalta-se que no âmbito do RDC-Arq poderá haver variações em relação ao objeto conceitual, seja na preservação de determinadas características em detrimento de outras; seja na variabilidade limitada. Mesmo assim, a essência da informação de conteúdo será preservada por meio da reunião de objetos digitais que compõem a informação conteúdo, de modo a manter as propriedades significativas e respeitar as variações intencionais criadas pelo autor.

3.3. Identificar e analisar o SIP

O RDC-Arq deve ser capaz de extrair a informação contida nos SIP's. Tal requisito pode ser evidenciado por: informação de empacotamento dos SIP's; informação de representação para os conteúdos dos SIP's; e especificações dos formatos de arquivo documentados. Além de reconhecer o conteúdo de um SIP, o RDC-Arq deve confirmar se corresponde ao esperado, se as informações de conteúdo estão corretamente identificadas, e se as propriedades significativas da informação de conteúdos foram selecionadas corretamente (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Dessa forma, o RDC-Arq poderá analisar o conteúdo de um determinado objeto digital e verificar se a sua estrutura lógica corresponde ao formato de arquivo que representa. Tal procedimento é pertinente, pois os formatos de arquivo podem não refletir o que realmente são. Ou seja, um documento de texto pode estar equivocadamente representado em um formato de imagem, o que resulta no erro de interpretação/representação da informação de conteúdo. Ressalta-se que tais questões são verificadas durante o processo de admissão do SIP ao RDC-Arq.

Inicialmente, a entidade de admissão recebe os SIP's, verifica a sua qualidade, gera os AIP's correspondentes conforme os padrões definidos pelo Arquivo, e após, gera a informação descritiva dos AIP's, que corresponde aos metadados para pesquisa e recuperação. Por fim, os AIP's criados e suas informações descritivas são transferidos, respectivamente, para a entidade de armazenamento arquivístico, e para a entidade de gerenciamento de dados (THOMAZ e SOARES, 2004).

Deve-se destacar que o pacote de informação consiste em um envelope conceitual no qual são encapsulados a informação de conteúdo e os metadados de preservação (SARAMAGO, 2004). Assim, tal pacote visa reunir o objeto de dados e a respectiva informação de representação para descrever corretamente o objeto de informação (documento arquivístico), bem como fornecer subsídios para preservação. Assim, o pacote de informação visa em manter o documento arquivístico digital atrelado à respectiva

informação de representação, de modo a contribuir na presunção de autenticidade e garantir o acesso inteligível no longo prazo. Ademais, a arquitetura desse pacote irá auxiliar a comunidade designada na recuperação das informações de conteúdo (SANTOS e FLORES, 2019a).

3.4. Identificar os produtores da informação

Compete ao RDC-Arq ter mecanismos para verificar a identidade dos produtores das informações de conteúdo. Isso evita que se atribua proveniência errônea às informações que serão preservadas. Tal requisito pode ser evidenciado com: procedimentos de autenticação; adição de vínculo jurídico aos acordos de submissão/contratos de depósito; e procedimentos/rotinas tecnológicas (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Os princípios da proveniência é um ponto fundamental da Arquivística que delimita a origem do acervo. Assim, reflete a origem da acumulação no que tange à evolução das estruturas, funções e atividades, tanto internas quanto externas ao órgão. Ao respeitar esse princípio, evita-se a mistura de acervos arquivísticos com os não arquivísticos. Logo, a classificação irá refletir a origem dos documentos e permitir a reconstrução do vínculo orgânico entre os documentos (LOPES, 2014).

Nesse sentido, as principais características que diferenciam os documentos de arquivo dos demais documentos são a proveniência e a organicidade. Sua combinação permite identificar o vínculo arquivístico, que consiste em uma conexão lógica e formal capaz de unir documentos de um mesmo conjunto conforme suas funções e atividades (BELLOTTO, 2014b).

A pertinência da organicidade e da proveniência se solidifica ao tornarem-se princípios da disciplina Arquivística. A combinação desses permite estabelecer o vínculo arquivístico, capaz de relacionar logicamente os documentos, constituindo assim, fundo documental.

Observa-se que a constituição do fundo vai além da reunião física de documentos, por isso tal conceito mantém-se adequado para documentos em ambiente digital. Pode-se manter o vínculo arquivístico dos documentos digitais por meio de metadados, e assim, assegurar princípios arquivísticos de: proveniência, organicidade, indivisibilidade, unicidade e naturalidade (BELLOTTO, 2014a).

Dessa forma, o RDC-Arq determinará corretamente os produtores de cada SIP recebido, mantendo os princípios da Arquivística. Neste ponto, ressalta-se a importância da inserção de metadados que auxiliem no processo de identificação de produtores, recebedores e acumuladores. Tais metadados contribuirão para relacionar logicamente os documentos, e assim, recuperar o vínculo arquivístico na busca pela reconstrução do fundo.

3.5. Verificar a integridade do SIP

O RDC-Arq deve ter um processo de admissão que verifique a integridade e a precisão de cada SIP recebido para detectar e corrigir erros de criação e transmissão. Tal requisito pode ser evidenciado por: políticas de preservação; implementação do plano de preservação; registros detalhados das transferências; e definições de integridade e precisão (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Dessa forma, as informações coletadas durante o processo de admissão podem ser comparadas com informações coletadas anteriormente, que retratam as expectativas do produtor/depositante. A correção do SIP irá depender dos conhecimentos que o RDC-Arq possui e das ferramentas que estão disponíveis para verificar a precisão. Isso inclui verificar se os formatos de arquivo são o que eles afirmam ser ou verificar o seu conteúdo. Ademais, o RDC-Arq pode rejeitar a transferência, somente admitindo o SIP após o produtor reparar os erros (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Os documentos arquivísticos em ambiente digital assumem formas diferentes dos em meio analógico. Tais formas são: a armazenada e a manifestada. O documento armazenado corresponde a todos os objetos digitais necessários para sua correta representação. Já a forma manifestada se refere a apresentação desse documento, que se dá por meio da recuperação a partir dos objetos digitais, que é expressa por um periférico de saída.

O documento manifestado tem caráter arquivístico, pois pode ser compreendido por humanos. Tal documento não se representa por si mesmo, ou seja, é composto por diversos objetos digitais, que após serem processados manifestam-no. Sendo assim, existe uma relação de interdependência entre o documento manifestado e os objetos digitais que o compõem (RONDINELLI, 2013).

Ao considerar o ambiente organizacional, observa-se que a integridade das informações está diretamente relacionada com a qualidade dos sistemas e das ferramentas de tecnologia da informação (DE SORDI, 2008). Logo, é essencial que os documentos digitais mantenham-se íntegros de modo que o sentido da mensagem comunicada não seja inalterado (INTERPARES, 2007b).

Nessa perspectiva, ressalta-se que um RDC-Arq deve ter um rígido controle da admissão de conteúdos, de modo que os pacotes AIP reflitam as informações de conteúdo dos pacotes SIP. Isso é essencial para demonstrar que o RDC-Arq está cumprindo com a preservação da integridade e demais compromissos firmados com os produtores.

3.6. Obter controle sobre os objetos digitais

Um RDC-Arq deve obter controle suficiente, tanto legal quanto físico, para preservar os objetos digitais. Tal requisito pode ser evidenciado por: documentos que comprovem o nível de controle físico; e um catálogo em forma de banco de dados, que seja capaz de listar todos os objetos digitais e seus respectivos metadados necessários para validar a integridade. Com esse controle, o RDC-Arq poderá executar planos de preservação para que os materiais custodiados tornem-se acessíveis aos consumidores (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Na ausência de licença para negociar a propriedade intelectual junto ao produtor, é essencial que o RDC-Arq tenha um acordo que lhe autorize a realizar as atividades de preservação. Isso contempla possível alteração dos *bits*, seja por meio de estratégias de migração, ou pela inserção de metadados. Igualmente, a disseminação dos documentos deve ser orientada por um acordo de direitos, instrumento pelo qual se definem os usos da informação custodiada pelo RDC-Arq (SANTOS e FLORES, 2019b).

Ao administrador do RDC-Arq aplica-se o conceito de “custodiante confiável”, logo, este requer a definição de mandato e competência, tanto jurídica quanto administrativa para que possa realizar as atividades de preservação (SILVA, 2017). Nesse sentido, o RDC-Arq

deverá negociar tais direitos com os produtores/detentores da informação. Com isso é possível executar procedimentos de preservação no longo prazo e disponibilizar a informação aos consumidores (SARAMAGO, 2004).

Observa-se que o RDC-Arq necessita obter o controle de todos os objetos digitais que são vinculados à informação de conteúdo para efetuar as atividades necessárias a sua preservação, e prover o acesso à comunidade designada. Isso requer o controle legal e físico/lógico, de modo que seja suficiente para executar estratégias, inserir metadados, bem como definir as propriedades significativas que serão mantidas. Ou seja, o RDC-Arq requer a permissão legal para alterar os objetos digitais, no entanto, deve preservar as características que conferem autenticidade à informação de conteúdo.

3.7. Fornecer *feedback* ao produtor durante a admissão

O RDC-Arq deve fornecer *feedback* ao produtor durante a admissão, para verificar que não existem lapsos de comunicação que possam ocasionar a perda de SIP's. Tal requisito pode ser evidenciado por: acordos de submissão; contratos de depósito; documentação de fluxo de trabalho; e demais relatos de evidência por meio de memorandos e e-mails. Com isso, o RDC-Arq fornece relatórios de progresso ao produtor/depositante especificando os pontos definidos durante o processo de admissão. Ademais, deve informar o produtor sobre relatório de erros, correções e qualquer transferência de custódia (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Cabe ao RDC-Arq ter controles para transferência/recolhimento de documentos arquivísticos digitais. Trata-se da alteração da cadeia de custódia que delega as responsabilidades do produtor para o preservador. Para tanto, deve estabelecer mecanismos de monitoramento que registrem o processo de admissão dos SIP's. Igualmente, deve-se verificar a proveniência dos documentos arquivísticos submetidos, bem como se correspondem ao que foi especificado pelo produtor (INTERPARES, 2007a).

O momento da admissão é um ponto crítico com relação a autenticidade das informações de conteúdo. Logo, é fundamental ter mecanismos para elevar a segurança da transferência, a fim de evitar manipulações de conteúdos, bem como inclusão de informações indevidas. Ademais, o RDC-Arq deverá notificar o produtor com relação ao andamento do processo, detalhando os eventos que vierem a ocorrer, como, por exemplo, erros de submissão, SIP's inadequados, falhas do sistema, entre outros.

Para tanto, o RDC-Arq deve demonstrar que avalia sistematicamente a satisfação de produtores e consumidores, buscando satisfazê-los com os serviços prestados (BRASIL, 2015). Logo, a confiabilidade do RDC-Arq se desenvolverá em três níveis, ao comprovar que: os produtores enviam as informações corretas; os consumidores recebem as informações corretas; e os fornecedores prestam os serviços adequados (THOMAZ, 2007).

Dessa forma, cabe ao RDC-Arq informar o produtor sobre o andamento dos procedimentos de admissão, de modo que seja possível demonstrar a conformidade das ações proferidas sobre o SIP frente às questões definidas previamente. Defende-se que o RDC-Arq mantenha uma relação de transparência com o produtor, informando-lhe sobre o andamento das ações de preservação digital.

3.8. Assegurar a autenticidade do conteúdo adquirido

Cabe ao RDC-Arq manter registros sobre ações e processos da administração relacionados a aquisição de conteúdo para garantir que a documentação capturada é autêntica, passível de ser utilizada em auditorias. Tal requisito pode ser evidenciado por: documentação relativa a decisões; metadados de preservação que sejam armazenados e associados aos objetos digitais; e recibos de confirmação enviados aos fornecedores. Tais registros podem ser criados de forma automática ou inseridos por indivíduos autorizados, logo, o RDC-Arq deve demonstrar que todas as ações relevantes são realizadas (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Sendo assim, o RDC-Arq precisa registrar todos os procedimentos administrativos para manter um histórico das ações realizadas, que servirá para comprovar a autenticidade das informações de conteúdo admitidas. Ressalta-se que manter o registro de tais procedimentos administrativos contribui para despertar a confiança dos produtores e da comunidade designada.

O processo de preservação deve assegurar que os objetos digitais foram mantidos de forma autêntica. Ou seja, os objetos digitais resultantes de tal processo mantêm todos os aspectos considerados essenciais (THIBODEAU, 2002). Com isso, pode-se comprovar a autenticidade desde a produção, até o recolhimento ao arquivo permanente (INNARELLI, 2009).

A presunção de autenticidade é definida a partir de fatos conhecidos sobre a produção e o armazenamento dos documentos digitais (INTERPARES, 2007b). Assim, devem-se analisar questões como: forma fixa, conteúdo estável, contexto de produção, manutenção/uso e preservação. Verificar a autenticidade requer ir além da observação características físicas e da implementação de soluções tecnológicas (BRASIL, 2015). Com isso, observa-se que a presunção de autenticidade está relacionada à informação orgânica e não ao suporte, entendido como neutro (DELMAS, 2010).

Dessa forma, a crítica com relação à veracidade dos documentos tornar-se-á desprovida de sentido caso não seja possível comprovar a sua autenticidade (LOPEZ, 2004). Ressalta-se que os documentos arquivísticos consistem em fontes de prova e informação, as quais registram informações de caráter cultural, histórico, científico, técnico, econômico e administrativo. Portanto, requerem autenticidade para que possam fornecer evidências das respectivas ações, e assim, contribuir para ampliar a memória social (BRASIL, 2004).

A manutenção da autenticidade é essencial para que os documentos arquivísticos possam ser utilizados para fins de prova ou informação. Para tanto surge a necessidade do RDC-Arq assegurar a integridade dos objetos digitais que compõem cada AIP.

4. Criação do AIP

Durante a criação do AIP, o RDC-Arq deve definir um identificador único de nomenclatura geral para cada AIP ou classe de informação, que demonstra a preservação de suas propriedades significativas. As transformações dos SIP's em AIP's precisam ser descritas, além de manter os identificadores únicos previamente associados. Um contexto semântico

entre objetos digitais armazenados deve ser estabelecido, e as informações de representação admitidas requerem registro.

Assim, é preciso documentar os processos de aquisição e gerenciamento dos metadados de preservação para as informações de conteúdo associadas, além de adquirir outros metadados necessários à preservação. O processo de criação do AIP ainda requer a verificação da compreensão da informação de conteúdo, da integridade e da precisão de cada AIP. De forma complementar, deve-se fornecer um mecanismo para auditoria da integridade dos materiais custodiados, e manter registros dos metadados de processos administrativos pertinente à preservação.

4.1. Identificar o AIP e todos os seus componentes

O RDC-Arq deve ter, para cada AIP ou classe de AIP, uma definição associada adequada para analisar esses AIP's e contemplar suas necessidades de preservação de longo prazo. Isso assegura que o AIP e sua definição associada, incluindo a informação de empacotamento, sempre poderão ser localizados, processados e gerenciados dentro do RDC-Arq (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Para tanto, o RDC-Arq deve ter capacidade de identificar qual definição se aplica para determinado AIP. Isso assegura que se utiliza a definição apropriada para analisar/interpretar o AIP. Tal requisito pode ser evidenciado por documentação que relacione claramente cada AIP ou classe de AIP à sua definição (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Compete ao RDC-Arq monitorar os componentes digitais por meio de ferramentas amplamente reconhecidas pela comunidade de preservação (BRASIL, 2015). Ademais, por vezes o preservador terá de extrair os documentos digitais do sistema no qual foram produzidos. Para tanto, deve garantir que todos os componentes considerados essenciais serão identificados, de modo que suas relações sejam detalhadas por meio de metadados, antes mesmo de sua transferência (INTERPARES, 2007a).

Sendo assim, o RDC-Arq poderá usar o método que considerar mais apropriado para associar as definições aos AIP's. Assim, tal requisito cria um elo lógico entre os objetos digitais que contribui para a correta representação das informações de conteúdo, bem como, auxilia no processo de busca e recuperação da informação.

Compete ao RDC-Arq ter uma definição adequada de cada AIP a fim de preservá-lo em longo prazo, de modo que seja possível identificar e analisar todos os seus componentes necessários. Isso possibilita mostrar explicitamente que os AIP's estão apropriados à sua finalidade, sendo que cada componente de um AIP foi concebido de forma adequada, e que os planos para manutenção de cada AIP estão definidos. Tal requisito pode ser evidenciado por demonstrações do uso das definições para extrair informações de conteúdo e Informação Descritiva de Preservação (*Preservation Description Information – PDI*) do AIP (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Dessa forma, deve-se identificar cada classe de AIP, descrever como cada uma é implementada no RDC-Arq, e relacionar os componentes necessários para a preservação do AIP para garantir aos produtores e consumidores que as propriedades significativas serão preservadas. Além disso, é preciso identificar claramente que componentes do AIP

podem ser geridos, bem como a necessidade de criar novas versões para cumprir sua finalidade (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Observa-se que o RDC-Arq deverá identificar e manter uma relação dos componentes necessários para preservar as propriedades significativas dos AIP's. Além disso, será necessário demonstrar, periodicamente por meio da revisão, que tais componentes satisfazem as necessidades de preservação.

4.2. Descrever a transformação do SIP em AIP

Com uma descrição de como o AIP é construído a partir SIP é possível assegurar que o AIP representa adequadamente as informações relativas ao SIP. Para isso será necessário uma descrição precisa das ações, suficiente até mesmo para as transformações complexas. Tal requisito pode ser evidenciado pela documentação sobre a relação entre SIP's e AIP's, explicitando como os AIP's são derivados dos SIP's (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Cabe ao RDC-Arq descrever o processo de transformação dos SIP's em AIP's, de modo que possa apontar todas as transformações perpassadas pelos documentos, seus metadados iniciais, bem como os metadados que foram adicionados no momento da criação do AIP. Ademais, deve-se ter capacidade de demonstrar se os SIP's foram aceitos e transformados em AIP's, seja de forma integral ou parcial, ou ainda, se foram rejeitados pelo RDC-Arq (BRASIL, 2015).

Dessa forma, o RDC-Arq demonstra que a informação de conteúdo armazenada na forma de AIP está em conformidade com aquela submetida originalmente pelo produtor na forma de SIP. Para tal, é necessário detalhar como ocorreram as transformações necessárias ao armazenamento. Essa descrição corrobora para demonstrar a autenticidade das informações de conteúdo, pois justifica as suas possíveis transformações, relacionando-as à necessidade de alterar a informação digital para melhor preservá-la. O registro dessas ações também auxilia no processo de presunção da autenticidade dos documentos.

4.3. Documentar a disposição final de todos os SIP's

O RDC-Arq deve registrar os procedimentos relativos ao tratamento dos SIP's admitidos, logo, é essencial indicar sua localização após ser transformados em AIP ou detalhar os motivos de sua eliminação, em casos especiais. Para tanto, deve-se seguir procedimentos documentados, e justificar os motivos, caso um SIP seja rejeitado ou descartado.

Sendo assim, é preciso assegurar que os SIP's recebidos foram tratados de forma apropriada, e que não ocorreram perdas acidentais. Tal requisito pode ser evidenciado por: registros de eliminação; acordos com depositantes; sistema de rastreamento da proveniência; e documentação sobre como os AIP's são derivadas do SIP's. Ademais, deve-se manter a informação descritiva apropriada sobre a proveniência de todos os objetos digitais (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

É preciso seguir políticas e procedimentos devidamente documentados para assegurar que a informação de conteúdo é preservada contra quaisquer entraves que possam ocorrer. Isso inclui o desaparecimento do acervo, logo, tal política garante que os AIP's nunca são excluídos, exceto que seja permitido por uma estratégia aprovada (ASSOCIAÇÃO..., 2007; CONSULTATIVE..., 2012; INTERNATIONAL..., 2012a). Tal estratégia se refere a possíveis

equivocos que podem ocorrer no momento da admissão de conteúdos. Dessa forma, será preciso justificar a exclusão, tendo em vista que um determinado objeto digital foi transformado em AIP por mero equívoco.

A preservação digital requer a implementação de um sistema de gestão documental integrado e que seja normalizado. Assim, os documentos capturados serão classificados, avaliados, preservados de forma autêntica e acessível. Ademais, devem ser descritos para otimizar a busca e a recuperação das informações (CASANOVAS, 2008).

Com isso, o RDC-Arq terá de registrar o motivo das exclusões de SIP's submetidos de forma equivocada, quando houver, visto que os documentos arquivísticos submetidos/recolhidos ao RDC-Arq (arquivo permanente) não devem ser eliminados ou recusados de forma arbitrária. Logo, é necessário justificar a natureza do equívoco/erro ou mesmo inconformidade dos SIP's com as normas de submissão previamente definidas.

4.4. Manter identificadores únicos para os AIP's

Ao utilizar uma convenção, que gera identificadores únicos para todos os AIP's e seus respectivos componentes, o RDC-Arq poderá fazer verificações para inibir duplicações. A identificação exclusiva otimiza a precisão no processo de busca e recuperação da informação de conteúdo, além de evitar a dispersão dos componentes digitais. Igualmente, é preciso descrever os processos utilizados para alterar tais identificadores, pois isso agrega confiabilidade ao sistema de identificação (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

A identificação exclusiva permite que o RDC-Arq tenha maior controle sobre a documentação. Assim, cada AIP e seus respectivos componentes podem ser localizados independentemente de sua complexidade. Com isso, é possível entregar as informações de conteúdo solicitadas aos consumidores com elevada precisão. Ademais, desperta-se a questão da confiabilidade, pois, além da identificação exclusiva, há ainda o registro das alterações sobre o sistema de identificação. Tal questão é essencial para comprovar que todas as alterações proferidas no ambiente de preservação são monitoradas e registradas, objetivando a presunção de autenticidade.

Nesse sentido, o RDC-Arq deve fornecer uma lista completa de todos os identificadores e fazer verificações pontuais para identificar possíveis duplicações. O sistema de identificadores deve ser adequado para comportar a demanda atual do RDC-Arq e as necessidades futuras no que tange ao número de objetos, bem como, assegurar que cada AIP possa ser inequivocamente encontrado e distinguido dos demais. Tal requisito pode ser evidenciado pela documentação que descreve o sistema de nomenclatura utilizado (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Dessa forma, o RDC-Arq deve garantir a capacidade de recuperar a informação de conteúdo desejada, com alto grau de precisão. Igualmente, deve prevenir a existência de informações duplicadas por meio de um sistema de identificadores exclusivos. Tais questões são essenciais para demonstrar confiança à comunidade designada.

Ressalta-se que a identificação exclusiva está prevista na Norma Brasileira de Descrição Arquivística (NOBRADE), logo, em seus elementos de descrição pode-se observar que o item "1 área de identificação" possui o subitem "1.1 código de referência" o qual tem como

objetivo identificar a unidade de descrição. Essa identificação¹ perpassa, obrigatoriamente, o registro do código do país (BR), o código da entidade custodiadora e o código específico da unidade de descrição (BRASIL, 2006).

Posteriormente, o Conselho Nacional de Arquivos (CONARQ), órgão vinculado ao Arquivo Nacional do Brasil, publicou a Resolução nº 28, de 17 de fevereiro de 2009. Tal resolução define que a instituição terá essa identificação ao realizar o Cadastro Nacional de Entidades Custodiadoras de Acervos Arquivísticos (CODEARQ), que deverá ser solicitada ao CONARQ. Por consequência, os acervos cadastrados terão códigos padronizados para facilitar a distinção entre as instituições cadastradas. Essa resolução também recomenda o uso da Nobrade aos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR) (BRASIL, 2009).

Cabe ao RDC-Arq ter um sistema confiável para localizar os AIP's e seus componentes de forma exclusiva e independente de sua localização física. Logo, é essencial rastrear as ações relacionadas ao AIP no longo prazo, considerando as alterações do sistema e as mudanças de armazenamento. Tal requisito pode ser evidenciado por meio de documentação que descreva a convenção de nomenclatura e a evidência física de sua aplicação. Identificadores únicos para uso interno e externo melhoram a visibilidade no entendimento de gestores e auditores, portanto é ideal que os identificadores sejam gerados no momento da criação do AIP, caso contrário, deve haver rastreabilidade (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Sendo assim, o RDC-Arq deve ser capaz de localizar os AIP's e seus respectivos componentes, mesmo que sejam realizadas atualizações no sistema, no suporte ou no local de armazenamento. Para tanto, deve-se solicitar o Codearq e considerar a implementação de identificadores únicos conforme a NOBRADE.

4.5. Fornecer informação de representação suficiente aos objetos digitais

O RDC-Arq precisa de ferramentas para fornecer informação de representação necessária para todos os objetos digitais armazenados. Portanto, deve identificar os formatos de arquivo dos objetos digitais para vincular a informação de representação de modo que a comunidade designada possa interpretar a informação de conteúdo corretamente (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Ao identificar o formato de arquivo de todos os objetos de dados submetidos, o RDC-Arq buscará técnicas de tratamento específicas para cada formato de arquivo. Posteriormente, deve determinar a informação de representação necessária para tornar cada objeto de dados compreensível à sua comunidade designada, bem como, assegurar que os requisitos da informação de representação são persistentemente associados a tais objetos (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

¹ Por exemplo, o código "BR AN Q6.LEG.COR,TEL" pertence a instituição "Arquivo Nacional do Brasil", e corresponde a subsérie "Telegramas", nível 3,5, do fundo "Floriano Peixoto", seção "Governo Legal", série "Correspondência" (BRASIL, 2006).

Tal requisito pode ser evidenciado por: registros da informação de representação; registros de bases de dados que incluem informação de representação e uma persistente ligação para objetos digitais relevantes. Ressalta-se que este requisito limita-se a exigir que cada RDC-Arq tenha acesso a tais ferramentas, de modo que não o obriga a ter as suas próprias. Isso permite elevar o controle de qualidade e reduzir os custos de manutenção no longo prazo (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

No âmbito dos documentos digitais há outras finalidades para os metadados que vão além das ferramentas para descrição e acesso. Assim, o gerenciamento requer processos para identificar informações de forma precisa, e assim, executá-los adequadamente (SAYÃO, 2010). Nessa perspectiva, os metadados têm finalidades além da busca e recuperação da informação, visto que são essenciais na gestão e na preservação. Logo, podem fornecer informação de representação, ou mesmo relacionar os objetos digitais para facilitar a tramitação, bem como a compreensão da informação de conteúdo.

Assim, o RDC-Arq irá reunir toda a informação de representação necessária, incluindo os metadados, junto aos produtores para garantir a correta interpretação/representação dos objetos digitais pela comunidade designada. Além de cumprir as funções de preservação, o uso de metadados permite relacionar os objetos digitais e fornecer acesso de forma inteligível à documentação.

4.6. Registrar a aquisição e a associação de PDI

Compete ao RDC-Arq registrar a aquisição de PDI que será vinculada à informação de conteúdo para representá-la corretamente. Esse procedimento de coleta de dados deve utilizar um mecanismo padronizado, definido *a priori*.

O RDC-Arq deve assegurar que a PDI é persistentemente associada às informações do conteúdo. Isso requer a manutenção de uma trilha de auditoria para apoiar reivindicações de autenticidade, de modo que mudanças não autorizadas sobre os objetos digitais possam ser detectadas. Dessa forma, é possível identificar os objetos digitais e colocá-los no contexto adequado. Tal requisito pode ser evidenciado por: procedimentos operacionais padronizados; manuais dos procedimentos de admissão; e documentação sobre aquisição/gerenciamento da PDI (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Ressalta-se que os documentos analógicos e os digitais possuem os mesmos componentes. No entanto, pode-se separar, armazenar e gerir os componentes dos documentos digitais individualmente na forma de metadados (RONDINELLI, 2005). Tal peculiaridade demonstra que os documentos arquivísticos em ambiente digital requerem informações adicionais como a PDI. Igualmente, é preciso ter procedimentos para realizar essa associação, e assim contribuir para a sua presunção de autenticidade.

Além de auxiliar o RDC-Arq a garantir que a informação de conteúdo não foi corrompida (informação de fixidez) e que é encontrável (informação de referência); a PDI auxilia na sua compreensão. Para tanto, fornece uma perspectiva histórica (informação de procedência/proveniência) assim como as relações com outros objetos (informação de contexto). Logo, ressalta-se que a PDI deve ser permanentemente associada com a informação de conteúdo (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Com isso, o RDC-Arq irá registrar informações adicionais e autorizadas que se relacionam à fixidez, referência, proveniência e contexto. Esse fluxo de constante associação eleva a

confiabilidade dos procedimentos de aquisição de PDI, de modo a corroborar com a presunção de autenticidade dos AIP's.

4.7. Assegurar que as informações de conteúdo do AIP são compreensíveis

Deve-se assegurar que a informação preservada é compreensível pela comunidade designada, de modo que é possível interpretá-la corretamente por meio de interfaces adequadas sem a necessidade da assistência de terceiros (SARAMAGO, 2004). Assim, o nível de compreensão dos AIP's criados pelo RDC-Arq irá corresponder às expectativas dos consumidores.

Logo, deve-se ter um processo documentado para testar os AIP's, no momento de sua criação, para verificar se a informação de conteúdo do AIP é compreensível à comunidade designada (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b). Assim, poderá inserir informações adicionais, caso seja necessário para representar/interpretar as informações de conteúdo.

Ressalta-se que o teste executado deve se estender para todas as classes de informação de conteúdo que compõem o AIP. Portanto, reúnem-se todos os componentes digitais considerados necessários à compreensão pela comunidade designada.

Caso o teste aponte falha de compreensibilidade, caberá ao RDC-Arq admitir informações adicionais para tornar as informações de conteúdo compreensíveis à comunidade designada. Tal requisito pode ser evidenciado por: procedimentos de teste executados sobre os AIP's para garantir o nível de compreensão definido à comunidade designada; registros desses testes de evidência de recolhimento ou identificação da informação de representação para preencher lacunas de inteligibilidade; e retenção de indivíduos com expertise sobre essa técnica (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

[...] a convergência entre o repositório arquivístico e o OAIS, possibilita manter a autenticidade e a custódia, respeitar os princípios da proveniência e da organicidade, além de manter-se adequado às sete funções arquivísticas. Um RDC-Arq possui uma série de responsabilidades, assim, é possível assegurar que os documentos admitidos podem ser preservados, que existe uma comunidade interessada capaz de compreendê-los, e que existem procedimentos e políticas para garantir a sua preservação e garantia de acesso em longo prazo. Dessa forma, o RDC-Arq consiste em um repositório digital especializado em preservar documentos arquivísticos digitais, e torna-se o “arquivo permanente digital”, um ponto de referência na implementação dos sistemas de arquivo (SANTOS e FLORES, 2019a:129).

Dessa forma, o RDC-Arq deve assegurar que as informações de conteúdo e demais componentes de seus AIP's sejam compreensíveis à comunidade designada. Caso necessário deverá buscar informações adicionais e acrescentá-las ao pacote para torná-lo inteligível aos usuários; ademais, tais ações elevam a presunção de autenticidade dos documentos digitais.

4.8. Verificar a integridade e a exatidão dos AIP's criados

O RDC-Arq deve assegurar que os materiais mantidos em longo prazo podem ser rastreados com as informações fornecidas pelos produtores. Tal requisito pode ser evidenciado pela descrição do procedimento que verifica a integridade e a exatidão dos AIP's. Observa-se que este procedimento tem início na recepção do SIP (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Os documentos devem manter a mesma apresentação que se faz perceptível por meio dos seus elementos identificadores. Portanto, não devem ser alterados, seja de forma intencional ou involuntária. Tal condição está relacionada à custódia confiável exercida pelo produtor ou custodiador devidamente autorizado (SANTOS, 2012). Logo, as únicas alterações possíveis nos documentos devem fazer parte de uma política de preservação definida *a priori*, que mantenha as propriedades significativas.

Dessa forma, caso o RDC-Arq tenha um processo de verificação (integridade e exatidão) do SIP, basta demonstrar como um AIP é derivado de um SIP que tenha sido previamente verificado. Logo, deve-se manter uma descrição capaz de relacionar o AIP armazenado com o SIP submetido pelo produtor, de modo que se consiga recuperar as informações de conteúdo com integridade e exatidão.

4.9. Verificar a integridade do acervo periodicamente

Cabe ao RDC-Arq a responsabilidade de manter um mecanismo independente para verificar a integridade dos conteúdos que armazena. Tal requisito pode ser evidenciado por: documentação de acordos com o produtor; e por relatórios de verificações periódicas. Sendo assim, é preciso demonstrar, para cada item, qual é o AIP do qual é derivado. Entretanto, pode ser necessário, em casos específicos, mostrar que não há AIP para um item, porque a admissão ainda está em andamento, ou porque o item foi rejeitado por algum motivo (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Nesse sentido, o RDC-Arq se compromete em definir, coletar, auditar e fornecer mecanismos para controlar a integridade dos documentos custodiados (BRASIL, 2015). A presunção de autenticidade desses documentos terá com base: a análise de uso, manutenção/preservação, forma e conteúdo. Destaca-se a importância dos procedimentos de controle e do sistema informatizado adotado pelo produtor, de modo a detalhar a produção, tramitação, direitos de acesso, classificação, metadados, preservação e destinação final dos documentos. Para tanto, será preciso um sistema confiável que contenha trilhas de auditoria, controle de usuários, armazenamento estável, controle de segurança da informação e métodos para monitorar alterações nos objetos digitais como *checksum* e/ou *hash* (BRASIL, 2012).

Dessa forma, o RDC-Arq deverá ter um mecanismo independente para verificar a integridade do acervo, identificando cada AIP e seus respectivos componentes. Isso é relevante para garantir princípios arquivísticos como o da proveniência e da indivisibilidade/integridade dos fundos. Tal verificação auxilia para reunir todos os objetos necessários à correta interpretação/representação das informações de conteúdo pela comunidade designada. Igualmente, pode-se verificar a integridade de cada objeto digital com o auxílio das ferramentas de *checksum* e *hash*.

4.10. Registrar ações da administração pertinentes à criação do AIP

O RDC-Arq deve assegurar um meio independente para verificar se todos os AIP's foram criados de acordo com os procedimentos documentados, e que nenhuma ação relevante foi omitida. Esse requisito justifica as práticas do RDC-Arq e pode ser evidenciado por: documentação de decisões e medidas tomadas; e por registros dos metadados de preservação referenciando os objetos digitais. Dessa forma, deve-se demonstrar, por meio de registros contemporâneos, que todas as ações necessárias são realizadas (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Os metadados devem fazer parte de uma política de preservação, de modo que é preciso: definir as responsabilidades pela captura e gerenciamento; identificar os elementos que serão capturados; estabelecer o momento e o método de captura; determinar o seu tempo de guarda; detalhar o armazenamento e as relações com os documentos a quem se referem; garantir que o armazenamento é confiável, com uma trilha de auditoria que registra quaisquer alterações a fim de assegurar a sua autenticidade; ter um *backup*; e manter rotinas de preservação (CASTRO, CASTRO e GASPARIAN, 2007). Assim como os documentos, ressalta-se que os metadados necessitam de rotinas de preservação, manutenção da autenticidade e *backup*.

Com isso, o RDC-Arq demonstra que segue uma política de criação de AIP's previamente definida. De modo que poderá registrar ações relevantes com o uso de metadados de preservação devidamente associados a todos os componentes digitais. Tais procedimentos enriquecem o rol de metadados dos objetos digitais, de modo que registram as ações administrativas pertinentes, logo, elevam a confiabilidade do sistema e corroboram com a presunção de autenticidade dos documentos arquivísticos.

5. Planejamento da preservação

Com relação ao planejamento da preservação, ressalta-se que o RDC-Arq deve identificar e documentar as estratégias de preservação executadas. Ademais, precisa notificar quando a informação de representação adquirir risco de obsolescência, bem como, alterar os planos de preservação conforme os resultados do monitoramento. Com isso, poderá fornecer evidências da eficácia do planejamento da preservação.

5.1. Documentar as estratégias de preservação adequadas ao acervo

Compete ao RDC-Arq fornecer meios para verificar e validar o seu trabalho de preservação. Com isso, define como pretende garantir que as informações permanecerão disponíveis e utilizáveis às gerações futuras. Tal requisito pode ser evidenciado por documentação que identifique cada risco da preservação e as respectivas estratégias para lidar com os riscos (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

As estratégias de preservação digital são essenciais para a confiabilidade do acervo, bem como para garantir o acesso e integridade dos documentos no longo prazo (MÁRDERO ARELLANO, 2004). No entanto, tais estratégias possuem vantagens e desvantagens, de modo que compete a cada instituição identificar o conjunto de estratégias adequado para o tipo de documentação custodiada (SANTOS, 2005).

É preciso considerar a aplicabilidade de uma determinada estratégia para a diversidade de formatos de arquivo existentes. Determinadas estratégias podem ter aplicação restrita a plataformas específicas de *hardware/software*, portanto, a aplicabilidade das estratégias consiste em outro fator para avaliar os serviços de preservação (THIBODEAU, 2002). Com isso surge a necessidade do estudo dos formatos de arquivo a fim de definir a estratégia mais adequada para cada um, o que naturalmente resulta, na necessidade do RDC-Arq implementar mais de uma estratégia.

Tais estratégias definidas no plano estratégico de preservação buscam solucionar riscos como a degradação dos meios de armazenamento, a obsolescência dos suportes de informação, e a obsolescência ou inadequação da informação de representação (incluindo formatos de arquivo). Dessa forma, o RDC-Arq terá o registro de todas as estratégias pertinentes que são utilizadas para preservar os documentos e garantir a autenticidade.

5.2. Ter mecanismos para monitorar o ambiente de preservação

Observa-se que o RDC-Arq precisa reagir às mudanças e assegurar que as informações preservadas se mantêm compreensíveis e utilizáveis pela comunidade designada. Ademais, necessita de um mecanismo para acompanhar e notificar, quando as informações de representação e os formatos de arquivo tornarem-se potencialmente obsoletas. Tal requisito pode ser evidenciado por meio de pesquisas da comunidade designada (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Com o monitoramento do ambiente de preservação o RDC-Arq poderá tomar as decisões adequadas para realizar a manutenção dos objetos digitais, e minimizar os efeitos da obsolescência. Assim, irá assegurar que a comunidade designada será capaz de compreender e utilizar os materiais preservados.

O RDC-Arq deve controlar o acesso ao seu ambiente de administração, permitindo somente pessoas autorizadas. Isso é fundamental para a presunção de autenticidade, de modo que os documentos sejam armazenados em uma “zona militarizada” em que não há acesso direto aos AIP’s, exceto ao administrador do RDC-Arq. Dessa forma, os consumidores somente terão contato com os documentos por meio de uma plataforma de acesso. Tal condição reforça a segurança e a confiabilidade desse ambiente (FLORES, ROCCO e SANTOS, 2016).

Ao monitorar a informação de representação, garante-se que a informação preservada permanecerá compreensível e utilizável pela comunidade designada. Para tanto, além das pesquisas na comunidade designada, pode-se utilizar a assinatura de um serviço de registo das informações de representação e de processos relevantes para lidar com essa informação (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Logo, o RDC-Arq deve manter mecanismos para verificar a obsolescência no que tange a base de conhecimento da comunidade designada. E dessa forma, poderá atualizar ou adicionar a informação de representação necessária para garantir a correta interpretação/representação da informação de conteúdo.

5.3. Adequar o plano de preservação conforme o monitoramento

Cabe ao RDC-Arq demonstrar que está preparado para variações no ambiente externo, sendo capaz alterar o curso do seu plano de preservação conforme as informações de

monitoramento. Tal requisito pode ser evidenciado por: planos de preservação vinculados ao monitoramento tecnológico; processos de preservação voltados ao curto prazo; documentação que comprove as atualizações frequentes das políticas e planos de preservação; e políticas que definam como os planos podem ser atualizados. Da mesma forma, podem-se usar as informações coletadas pelo monitoramento para criar PDI e/ou informações de representação adicionais (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Conforme a tecnologia da informação evolui, torna-se necessário adaptar o processo de preservação dos documentos digitais em virtude do surgimento de novos formatos e funcionalidades. Igualmente, há formatos de arquivo e *softwares* que tornam-se obsoletos. Portanto, o acervo deve estar preparado para transformações de ordem política, tecnológica e financeira. A longevidade do RDC-Arq está relacionada a sua capacidade de adaptação à evolução tecnológica, tendo por missão preservar o patrimônio documental e garantir acesso às gerações futuras (SANTOS e FLORES, 2018).

Com o monitoramento do ambiente de preservação, o RDC-Arq terá condições para alterar o planejamento, de modo a se adequar aos imprevistos e as novas necessidades que surjam durante a execução do plano de preservação. Da mesma forma, poderá reunir informações adicionais que corroborem com a preservação e interpretação dos objetos digitais.

Para tanto, o RDC-Arq necessita de mecanismos para criar, identificar e reunir as informações de representação adicionais. Com isso, pode-se garantir que a informação preservada permanece compreensível e utilizável pela comunidade designada. Tal requisito pode ser evidenciado com: um plano de preservação; uma definição de um serviço de registro de formato; e um serviço de monitoramento tecnológico (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Dessa forma, o RDC-Arq identificará a informação de representação e os formatos de arquivo potencialmente obsoletos. Por conseguinte, irá atualizar o AIP, com adição de PDI ou informações de representação para que possam auxiliar no processo de preservação e na garantia de acesso inteligível.

5.4. Comprovar a eficácia das ações de preservação

Compete ao RDC-Arq demonstrar sua capacidade de manter a informação disponível e utilizável à comunidade designada, tanto no médio, quanto no longo prazo. Tal requisito pode ser evidenciado por: registros de metadados de preservação; prova de usabilidade² dos objetos digitais; e histórico de demonstração para reter objetos digitais utilizáveis no longo prazo (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Tradicionalmente, os Arquivos assim como as Bibliotecas são criados para preservar e garantir a capacidade de acessar as informações registradas no longo prazo, sendo essas as suas principais atribuições. A mesma responsabilidade pela preservação de informações registradas em suportes analógicos é transposta ao ambiente digital (SMITH, 2000).

² O sistema seleciona objetos aleatoriamente para realizar o teste.

Igualmente, é preciso planejar a integração de requisitos para os sistemas de preservação e acesso a fim de mantê-los de forma plena e eficaz para apoiar os processos como a migração e o histórico de custódia dos objetos digitais (HEDSTROM, 1998). Ou seja, tais sistemas não devem ser conflitantes, logo, a escolha dos padrões de metadados deve considerar elementos pertinentes para a presunção de autenticidade, bem como, para facilitar o processo de busca e recuperação da informação no RDC-Arq.

Podem-se realizar testes aleatórios de auditoria, para comprovar a eficiência dos métodos utilizados pelo RDC-Arq. Logo, será possível demonstrar capacidade para preservar continuamente, e garantir a correta representação/interpretação da informação de conteúdo.

6. Preservação do AIP

Preservar as informações de conteúdo dos AIP's requer a implementação de estratégias registradas por meio de metadados adequados, nos quais constam as ações aplicadas. Além disso, o RDC-Arq deve monitorar continuamente a integridade dos AIP's, bem como, manter o registro de ações e processos administrativos pertinentes à preservação.

6.1. Detalhar o armazenamento do AIP

O RDC-Arq deve ter especificações sobre a forma que os AIP's são armazenados até o nível de *bit*. Isso garante que a informação poderá ser extraída no longo prazo. Tal requisito pode ser evidenciado pela documentação que especifica o formato do AIP. Dessa forma, as informações de representação devem especificar os conteúdos de cada componente do AIP até o nível de *bit*, bem como estes componentes são empacotados (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b). Com um conjunto de informações que detalha o armazenamento do AIP, o RDC-Arq poderá recuperar/extrair as informações de conteúdo em qualquer momento.

Destaca-se que a missão fundamental de um RDC-Arq consiste em preservar as informações de conteúdo para suas comunidades designadas. Logo, é preciso demonstrar que os AIP's refletem fielmente as informações de conteúdo que foram capturadas durante a admissão, e que quaisquer transformações planejadas subsequentes continuarão a preservar todas as propriedades das informações requeridas (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Dessa forma, é preciso ter uma política especificando que os AIP's não podem ser excluídos a qualquer momento, assim, preservam-se as ligações entre os AIP's que foram admitidos e as novas versões que tenham sido transformadas ou alteradas *a posteriori*. Tal requisito pode ser evidenciado por: documentação sobre os procedimentos do fluxo de trabalho; documentação sobre a política de preservação especificando o gerenciamento dos AIP's; e ao demonstrar a sequência de conversões realizadas sobre qualquer objeto digital de um AIP (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Com isso, o RDC-Arq manterá registros de todas as transformações realizadas sobre as informações de conteúdo recebidas. Caso sejam necessárias conversões ou informações adicionais, todos estes procedimentos serão registrados, compondo um testemunho do

histórico dos objetos digitais. Logo, esse registro será determinante para assegurar a presunção de autenticidade dos documentos em custódia.

Ressalta-se que a autenticidade dos documentos é determinada por sua tramitação, condições de preservação e custódia. Logo, o conceito de autenticidade depende dos métodos que impedem a adulteração do documento após sua produção (RONDINELLI, 2005). Nesse sentido, detalhar o armazenamento do AIP implica em adicionar informações que se referem a custódia e possíveis manipulações ao ser obtido por meio do SIP.

Para tanto, o RDC-Arq deve monitorar constantemente a integridade do AIP para protegê-lo no longo prazo. Tal requisito pode ser evidenciado ao se adicionar informações de fixidez para cada objeto digital admitido. Assim, o RDC-Arq demonstrará que verifica a integridade de forma regular, captura todas as alterações do AIP e realiza as ações corretivas o mais breve possível (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Observa-se que o RDC-Arq manterá um processo regular de verificação da integridade para cada objeto digital admitido. Dessa forma, irá adicionar informações de fixidez que corroboram com a presunção de autenticidade, além de reparar os objetos que estão corrompidos.

6.2. Registrar as ações administrativas relacionadas aos AIP's

Compete ao RDC-Arq registrar as ações e processos da administração que sejam relevantes ao armazenamento e à preservação dos AIP's. Isso garante que a documentação não é omitida, nem mesmo errônea ou de autenticidade questionável. Tal requisito pode ser evidenciado por meio da documentação de medidas tomadas, e por metadados de preservação associados aos objetos digitais. Esse registro pode ser realizado de forma automatizada ou por indivíduos (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b). Com tais registros em metadados, o RDC-Arq demonstra que todas as ações relevantes foram realizadas e devidamente documentadas, agregando confiabilidade às decisões administrativas proferidas sobre os AIP's.

Para tanto, o RDC-Arq deve ter procedimentos definidos para todas as ações tomadas em cada AIP a fim de assegurar que não ocorreram alterações consideradas inaceitáveis pela comunidade designada. Tal requisito pode ser evidenciado por uma documentação formalizada desde o projeto do RDC-Arq, que descreva todas as ações que podem ser executadas sobre um AIP, e que também defina processos de monitoramento para essas ações (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Assim, o RDC-Arq irá respeitar uma variabilidade limitada, a qual é um parâmetro entre as necessidades de alterar as informações de conteúdo e de manter as propriedades significativas. Com isso, a informação de conteúdo poderá sofrer alterações desde que mantenham as propriedades significativas requeridas para manutenção da sua autenticidade. Logo, as transformações realizadas pelo RDC-Arq não devem descaracterizar os objetos digitais com relação à sua representação, para isso, deve-se considerar um conjunto de alterações aceitáveis, e registrar todas as ações por meio de metadados.

Nessa perspectiva, a autenticidade dos documentos digitais depende do nível de eficácia dos procedimentos de segurança utilizados em sua gênese, tramitação e armazenamento. A sua aceitação como evidência ou prova requer que tais métodos sejam confiáveis

(SANTOS, 2005). Assim, devem-se registrar todos os eventos pertinentes à administração para assegurar a presunção de autenticidade.

O RDC-Arq precisa demonstrar que as medidas tomadas em um AIP estão em conformidade com as especificações das ações definidas *a priori*. Isso assegura que quaisquer ações realizadas sobre um AIP não alteram suas informações de forma inaceitável à comunidade designada. Tal requisito pode ser evidenciado por: metadados de preservação registrados e vinculados aos objetos digitais; documentação sobre as ações realizadas; e auditorias demonstrando que todas as ações mantêm conformidade com os processos documentados (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Quaisquer ações que afetem os conteúdos armazenados no RDC-Arq devem seguir procedimentos previamente estabelecidos, e receber o registro por metadados. Dessa forma, é possível demonstrar que tais alterações são aceitáveis por preservarem o conjunto de propriedades significativas. O registro das alterações corrobora com a presunção de autenticidade de todos os objetos digitais que constituem o AIP.

7. Gestão da informação

O RDC-Arq é responsável por capturar ou criar os metadados de descrição necessários, e associá-los aos AIP's, para que a comunidade designada identifique os materiais de interesse. Assim, é possível demonstrar que a integridade referencial foi criada e mantida entre todos os AIP's e suas informações descritivas associadas.

7.1. Adicionar informação descritiva para recuperar os AIP's

Cabe ao RDC-Arq especificar os requisitos mínimos de informação para permitir que a comunidade designada localize o material de interesse. Tal requisito pode ser evidenciado por: informações descritivas e de recuperação; e demais documentação que descreva os objetos. Assim, os metadados de recuperação localizam os objetos, e a informação descritiva irá descrever o que foi encontrado (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Para isso, pode-se fazer uso da taxonomia a fim de esclarecer conceitos em uso e evitar a criação de novos termos para a mesma finalidade. Logo, é possível introduzir uma ordem para as massas informacionais, de modo a eliminar ambiguidades e classificar os objetos digitais de forma lógica (LUZ, 2010).

Dessa forma, o RDC-Arq deve acrescentar informações descritivas aos objetos digitais admitidos, de modo a auxiliar no processo de busca e recuperação da informação de conteúdo desejada pela comunidade designada. Logo, ressalta-se a necessidade de definir padrões de metadados, assim como um vocabulário controlado e/ou taxinomia para evitar ambiguidades e otimizar a precisão do processo de busca e recuperação da informação.

7.2. Associar a informação descritiva criada/capturada ao AIP

O RDC-Arq deve capturar ou criar informação descritiva suficiente, e assegurar que ela seja associada ao AIP. Tal requisito pode ser evidenciado por: metadados descritivos; identificadores únicos (internos ou externos) para cada AIP; documentação e arquitetura

técnica; acordos de depósito; documentação do fluxo de trabalho; política de metadados documentada incorporando detalhes dos requisitos; e declaração de responsabilidade pela aquisição. Dessa forma, é possível demonstrar que o RDC-Arq associa a informação descritiva suficiente para cada AIP. Observa-se que tal associação não precisa, necessariamente, ser armazenada com o AIP (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Há de se ressaltar aspectos que diferenciam a preservação de documentos digitais bibliográficos dos arquivísticos. Os Arquivos são constituídos naturalmente em virtude das atividades do produtor (proveniência), portanto, as relações entre os documentos (organicidade) são essenciais no processo de busca, recuperação e compreensão das informações registradas (MÁRDERO ARELLANO e ANDRADE, 2006). Sendo assim, além de contribuir para a presunção de autenticidade, a associação de informações descritivas contribuem para manter outros princípios, como os da proveniência e da organicidade, ademais auxiliam no acesso à informação.

O RDC-Arq deverá associar a informação descritiva necessária para cada AIP, de modo que poderá atuar por meio de identificadores únicos. Da mesma forma, a informação descritiva poderá fornecer detalhes adicionais relacionados às responsabilidades advindas do processo de admissão de conteúdos. Ressalta-se que essa descrição deve seguir os padrões preconizados pela Arquivística a fim de assegurar seus princípios.

7.3. Manter relação bidirecional entre o AIP e sua informação descritiva

Cabe ao RDC-Arq manter ligação bidirecional entre cada AIP e sua informação descritiva, pois isso assegura que todos os AIP's poderão ser devidamente localizados e recuperados. Tal requisito pode ser evidenciado por: metadados descritivos; identificador único/localizador associado ao AIP; documentação sobre a relação entre o AIP e seus metadados; documentação do sistema e arquitetura técnica; e documentação do fluxo de trabalho (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b). Dessa forma, o RDC-Arq deve estabelecer e manter informações descritivas associadas para cada AIP em uma relação bidirecional, permitindo que um possa ser encontrado por meio do outro.

Nessa perspectiva, a Ciência da Informação vislumbra a descrição de objetos digitais com objetivo de recuperar a informação armazenada. Observa-se que a descrição arquivística e a descrição bibliográfica possuem seus próprios padrões que comportam o contexto e o conteúdo dos documentos digitais. No entanto, tais padrões começam a se homogeneizar, o que poderá facilitar a criação de redes interoperáveis entre Arquivos e Bibliotecas (MÁRDERO ARELLANO e ANDRADE, 2006). Embora os Arquivos e as Bibliotecas tenham objetos de estudo e técnicas diferentes, há possibilidade de trocar conhecimentos no uso de padrões de metadados e requisitos de segurança dos sistemas informatizados, respeitando as peculiaridades de cada área.

Os AIP's podem ser recuperados no longo prazo ao se manter uma associação contínua com as suas informações descritivas. Tal requisito pode ser evidenciado pelo detalhamento da manutenção contínua ou verificação da integridade dos dados e as suas relações com a informação descritiva associada, especialmente após a reparação ou modificação do AIP. Além de outras questões como a documentação do sistema e da arquitetura técnica, a documentação dos processos de fluxo de trabalho, o registro de informações descritivas, a

persistência do identificador/localizador, e a documentação sobre a relação entre o AIP e sua informação descritiva (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

De forma geral, o RDC-Arq deve identificar qualquer interrupção entre os AIP's e a informação descritiva associada, para garantir que ela poderá ser restaurada. Essa relação bidimensional contribui para a recuperação da informação de conteúdo, dá sentido aos objetos digitais, e evita que se percam dentro do RDC-Arq.

8. Gestão de acesso

A gestão de acesso permite ao RDC-Arq documentar e comunicar opções de acesso/entrega que estão disponíveis à comunidade designada. Todas as solicitações de acesso devem ser registradas, e visam atender aos requisitos do RDC-Arq e dos produtores, além de cumprir os acordos relacionados às condições de acesso. A gestão de acesso irá definir e implementar uma política de acesso segura via sistema de gerenciamento, aos contratos de depósito. Dessa forma, demonstra-se que todas as solicitações de acesso resultam em uma resposta de aceitação ou rejeição, logo, devem-se registrar todas as falhas de gerenciamento de acesso e analisar os casos em que houver negação de acesso.

8.1. Cumprir as políticas de acesso

Compete ao RDC-Arq resolver todos os aspectos do uso que podem afetar a sua confiabilidade, especialmente, no que se refere ao suporte oferecido à sua comunidade de usuários. Tal requisito pode ser evidenciado por: trilhas de auditoria sobre solicitações de acesso; testes explícitos de alguns tipos de acesso; disponibilização das políticas para as comunidades de usuários; e informações sobre as capacidades dos usuários. Dessa forma, definem-se condições e os mecanismos para controle de acesso, relacionados à autenticação, autorização e registro de acesso (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Além de definir o planejamento, os objetivos e o escopo da preservação digital, é preciso considerar as peculiaridades dos consumidores. De modo que há consumidores tecnicamente avançados, que por sua vez, exigem menos assistência durante o acesso. Em contrapartida, os demais consumidores podem exigir *interfaces* de acesso “amigáveis”, bem como, materiais convertidos para formatos de arquivo “simples” (INTERPARES, 2007a).

Ademais, o RDC-Arq deverá demonstrar que cumpre as políticas de acesso, de modo que atende todas as solicitações da comunidade designada e mantém mecanismos de autenticação de usuários para controlar o acesso. Igualmente, desperta-se a importância de se registrar e analisar as falhas que ocorrerem.

Dessa forma, o RDC-Arq poderá identificar ameaças de segurança e falhas no sistema de gerenciamento de acesso. Tal requisito pode ser evidenciado ao demonstrar que o sistema tem capacidade de usar ferramentas para análise/monitoramento automatizado e gerar mensagens de problema/erro. Da mesma forma, pode-se demonstrar com notas de avaliações realizadas ou medidas tomadas como resultado de comentários. Portanto, o RDC-Arq precisa ter um mecanismo automatizado para rastrear negações anômalas ou

incomuns, e usá-las para identificar ameaças ou falhas de segurança no sistema de gestão de acesso (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Com isso, o RDC-Arq irá descobrir todas as falhas relacionadas ao acesso que afetam a sua confiabilidade. Ao identificar anomalias e vulnerabilidades podem-se concentrar esforços para solucioná-las.

8.2. Ter políticas e procedimentos para disseminar objetos digitais

Cabe ao RDC-Arq seguir políticas e procedimentos que permitam a disseminação objetos de digitais. Tais objetos devem ser rastreáveis em relação aos originais. Com isso, se estabelece uma cadeia de autenticidade auditável do AIP para os objetos digitais disseminados. Esse requisito pode ser evidenciado com: procedimentos de orientação; e documentação dos requisitos de autenticidade (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Tais evidências são fundamentais para avaliar a presunção de autenticidade, e demonstrar que os materiais admitidos não perdem informações durante as transformações. Dessa forma, devem-se registrar os processos de construção do Pacote de Informação para Disseminação (*Dissemination Information Package – DIP*) a partir do AIP, sendo derivado de transformação ou cópia idêntica, porém sempre refletindo o seu conteúdo original (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b). Logo, torna-se fundamental definir procedimentos padronizados para a criação do DIP a fim de assegurar a presunção de autenticidade frente ao AIP.

A confiabilidade da informação é um problema crescente tendo em vista as fontes de informação via *internet*. Ademais, deve-se observar a diferença entre informação confiável e informação verdadeira. A informação confiável é aquela em que os consumidores acreditam, mesmo que não seja possível atestar a sua veracidade (DE SORDI, 2008). Sendo assim, a acurácia e a autenticidade da informação podem ser presumidas em um sistema de preservação confiável. Logo, devem existir mecanismos para identificar e registrar todas as alterações nos documentos e seus componentes digitais. Caso não existam alterações indevidas, esses documentos serão autênticos (INTERPARES, 2007b; THIBODEAU, 2002).

Para tanto, surge a necessidade do RDC-Arq ser considerado uma fonte de informação confiável por seus utilizadores. Tal requisito pode ser evidenciado por documentação sobre: o projeto do sistema; e os relatórios de erros com as respectivas ações tomadas. Dessa forma, estima-se que o usuário irá receber uma versão do objeto digital utilizável em conformidade com o que foi requerido. Caso ocorram quaisquer problemas que sejam levados ao seu conhecimento, estes serão investigados e tratados. Ressalta-se que essa resposta é essencial para o RDC-Arq ser considerado confiável (CONSULTATIVE..., 2011; INTERNATIONAL..., 2012b).

Portanto, o RDC-Arq deverá considerar os relatórios de erros sobre as solicitações de acesso, de modo que a sua confiabilidade estará relacionada à capacidade de investigar e tomar decisões com relação a tais erros. Logo, as ações tomadas para solucionar os problemas de acesso irão despertar a confiança da comunidade designada.

9. Considerações finais

Este estudo realizou uma triangulação entre a gestão de objetos digitais (conforme o ACTDR), os fundamentos da Arquivística, e o RDC-Arq. Com isso, obteve-se um artigo de revisão narrativa capaz de elucidar as relações entre o modelo OAIS e o padrão de auditoria ACTDR, com os princípios da Arquivística.

Tais aspectos são sistematizados no escopo do RDC-Arq, ideal para preservar documentos arquivísticos em ambiente digital, de modo que respeita os princípios da proveniência, organicidade, unicidade, indivisibilidade e naturalidade. Igualmente, visa manter uma cadeia de custódia ininterrupta, executar estratégias de preservação digital, entre outras atividades, as quais são devidamente registradas por meio de metadados.

O RDC-Arq é entendido como um ambiente confiável, capaz de preservar e garantir acesso aos documentos no longo prazo com garantia de autenticidade. Ademais, é uma construção que segue os moldes da preservação digital sistêmica, fundamentada em normas e padrões pertinentes à comunidade de preservação. Daí compreende-se a importância de tomar por base estudos como OAIS, ACTDR, Nobrade, entre outros, e buscar uma convergência em prol Arquivística, que ainda está se familiarizando com a preservação digital.

Há de se ressaltar que estudos como o OAIS e o ACTDR possuem uma terminologia intercambiável, de modo que são compreensíveis às diversas áreas que têm a informação registrada como um de seus objetos. No entanto, há peculiaridades que devem ser respeitadas, por exemplo, na distinção do universo teórico-prático de Arquivos e Bibliotecas. Portanto, buscou-se fundamentar e adaptar a seção “gestão de objetos digitais” tendo em vista a auditoria de RDC-Arq’s.

Observa-se que a gestão de objetos digitais, é relacionada ao tratamento da informação de conteúdo por meio de intervenções, e compreende os requisitos necessários desde a sua aquisição até os meios para garantir acesso à comunidade designada. Assim, após a aquisição, são perpassadas questões relativas ao processo de criação do AIP, políticas de preservação, planejamento, manutenção dos AIP’s, gerenciamento das informações por metadados, e políticas de acesso.

Ao cumprir os requisitos da gestão de objetos digitais, o RDC-Arq demonstra que segue procedimentos padronizados para tratar pacotes AIP, e mantém conformidade com os fluxos de informação preconizados pelo OAIS. Essas atividades correspondem às intervenções realizadas diretamente nos objetos digitais, como, por exemplo, migração e inserção de metadados. Logo, tais requisitos auxiliam o auditor na verificação da conformidade do RDC-Arq com OAIS.

Ao perpassar os diversos requisitos para auditoria, observou-se a pertinência de questões como as propriedades significativas e a variabilidade limitada. Tais questões impactam diretamente na presunção de autenticidade, de modo que reforçam a adaptação de preceitos do ambiente analógico para o digital. Somam-se a esses, os conceitos tradicionais de princípios e funções, igualmente adaptados ao contexto dos documentos digitais, os quais remodelam o *corpus* teórico da Arquivística e expandem o seu horizonte de atuação.

Por fim, este estudo contribui para fomentar pesquisas em torno da auditoria de RDC-Arq’s conforme o ACTDR, pois fornece subsídios teóricos suficientes para compreender as especificidades dos documentos arquivísticos e as complexidades do ambiente digital. Sua

principal limitação consiste em abordar apenas a gestão de objetos digitais do ACTDR, de modo que não versa sobre as políticas organizacionais e a segurança da informação. No entanto, tal delimitação permite explorar os requisitos e contextualizá-los na literatura, tanto da Arquivística quanto de preservação digital. Com isso, espera-se que a Arquivística possa se apropriar de discussões em torno das normas e padrões que circunscrevem a preservação digital sistêmica.

Referências bibliográficas

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.

BELLOTTO, H. L.

2014a Constituição, dispersão e reintegração de fundos. In BELLOTTO, H. L. – *Arquivo: estudos e reflexões*. Belo Horizonte: Editora UFMG, 2014, cap. 1, p. 80-94.

BELLOTTO, H. L.

2014b Da gênese à função: o documento de arquivo como informação e testemunho. In BELLOTTO, H. L. – *Arquivo: estudos e reflexões*. Belo Horizonte: Editora UFMG, 2014, cap. 3, p. 329-344.

BOERES, S. A. A.; CUNHA, M. B.

2012 Competências básicas para os gestores de preservação digital. *Ciência da Informação*. [Em linha]. 41:1 (2012) 103-113. [Consult. 17 nov. 2019]. Disponível em: <http://revista.ibict.br/ciinf/article/view/1356/1535>.

BRASIL. Conselho Nacional de Arquivos

2009 *Resolução no 28, de 17 de fevereiro de 2009*. [Em linha]. 2009. [Consult. 17 nov. 2019]. Disponível em: <http://conarq.arquivonacional.gov.br/index.php/resolucoes-do-conarq/270-resolucao-n-28,-de-17-de-fevereiro-de-2009>.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos

2015 *Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis: RDC-Arq*. [Em linha]. Rio de Janeiro: Arquivo Nacional, 2015. [Consult. 17 nov. 2019]. Disponível em: http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos

2012 *Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais*. [Em linha]. Rio de Janeiro: Arquivo Nacional, 2012. [Consult. 17 nov. 2019]. Disponível em: http://conarq.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_e_completa.pdf.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos

2004 *Carta para a preservação do patrimônio arquivístico digital*. [Em linha]. Rio de Janeiro: Arquivo Nacional, 2004. [Consult. 17 nov. 2019]. Disponível em: http://www.conarq.gov.br/images/publicacoes_textos/Carta_preservacao.pdf.

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Normalização da Descrição Arquivística

2006 *Norma brasileira de descrição arquivística: NOBRADE*. Rio de Janeiro: Arquivo Nacional, 2006.

CASANOVAS, I.

2008 *Gestión de archivos electrónicos*. Buenos Aires: Alfagrama, 2008.

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

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

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM

2012 *Reference model for an Open Archival Information System: OAIS*. [Em linha]. Washington: CCSDS, 2012. [Consult. 17 nov. 2019]. Disponível em: <http://public.ccsds.org/publications/archive/650xom2.pdf>.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM

2011 *Audit and Certification of Trustworthy Digital Repositories: ACTDR*. [Em linha]. Washington: CCSDS, 2011. [Consult. 17 nov. 2019]. Disponível em: <http://public.ccsds.org/publications/archive/652xom1.pdf>.

CORDEIRO, A. M. [et al.]

2007 Revisão sistemática: uma revisão narrativa. *Revista do Colégio Brasileiro de Cirurgiões*. [Em linha]. 34:6 (2007) 428-431. [Consult. 17 nov. 2019]. Disponível em: <http://dx.doi.org/10.1590/S0100-69912007000600012>.

DE SORDI, J. O.

2008 *Administração da informação : fundamentos e práticas para uma nova gestão do conhecimento*. São Paulo: Saraiva, 2008.

DELMAS, B.

2010 *Arquivos pra quê?: textos escolhidos*. São Paulo: iFHC, 2010.

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. 17 nov. 2019]. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/download/717/732/>.

GIL, A. C.

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

GONÇALVES, E. P.

2011 *Conversas sobre iniciação científica*. 5ª ed. Campinas: Alínea, 2011.

HEDSTROM, M.

1998 Digital preservation: a time bomb for digital libraries. *Computer and the humanities*. [Em linha]. 31 (1998) 189-202. [Consult. 17 nov. 2019]. Disponível em: http://deepblue.lib.umich.edu/bitstream/2027.42/42573/1/10579_2004_Article_153071.pdf.

INNARELLI, H. C.

2009 Preservação digital e seus dez mandamentos. In SANTOS, V. B. – *Arquivística: temas contemporâneos*. 3ª ed. Distrito Federal: SENAC, 2009, cap. 1, p. 21-75.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

2012a *INTERNATIONAL... 14.721: 2012: space data and information transfer systems: Open Archival Information System: reference model*. Genebra: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

2012b *INTERNATIONAL... 16.363: 2012: space data and information transfer systems: audit and certification of trustworthy digital*. Genebra: ISO, 2012.

INTERPARES 2 PROJECT

2007a *Diretrizes do preservador: a preservação de documentos arquivísticos digitais: diretrizes para organizações*. Trad. Arquivo Nacional e Câmara dos Deputados. [Em linha]. Vancouver: University of British Columbia, 2007. [Consult. 17 nov. 2019]. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf.

INTERPARES 2 PROJECT

2007b *Diretrizes do produtor: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos*. Trad. Arquivo Nacional do Brasil e Câmara dos Deputados. [Em linha]. Vancouver: University of British Columbia, 2007. [Consult. 17 nov. 2019]. Disponível em: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf.

LOPES, L. C.

2014 *A Nova administração na modernização arquivística*. 3ª ed. Brasília: Annabel Lee, 2014.

LOPEZ, A. P. A.

2004 Princípios arquivísticos e documentos digitais. *Revista do Arquivo Público e Histórico do Município de Rio Claro*. [Em linha]. 2 (2004) 70-85. [Consult. 17 nov. 2019]. Disponível em: <https://repositorio.unb.br/handle/10482/1428>.

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.

MÁRDERO ARELLANO, M. A.

2004 Preservação de documentos digitais. *Ciência da Informação*. [Em linha]. 33:2 (2004) 15-27. [Consult. 17 nov. 2019]. Disponível em: <http://revista.ibict.br/ciinf/article/view/1043/1113>.

MÁRDERO ARELLANO, M. A.; ANDRADE, R. S.

2006 Preservação digital e os profissionais da informação. *DataGramaZero*. [Em linha]. 7:5 (2006) [Consult. 17 nov. 2019]. Disponível em: <http://repositorio.ufba.br/ri/handle/ri/3039>.

OLIVEIRA, E. B.; BATISTA, D. A.

2019 Auditoria arquivística: uma proposta de requisitos. *Informação & Sociedade: estudos*. [Em linha]. 29:1 (2019). [Consult. 17 nov. 2019]. Disponível em: <https://repositorio.unb.br/handle/10482/20288>.

PESTANA, O.

Auditoria de informação: definição e evolução da atividade no contexto da gestão da informação e das organizações. *Páginas a&b : arquivos e bibliotecas*. [Em linha]. 2 (2014) 49-64. [Consult. 17 nov. 2019]. Disponível em: <http://ojs.letras.up.pt/index.php/paginasueb/article/view/599/579>.

PINTO, M. M. G. A.

2009 *PRESEVMAP: um roteiro da preservação na era digital*. Porto: Edições Afrontamento; CETAC.media, 2009.

ROCHA, C. L.; SILVA, M.

2007 Padrões para garantir a preservação e o acesso aos documentos digitais. *Acervo*. [Em linha]. 20:1 (2007) 113-124. [Consult. 17 nov. 2019]. Disponível em: <http://revistaacervo.an.gov.br/index.php/revistaacervo/article/view/76/76>.

RONDINELLI, R. C.

2013 *O Documento arquivístico ante a realidade digital: uma revisão conceitual necessária*. Rio de Janeiro: Fundação Getúlio Vargas, 2013.

RONDINELLI, R. C.

2005 *Gerenciamento arquivístico de documentos eletrônicos : uma abordagem teórica da diplomática arquivística contemporânea*. 4ª ed. Rio de Janeiro: Fundação Getúlio Vargas, 2005.

SANTOS, H. M.; FLORES, D.

2019a Introdução aos conceitos básicos do modelo Open Archival Information System no contexto da arquivística. *Acervo*. [Em linha]. 32:1 (2019) 8-26. [Consult. 17 nov. 2019]. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/981/118>.

SANTOS, H. M.; FLORES, D.

2019b Responsabilidades de um Repositório Arquivístico Digital Confiável na perspectiva do Open Archival Information System. *Páginas a&b: arquivos e bibliotecas*, 11:3 (2019b), p. 116-132. [Consult. 17 nov. 2019]. Disponível em: <https://doi.org/10.21747/21836671/pag11a9>.

SANTOS, H. M.; FLORES, D.

2018 Novos rumos da preservação digital: das estratégias aos sistemas informatizados. *Biblios: Journal of Librarianship and Information Science*. [Em linha]. 70 (2018) 31-43. [Consult. 17 nov. 2019]. Disponível em: <http://dx.doi.org/10.5195/biblios.2017.326>.

SANTOS, V. B.

2012 Preservação de documentos arquivísticos digitais. *Ciência da Informação*. [Em linha]. 41:1 (2012) 114-126. [Consult. 17 nov. 2019]. Disponível em: <http://revista.ibict.br/ciinf/article/view/1357>.

SANTOS, V. B.

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

SARAMAGO, M. L.

2004 Metadados para preservação digital e aplicação do modelo OAIS. In CONGRESSO NACIONAL DE BIBLIOTECARIOS, ARQUIVISTAS E DOCUMENTALISTAS, 8º, Estoril, 2004 - *Nas encruzilhadas da informação e da cultura: (re)inventar a profissão: actas*. Estoril: BAD, 2004. [Consult. 17 nov. 2019]. Disponível em: <https://www.bad.pt/publicacoes/index.php/congressosbad/article/view/640/637>.

SAYÃO, L. F.

2010 Uma Outra face dos metadados: informações para a gestão da preservação digital. *Encontros Bibli: revista eletrônica de Biblioteconomia e Ciência da Informação*. [Em linha]. 15:30 (2010) 1-31. [Consult. 17 nov. 2019]. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2010v15n30p1>.

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

2005 *Metodologia da pesquisa e elaboração de dissertação*. [Em linha]. Florianópolis: UFSC, 2005. [Consult. 17 nov. 2019]. Disponível em: https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf.

SILVA, M.

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

SMITH, A.

2000 Digital preservation research and developments. *Russian Digital Libraries Journal*. [Em linha]. 3:3 (2000). [Consult. 17 nov. 2019]. Disponível em: <https://elbib.ru/ru/article/77>.

THIBODEAU, K.

2002 *Overview of technological approaches to digital preservation and challenges in coming years: the state of digital preservation*. Washington: CLIR and Library of Congress, 2002. [17 nov. 2019]. Disponível em: <http://www.clir.org/pubs/reports/pub107/thibodeau.html>.

THOMAZ, K. P.

2007 Repositórios digitais confiáveis e certificação. *Arquivística.net*. [Em linha]. 3:1 (2007) 80-89. [Consult. 17 nov. 2019]. Disponível em: http://www.brapci.inf.br/repositorio/2010/05/pdf_fedo72oddb_0010726.pdf.

THOMAZ, K. P.

2006 Gestão e preservação de documentos eletrônicos de arquivo: revisão de literatura. Parte 2. *Arquivística.net*. [Em linha]. 2:1 (2006) 114-131. [Consult. 17 nov. 2019]. Disponível em: <http://www.brapci.inf.br/index.php/article/download/6733>.

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

2004 A Preservação digital e o modelo de referência Open Archival Information System: OAIS. *DataGramZero*. [Em linha]. 5:1 (2004). [Consult. 17 nov. 2019]. Disponível em: <http://www.brapci.inf.br/index.php/article/download/7616>.

VOLPATO [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