https://doi.org/10.29397/reciis.v14i3.2089

ARTIGOS DE REVISÃO

Preservação sistêmica para repositórios arquivísticos

Systemic preservation for archival repositories

Preservación sistémica para repositorios de archivo

Henrique Machado dos Santos[1,a]
henrique.hms.br@gmail.com | https://orcid.org/0000-0002-2497-7321

Daniel Flores[2,b]
dfloresbr@gmail.com | http://orcid.org/0000-0001 -8888-2834

[1] Universidade Federal do Rio Grande, Arquivo Geral. Rio Grande, RS, Brasil.
[2] Universidade Federal Fluminense, Departamento de Ciência da Informação. Niterói, RJ, Brasil.

[a] Mestrado em Patrimônio Cultural pela Universidade Federal de Santa Maria.
[b] Doutorado em Metodologías y Líneas de Investigación en Biblioteconomía y Documentación pela Universidad de Salamanca.

RESUMO

Este estudo realiza uma reflexão sobre a preservação de documentos arquivísticos digitais em uma perspectiva sistêmica, pautada em padrões reconhecidos pela literatura científica. De tal forma, utiliza-se da visão holística para ressaltar a pertinência da preservação ser pensada em todo o ciclo de vida dos documentos. A metodologia parte do levantamento bibliográfico composto por artigos, livros e publicações técnicas, para assim, obter uma revisão narrativa. Ressalta-se que a preservação digital tem evoluído para novos patamares e requer o uso de padrões para implementar sistemas informatizados confiáveis. Com isso, pode-se envolver todo o ciclo vital em uma cadeia de custódia ininterrupta capaz de assegurar a autenticidade dos documentos digitais. Por fim, defende-se uma abordagem sistêmico-holística, em que os documentos são planejados e produzidos tendo em vista a preservação e o acesso em longo prazo.

Palavras-chave: Preservação digital; Documentos digitais; Repositórios digitais; Cadeia de custódia; Documento arquivístico; Arquivologia; Gestão de documentos.

ABSTRACT

This study reflects on the preservation of digital archival records from a systemic perspective, based on standards recognized by scientific literature. In such a way, it uses a holistic view to emphasize the relevance of preservation to be considered throughout the life cycle of records. The methodology is based on a bibliographic survey composed of articles, books, and technical publications, to obtain a narrative review. It is noteworthy that digital preservation has evolved to new heights, and requires the use of standards to implement reliable computer systems. With this, the entire life cycle can be involved in an uninterrupted chain of custody capable of ensuring the authenticity of digital records. Finally, a systemic-holistic approach is advocated, in which records are planned and produced with a view of the preservation and access in the long-term.

Keywords: Digital preservation; Digital records; Digital repositories; Chain of custody; Archival record; Archival Science; Records management.

RESUMEN

Este estudio reflexiona sobre la preservación de los documentos de archivo digital en una perspectiva sistémica, basada en normas y estándares reconocidos por la literatura científica. De esta manera, utiliza la visión holística para enfatizar la relevancia de la preservación a ser considerada a lo largo del ciclo de vida de los documentos. La metodología se basa en una encuesta bibliográfica compuesta de artículos, libros y publicaciones técnicas, para obtener una revisión narrativa. Es de destacar que la preservación digital ha evolucionado a nuevas alturas y requiere el uso de estándares para implementar sistemas informáticos confiables. Con esto, todo el ciclo de vida puede involucrarse en una cadena de custodia ininterrumpida capaz de garantizar la autenticidad de los documentos digitales. Finalmente, se aboga por un enfoque holístico-sistémico, en que los documentos se planifican y producen con miras la preservación y acceso a largo plazo.

Palabras-clave: Preservación digital; Documentos digitales; Repositorios digitales; Cadena de custodia; Documento de archivo; Archivología; Gestión de documentos.

INFORMAÇÕES DO ARTIGO

Este artigo compõe o dossiê Preservação Digital.

Contribuição dos autores:
Concepção e desenho do estudo: Daniel Flores, Henrique Machado dos Santos.
Aquisição, análise ou interpretação dos dados: Daniel Flores, Henrique Machado dos Santos.
Redação do manuscrito: Henrique Machado dos Santos.
Revisão crítica do conteúdo intelectual: Daniel Flores, Henrique Machado dos Santos.

Declaração de conflito de interesses: não há.

Fontes de financiamento: não houve.

Considerações éticas: não há.

Agradecimentos/Contribuições adicionais: não há.

Histórico do artigo: submetido: 18 abr. 2020 | aceito: 26 jun. 2020 | publicado: 30 set. 2020.

Apresentação anterior: não há.

INTRODUÇÃO

A preservação de documentos digitais se tornou um tema de constante discussão no âmbito da Arquivística/ Arquivologia. A possibilidade de separar a informação do suporte é uma exclusividade do ambiente digital que rompe com os tradicionais conceitos de documento arquivístico, atrelados à ideia de fixação. Com isso, além das ferramentas de tecnologia da informação permitirem produzir, editar, disseminar e excluir documentos com facilidade, é possível migrar as informações de um suporte para outro.

Entende-se que o documento digital (*digital record*) consiste na informação registrada e codificada em dígitos binários. Assim poderá ser armazenado em suportes magnéticos, ópticos ou óptico-magnéticos e interpretado por sistemas informatizados. Ademais, destaca-se a existência do documento nato-digital, que é originalmente produzido em formato digital (*born digital*), diferenciando-lhe dos demais documentos digitais, como por exemplo, aqueles que são produzidos originalmente em formato analógico e posteriormente convertidos em formato digital por meio da digitalização. Os demais documentos em suportes como o papel são conhecidos como analógicos, convencionais ou 'não digitais'.

No entanto, todo esse dinamismo proporcionado pela evolução das tecnologias da informação pode ser considerado uma vulnerabilidade. As plataformas de *hardware*, *software* e os suportes digitais estão em constante transformação, e o seu avanço desenfreado provoca a obsolescência tecnológica, em ciclos cada vez mais curtos. Igualmente, o conhecimento sobre tais tecnologias é ameaçado, pois força os profissionais a manterem uma constante atualização de seus conhecimentos, negligenciando inclusive, o conhecimento sobre plataformas ditas ultrapassadas.

Nessa perspectiva, o patrimônio arquivístico passou a ser composto por documentos analógicos e documentos digitais. Ademais, observa-se que os documentos digitais ainda podem ser produzidos por tecnologias atuais e potencialmente obsoletas, fator que adiciona complexidade ao processo de preservação. Logo, é preciso manter conformidade com as especificidades do documento arquivístico, dentre elas, a relação orgânica, a proveniência, o registro da custódia, a forma fixa e o conteúdo estável, artifícios que corroboram para manter a autenticidade.

Para contornar os efeitos da obsolescência tecnológica e manter conformidade com as complexidades da tecnologia e as especificidades da Arquivística, convencionou-se a definição de políticas de preservação digital, que devem ser implementadas no âmbito organizacional. Trata-se de um planejamento estratégico que define a infraestrutura, as tecnologias, as pessoas, as fontes de recursos e demais esforços necessários para que a organização obtenha êxito no processo de preservação em longo prazo. Tais políticas consistem em uma série de procedimentos e requisitos que orientam a produção, o uso e o armazenamento dos documentos arquivísticos digitais, tendo em vista a preservação e a garantia de acesso contínuo ao longo do tempo.

A definição de uma política de preservação em nível organizacional demonstra que as ações proferidas sobre os documentos devem ser realizadas por meio da automação. Logo, é preciso dispor de sistemas informatizados para gerir os documentos arquivísticos digitais, doravante, sistemas de gestão e de preservação. Estes sistemas informatizados são cruciais para registrar todas as intervenções e alterações nos documentos por meio de metadados, a fim de assegurar a autenticidade.

Sendo assim, a preservação digital passa a ser pensada antes mesmo da produção dos documentos, o que reforça a ideia de se preocupar com todo o ciclo vital, não se limitando ao ambiente de preservação. A visão do todo aliada à normatização dos procedimentos irá adicionar confiabilidade ao processo de preservação.

Tendo em vista o exposto, tem-se por objetivo realizar uma reflexão sobre a perspectiva sistêmica da preservação digital, de modo que seja orientada por normas e padrões relevantes à literatura científica. Ademais, pretende-se expandir o horizonte da preservação para uma visão holística, que comporta todo o ciclo de vida dos documentos arquivísticos.

Para tanto, a metodologia parte do levantamento bibliográfico[1,2] composto por livros, publicações técnicas e artigos científicos. Sendo que os artigos são recuperados por meio de bases de dados elencadas no Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), dentre elas: a ferramenta de pesquisa Google Scholar e Scientific Electronic Library Online (SciELO).

Destaca-se que o Google Scholar e a SciELO possuem viés multidisciplinar, tendo capacidade de recuperar materiais de diversas fontes de informação. Ademais, utilizou-se a Base de Dados em Ciência da Informação (BRAPCI), que se concentra na área de Ciência da Informação e indexa diversos periódicos do Brasil e do exterior. Os dados coletados são analisados na perspectiva sistêmica aliada à abordagem holística de ciclo de vida documental. Dessa forma, o presente estudo caracteriza-se pela subjetividade da interpretação[3], e a discussão dos resultados segue a lógica dedutiva[4].

Obtém-se um artigo de revisão assistemática/narrativa[5] que parte da temática aberta, fundamentada pelos referenciais da Arquivística e da preservação digital, e que, posteriormente, estabelece relação com padrões, tendo em vista orientar a implementação dos sistemas informatizados de gestão e preservação.

CADEIA DE CUSTÓDIA ININTERRUPTA

A manutenção da autenticidade está relacionada à custódia adequada que se estende desde o produtor e pode perpassar uma sequência de custodiadores autorizados. Ou seja, a responsabilidade legal pela custódia pode ser transmitida entre indivíduos no decorrer do tempo. O rigor dos mecanismos de segurança e preservação, empregados por estes indivíduos, presume que os documentos arquivísticos não tenham sido alterados, com ou sem intenção[6]. A custódia visa proteger o acervo, de modo que os documentos possam ser utilizados como fonte de evidência ou prova. Logo, os planos de sucessão dos documentos arquivísticos devem ser executados sob uma cadeia de custódia ininterrupta, para garantir a confiabilidade do procedimento.

Para documentos analógicos, a manutenção de uma cadeia de custódia ininterrupta, entre produtor e preservador, era suficiente para assegurar a autenticidade. De modo que, fora dessa cadeia, o acervo poderia sofrer mutilações, bem como ficar sujeito a falsificações e, assim, gerar dúvidas com relação à autenticidade dos documentos[7].

No entanto, quando abordada em ambiente digital, a custódia torna-se um desafio significativo em virtude das diversas vulnerabilidades apresentadas pelos documentos arquivísticos digitais. Logo, surgiu a necessidade de revisitar o conceito de custódia para compreender como esta seria adaptada.

A autenticidade dos documentos analógicos é assegurada conforme suas características sejam mantidas de forma inalterada, aspecto igualmente válido para documentos digitais. No entanto, a preservação digital requer alterações, como por exemplo, os procedimentos de migração e até mesmo cópia, tendo em vista a fragilidade dos suportes e a obsolescência tecnológica de *hardware* e *software*. Nessa perspectiva, a inserção controlada de metadados torna-se necessária à presunção de autenticidade, pois permite ter ciência dos procedimentos executados sobre os documentos[8]. Os problemas relacionados à autenticidade dos documentos digitais são semelhantes aos documentos analógicos. No entanto, a autenticidade de documentos arquivísticos digitais é mais sensível e complexa em virtude da simplicidade com que podem ser alterados, bem como da dificuldade em detectar adulterações[9].

Diferentemente dos documentos analógicos, os digitais necessitam de procedimentos técnicos para garantir a preservação e o acesso contínuo, os quais paradoxalmente colocam em risco a autenticidade. Logo, deve-se implementar um conjunto de estratégias de preservação, devidamente orientadas pelas políticas organizacionais e atestadas pelo registro em metadados. O meio para contornar as complexidades e especificidades dos documentos arquivísticos digitais é envolver o acervo por meio de sistemas informatizados confiáveis, criando assim, uma cadeia de custódia e preservação ininterrupta.

Entretanto, por vezes, os mecanismos utilizados para monitorar os documentos arquivísticos digitais e garantir sua presunção da autenticidade não acompanham o ritmo da evolução tecnológica, limitando assim, as opções nessas ferramentas. Com isso, observa-se a urgência de implementar ou desenvolver um conjunto de ferramentas para minimizar as vulnerabilidades dos documentos arquivísticos. Do contrário, quaisquer adulterações serão imperceptíveis, quer dizer, sem que haja vestígios aparentes[10].

No ambiente digital, a presunção de autenticidade está condicionada aos sistemas informatizados que produzem, armazenam, preservam e disponibilizam acesso aos documentos. Para tanto, tais sistemas devem ser confiáveis, desenvolvidos a partir de padrões sedimentados na literatura científica. Sendo assim, os sistemas informatizados devem contemplar todo o ciclo de vida dos documentos arquivísticos, constituindo assim, uma abordagem holística em que a preservação é posta em prática desde o planejamento para produção de documentos.

Pode-se dizer que a autenticidade dos documentos arquivísticos dependerá dos métodos empregados para produção, tramitação, preservação e manutenção da cadeia de custódia. O conceito de autenticidade consiste em garantir que não houve alterações indevidas após a produção do documento, sendo este tão fidedigno quanto no momento de sua produção[8].

Sendo assim, a autenticidade depende de uma série de elementos atrelados à confiabilidade das plataformas de gestão e preservação, de modo que essas possam garantir a fixidez dos documentos arquivísticos. Igualmente, requer a custódia realizada por uma instituição responsável que possa garantir a manutenção de elementos que compõem a estrutura diplomática dos documentos, como, por exemplo, a autoria e a data[11].

A autenticidade dos documentos arquivísticos custodiados depende da confiabilidade dos sistemas informatizados que comportam o seu ciclo vital. Logo, surge a necessidade de implementar sistemas de gestão e preservação interoperáveis, para que, assim, não ocorram rupturas da cadeia de custódia. Tal interoperabilidade consiste em compatibilizar os padrões utilizados, de modo a reduzir o risco de inconsistências na comunicação entre os sistemas informatizados. Por consequência, isso evita a perda de metadados, bem como demais alterações não autorizadas sobre os documentos arquivísticos digitais.

PLATAFORMA DE GESTÃO DOCUMENTAL

No ambiente de gestão, composto por arquivo corrente e intermediário, ocorre a produção dos documentos arquivísticos, tendo em vista o cumprimento das funções e atividades organizacionais. Assim, o valor imediato dá significado inicial aos documentos arquivísticos e carrega um viés burocrático, advindo da moderna administração, que é dividido em atividades-meio e atividades-fim. Todas as organizações têm um propósito, entendido como atividade-fim, as demais atividades que auxiliam indiretamente para cumprir este propósito são atividades-meio.

Para a administração é pertinente otimizar o uso dos arquivos correntes. Assim, com a classificação e a ordenação adequadas pode-se melhorar o processo de busca e recuperação dos documentos e, consequentemente, aumentar a eficácia administrativa[12]. Nessa perspectiva, a gestão de documentos deverá contemplar atividades de produção, aquisição, classificação, avaliação, preservação, descrição e acesso. Tais ações devem ser pautadas na eficiência e visar o reuso da informação, de modo que este serviço seja pensado tanto para os administradores quanto para os usuários[13].

Com o advento das tecnologias da informação, os arquivos passam a contar com um acervo híbrido, de modo que a gestão se estende aos documentos arquivísticos digitais. No entanto, esses necessitam de um tratamento diferenciado, tendo em vista as suas complexidades e especificidades. Dessa forma, além de gerenciar os documentos digitais, os sistemas informatizados podem gerenciar os representantes digitais dos documentos analógicos, facilitando assim, a localização física e o acesso à informação.

A gestão dos documentos digitais tornou-se urgente para as organizações públicas e privadas, acelerando assim, o uso de ferramentas de gerenciamento, capazes de gerir, inclusive, os documentos analógicos. Pondera-se que não há diferença entre gerir documentos digitais e analógicos, porém, a problemática observada consiste na manutenção dos documentos arquivísticos digitais, pois estes dependem de um sistema de gestão adequado[14].

A corrida tecnológica fez as organizações implementarem diferentes sistemas informatizados em busca de obter vantagem competitiva, bem como atender as demandas de seus usuários/consumidores. No entanto, tais sistemas, em sua maioria, foram postos em prática sem a observância da gestão arquivística, comprometendo assim, questões como a autenticidade dos documentos.

Sendo assim, para orientar a implementação de sistemas de gestão, deve-se seguir o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil). Trata-se de um conjunto de requisitos necessários à organização produtora/recebedora dos documentos arquivísticos com o objetivo de assegurar a confiabilidade do sistema informatizado e, consequentemente, garantir o acesso. Ademais, o modelo e-Arq Brasil define os requisitos essenciais para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), de modo que sua implementação não depende de tecnológica específica[15]. No momento, o e-Arq Brasil encontra-se em sua versão datada de 2011, portanto, precisa ser atualizado para melhor refletir o estado da arte da preservação digital, sobretudo no que toca os repositórios arquivísticos digitais.

Observa-se que as ferramentas de Gestão Eletrônica de Documentos (GED) dificilmente atenderão todos os requisitos arquivísticos preconizados pelo e-Arq Brasil, que são indispensáveis para implementar um SIGAD[14]. Nesse sentido, o modelo e-Arq Brasil deve ser entendido como o requisito fundamental para implementar o sistema responsável pela gestão, doravante SIGAD.

Pode-se definir o SIGAD como um conjunto de procedimentos e técnicas para a gestão arquivística de documentos. É possível que consista em um *software* específico ou em um conjunto de *softwares* integrados. Ademais, o êxito do SIGAD está condicionado a uma política de gestão arquivística definida *a priori*[15]. É elementar que os sistemas informatizados sigam as políticas organizacionais, e nunca o contrário. Logo, o planejamento deve considerar as complexidades e especificidades dos tipos de documentos arquivísticos digitais que são produzidos.

Com os sistemas de gestão arquivística é possível capturar evidências das atividades organizacionais, proporcionando gerenciar o conteúdo e a estrutura dos documentos, manter sua relação orgânica e garantir o acesso contínuo[16]. Nessa perspectiva, o e-Arq Brasil destaca a importância de uma política de gestão documental previamente definida. Com isso, o organismo produtor poderá distribuir responsabilidades, definir procedimentos e elaborar instrumentos de gestão, como, por exemplo: o plano de classificação de documentos e a sua respectiva tabela de temporalidade e destinação[17].

Ao considerar tais aspectos, tem-se um conjunto de políticas organizacionais para gestão arquivística de documentos capaz de orientar a implementação de um SIGAD em conformidade com os requisitos preconizados pelo modelo e-Arq Brasil. Assim, o SIGAD será responsável pela aquisição, armazenamento, tramitação, avaliação e destinação dos documentos arquivísticos. Considerando que a tramitação depende do *workflow* a ser estabelecido, a avaliação deve seguir o plano de classificação, e a destinação deve manter conformidade com a tabela de temporalidade.

O controle de acesso é um dos métodos para garantir a idoneidade do SIGAD, especialmente no que tange às configurações do sistema informatizado e suas regras de *workflow*. Com isso, criam-se privilégios de acesso por meio de senhas diferenciando os usuários. Com relação ao *workflow*, é preciso integrar os procedimentos administrativos e os arquivísticos[8]. Dessa forma, cada usuário terá acesso somente ao que está devidamente autorizado e não poderá realizar ações que não correspondam às suas funções/atividades.

O ambiente de gestão documental requer infraestrutura adequada para que o SIGAD possa gerenciar os documentos de forma confiável, a fim de mantê-los autênticos. Tal confiabilidade se desenvolve ao sincronizar as políticas de gestão, a teoria Arquivística, os indivíduos e o SIGAD. Com isso, cria-se um ambiente confiável envolvido em uma cadeia de custódia ininterrupta que garante a produção, o armazenamento e a manutenção de documentos arquivísticos digitais, capazes de comprovar os fatos que atestam.

Observa-se que a gestão de documentos arquivísticos digitais depende dos sistemas informatizados, e a sua escolha não deve se fundamentar na opção por uma tecnologia mais recente ou de menor custo. Trata-se da escolha de sistemas adequados que possam gerenciar todo o ciclo de vida e, assim, manter sua fixidez, organicidade e autenticidade[18]. Dessa forma, a gestão de documentos de arquivo corrente e intermediário deverá ser mediada por um SIGAD, e este precisa interoperar com o repositório digital que será implementado no ambiente de preservação para que atue como um arquivo permanente digital.

Ressalta-se que, para preservar documentos arquivísticos autênticos, deve-se produzi-los com tal característica. Igualmente, é preciso manter uma cadeia de custódia confiável que se estenda da gestão até o momento em que os documentos gerenciados pelo SIGAD são transferidos/recolhidos ao repositório digital. Essa linha ininterrupta de confiança deve ser amparada por metadados que registrem quaisquer eventos pertinentes aos documentos arquivísticos digitais, como por exemplo, alteração da custódia e estratégias de migração de formato ou suporte. Destaca-se que a relação entre o SIGAD e o repositório digital é fundamental para assegurar a confiabilidade do sistema de arquivos e garantir que os documentos recolhidos permaneçam autênticos.

O registro em metadados permite obter o controle do ciclo de vida, visando a assegurar a autenticidade, facilitar o acesso e reunir informações pertinentes à preservação. Ademais, o registro por meio de trilhas de auditoria eleva a segurança do armazenamento e torna as ações transparentes. Isso faz do SIGAD um ambiente confiável capaz de capturar documentos arquivísticos, executar sua avaliação e apontar sua destinação (eliminação ou guarda permanente). Entretanto, a eliminação não será automática. Para documentos públicos, por exemplo, há necessidade de aprovação por parte da Comissão Permanente de Avaliação de Documentos (CPAD), conforme indica a legislação vigente[19].

Em linhas gerais, a plataforma de gestão é representada pelo SIGAD, responsável por capturar documentos arquivísticos e informações orgânicas produzidos por pessoas e sistemas de negócio da organização. A confiabilidade e os requisitos do SIGAD serão pautados no modelo e-Arq Brasil, de modo que será crucial manter estruturas de metadados que registrem os eventos pertinentes para presunção da autenticidade e preservação. Ademais, a manutenção de uma cadeia de custódia ininterrupta se faz necessária para que os documentos arquivísticos digitais gerenciados pelo SIGAD sejam transferidos de forma confiável ao repositório digital. Logo, destaca-se a pertinência de se implementar sistemas interoperáveis de gestão e preservação.

PLATAFORMA DE PRESERVAÇÃO E ACESSO

O ambiente de preservação é responsável por proteger a documentação e mediar o acesso. Ao considerar a problemática dos documentos arquivísticos digitais, surge a necessidade de adotar um conjunto de práticas para manter a autenticidade e garantir o acesso em longo prazo. Ressalta-se que, em ambiente digital, o conceito de autenticidade precisa ser revisto tendo em vista a necessidade de alterar os documentos para que possam ser preservados. Sendo assim, a autenticidade centra-se na capacidade de controlar e identificar tais alterações de modo que não comprometam o sentido dado originalmente ao documento arquivístico digital.

A autenticidade pode ser comprovada por meio da assinatura digital, que permite verificar questões como a origem e a integridade dos documentos arquivísticos, possibilitando assim, comprovar a autoria e

assegurar o 'não repúdio'. Logo, a assinatura digital é um componente elementar na busca pela presunção de autenticidade, de modo que soluções como o *blockchain* podem ser incorporadas pelo RDC-Arq para manter a fixidez dos documentos arquivísticos digitais.

Destaca-se que é possível atribuir assinatura digital por meio do *blockchain*, uma tecnologia de registro que utiliza a descentralização para elevar a segurança. O *blockchain* consiste em uma rede com blocos encadeados que sempre carregam um conteúdo junto a um identificador que garante a unicidade dos registros e os coloca em um índice global. Para alterar dados gravados em um determinado bloco, será necessário alterar todos os blocos subsequentes, fato que requer consenso da maioria da rede.

Preservar um documento arquivístico digital consiste em garantir sua integridade e o acesso contínuo em longo prazo, de modo que seja interpretado no futuro por meio de uma plataforma tecnológica diferente da que foi utilizada em sua produção, sem alterar a percepção dos consumidores/usuários[9]. Logo, a preservação digital deve ser estudada de forma interdisciplinar e no escopo organizacional, de modo que os profissionais da informação fiquem responsáveis por preservar a integridade e manter a autenticidade dos documentos arquivísticos digitais por meio de procedimentos que assegurem a sua fixidez[20].

As tecnologias da informação evoluem em ritmo desenfreado, em uma velocidade que os métodos de preservação não conseguem acompanhar. Consequentemente, surgem formatos de arquivo, versões de *softwares*, *hardware* e suportes nunca antes imaginados. Tais questões agravam a obsolescência tecnológica e igualmente geram uma diversidade descontrolada de tecnologias, quer dizer, documentos arquivísticos que foram produzidos por diferentes gerações de *softwares* e formatos. Nessa perspectiva, observa-se que os documentos arquivísticos digitais jamais sobreviverão na inércia, sendo essencial promover a intervenção por meio de políticas e métodos de preservação digital.

Um aspecto peculiar da preservação é a preocupação com o 'longo prazo', de modo que esse já não é representado por gerações ou séculos e pode significar apenas o tempo suficiente para se preocupar com os efeitos da obsolescência da tecnologia[21]. Contudo, a preservação digital já não poderá ser pensada como um conjunto de procedimentos isolados, mas sim, como parte de uma política organizacional, que considera todas as partes envolvidas no ciclo de vida dos documentos arquivísticos digitais[22].

Destaca-se a pertinência de definir as políticas de preservação antes da escolha dos sistemas informatizados e de quaisquer intervenções proferidas sobre os documentos arquivísticos digitais, incluindo questões como: a implementação de rotinas de *backup* para documentos e sistemas, bem como, os padrões que esses devem seguir; a análise dos custos envolvidos para montar a infraestrutura adequada tendo em vista elevar a confiabilidade e a segurança do ambiente; as técnicas de preservação que serão utilizadas; e a fonte de recursos que irá garantir a sustentabilidade da preservação digital no longo prazo[23].

Nessa perspectiva, o ambiente de preservação atua em sincronia com o ambiente de gestão documental, de modo a sugerir questões como, por exemplo, formatos de arquivo adequados para produção de documentos arquivísticos digitais. Ademais, o ambiente de preservação deve ser igualmente envolvido por uma cadeia de custódia ininterrupta, que irá agregar confiabilidade ao sistema de arquivos como um todo.

Em geral, os principais procedimentos de preservação digital podem ser agrupados em duas categorias: estratégias estruturais e estratégias operacionais. As estratégias estruturais consistem nos investimentos iniciais que a organização faz para preparar seu ambiente. Para tanto, definem-se questões como: adoção de padrões de *softwares* e formatos de arquivo, elaboração de padrões, escolha ou desenvolvimento de esquemas de metadados para preservação, construção da infraestrutura e formalização de consórcios. Já as estratégias operacionais são atividades essencialmente práticas de preservação digital, ou seja, ações aplicadas sobre os documentos arquivísticos digitais. Dentre tais estratégias, destacam-se: refrescamento, migração/conversão de formatos, emulação e encapsulamento[24,25].

As estratégias estruturais estão relacionadas às questões políticas e de infraestrutura, já as estratégias operacionais se referem às ações diretas no acervo. No caso dos documentos arquivísticos digitais, deve-se,

inicialmente, definir os elementos que precisam ser protegidos, para assim, mantê-los autênticos conforme estavam no ambiente de gestão.

Preservar documentos arquivísticos em ambiente digital requer a manutenção da autenticidade, de modo que sejam compreendidos pela comunidade designada e demais usuários. Portanto, a preservação digital tem o desafio de garantir o acesso contínuo no longo prazo, preservando os conteúdos e as propriedades significativas dos documentos[26].

Destaca-se que as propriedades significativas consistem em um conjunto de características que devem ser preservadas, para cada classe de documento arquivístico digital, por serem consideradas essenciais em sua concepção. Logo, podem incluir aspectos como: formatação, cores e interação. Além disso, são indispensáveis manter o vínculo arquivístico e adicionar informações referentes às sucessões de custódia, migrações, bem como, inserir informações descritivas que facilitem a localização dos documentos no repositório digital.

Repositórios arquivísticos digitais confiáveis

A preservação de documentos arquivísticos digitais necessita de políticas previamente definidas e de estratégias práticas para, assim, mitigar os efeitos da obsolescência tecnológica, contornar a fragilidade dos suportes e realizar a manutenção dos sistemas computacionais. No entanto, tais ações precisam ser executadas de forma controlada, para que, assim, seja possível presumir a autenticidade dos documentos arquivísticos no longo prazo. Impreterivelmente, devem-se implementar sistemas informatizados para controlar o ambiente de preservação e acesso. Assim, a preservação digital deixa de ser composta por procedimentos isolados e passa a ser gerenciada pelo repositório digital.

Além de serem um meio para disseminar a informação às comunidades designadas, os repositórios têm por fundamento garantir o acesso contínuo no longo prazo, o que reforça a ideia de proteção e preservação do material custodiado[27]. O repositório digital consiste em um ambiente tecnológico complexo no qual os documentos arquivísticos digitais serão armazenados e devidamente geridos. Trata-se de um sistema informatizado responsável por capturar, armazenar, preservar e disponibilizar o acesso à informação digital ao longo do tempo. Ademais, o repositório digital é formado por plataformas de *hardware* e *software*, serviços, e o acervo com seus respectivos metadados associados[17].

É nesse ambiente complexo do repositório em que serão executadas as estratégias de preservação, as quais serão devidamente registradas por meio de uma estrutura de metadados a fim de conferir um histórico de modificações dos documentos arquivísticos, corroborando com sua autenticidade. Com o uso de sistemas informatizados como o repositório, a preservação digital passa a ser pensada de maneira sistêmica, de modo que existam políticas e padrões a serem seguidos em busca da construção de um ambiente confiável.

Sendo assim, é fundamental implementar um Repositório Arquivístico Digital Confiável (RDC-Arq), sistema informatizado capaz de organizar e recuperar os documentos, além de manter sua organicidade. Com isso, sua organização hierárquica deve ser pautada no plano de classificação e, assim, possibilitar a descrição multinível conforme as normas internacionais para descrição arquivística[28].

Observa-se que a confiança se desenvolve em diversos níveis, de modo que ela será elevada quando: produtores enviam os documentos arquivísticos digitais que cumprem os requisitos definidos pelo RDC-Arq; consumidores recebem documentos autênticos após solicitá-los ao RDC-Arq (em caso de negação do acesso entrega-se uma justificativa); e o RDC-Arq demonstra que presta serviços adequados, isto é, com base em uma política de preservação que é disponibilizada aos interessados[29]. Além de garantir a preservação dos *bits*, é preciso despertar a confiança das comunidades designadas e demais consumidores, de que os serviços prestados garantem a confiabilidade do sistema informatizado, de modo que o acervo permanecerá disponível no longo prazo[30].

Desenvolver um RDC-Arq requer a sintonia entre produtores, preservadores e consumidores. Logo, é preciso que os produtores sigam boas práticas de preservação a fim de diminuir as ações futuras, executadas pelo preservador. Igualmente, o preservador deve atentar para as necessidades dos consumidores, e verificar se estes estão satisfeitos com os serviços prestados, bem como se consideram o RDC-Arq realmente confiável.

Inevitavelmente, os documentos arquivísticos digitais serão alterados ao longo do tempo, no entanto, é preciso saber quais características foram alteradas, por quem e quando, de modo que seja possível obter certo controle das alterações para assegurar a autenticidade[31]. A confiabilidade de um RDC-Arq deriva da capacidade de preservar, gerir e disponibilizar documentos arquivísticos digitais para acesso, de modo que seja possível presumir a sua autenticidade. Para tanto, a organização deve manter uma abordagem efetiva do gerenciamento de riscos em todo o ciclo de vida documental[32].

Logo, faz-se necessária uma abordagem holística da autenticidade nos ambientes de gestão e preservação, reforçando assim, a interoperabilidade entre o SIGAD e o RDC-Arq. Contudo, tais sistemas devem demonstrar-se confiáveis, e para isso, surge a necessidade de seguir padrões amplamente aceitos pela comunidade de preservação. Sendo assim, o SIGAD deve estar em conformidade com o modelo e-Arq Brasil, já para o RDC-Arq deverá seguir o modelo Open Archival Information System (OAIS).

O modelo OAIS tornou-se a norma International Organization for Standardization (ISO) 14721:2012, então traduzida para o Brasil pela Associação Brasileira de Normas Técnicas (ABNT), como Norma Brasileira Recomendada (NBR), sendo assim, ABNT/NBR 15472:2007, Sistema Aberto de Arquivamento de Informação (SAAI).

O modelo OAIS comporta uma série de funções para preservar documentos arquivísticos, incluindo: admissão de conteúdos, armazenamento arquivístico, gerenciamento de dados, acesso e disseminação. Dessa forma, apresenta um modelo lógico para representar documentos e suas informações relacionadas, além de abordar a migração dos documentos arquivísticos digitais para novos formatos e suportes[33-35].

O modelo OAIS comporta um conjunto de fluxos de informação necessários para preservar os documentos arquivísticos digitais custodiados. Assim, para facilitar o transporte de documentos entre o RDC-Arq e o ambiente externo, utilizam-se três tipos de pacotes de informação: o Pacote de Informação para Submissão (Submission Information Package – SIP); o Pacote de Informação para Arquivamento (Archival Information Package – AIP); e o Pacote de Informação para Disseminação (Dissemination Information Package – DIP).

Sendo assim, o RDC-Arq recebe documentos arquivísticos digitais enviados pelos produtores na forma de SIPs, e após aceitá-los, os SIPs são transformados em AIPs para que assim sejam armazenados e devidamente preservados no ambiente OAIS. Caso haja solicitações e pesquisas vindas da comunidade designada ou de outros consumidores, será disponibilizado um DIP com os documentos solicitados (exceto para documentos sigilosos).

Desse modo, o SIP deverá conter as informações administrativas relevantes para presunção da autenticidade; enquanto o AIP deve preservar o SIP e adicionar informações que corroborem com sua manutenção; já o DIP consiste em uma cópia dos materiais em formatos de fácil acesso aos consumidores, sem que se perca de vista as propriedades significativas dos documentos arquivísticos digitais. Portanto, deve-se demonstrar que o DIP disponibilizado é autêntico, seja por meio de uma declaração ou assinatura digital que ateste que o DIP corresponde ao AIP preservado; há casos em que poderá ser disponibilizada uma cópia dos metadados do AIP correspondente.

Ressalta-se que o RDC-Arq deve impedir o acesso direto ao ambiente de administração, assim irá proteger a autenticidade dos documentos arquivísticos digitais por meio de uma 'zona militarizada', de modo que somente a administração do OAIS terá acesso. Ao restringir o acesso externo, eleva-se a confiabilidade do sistema informatizado, pois se minimizam os riscos de invasões. Logo, para mediar o acesso à informação será preciso implementar uma plataforma de acesso, externa ao ambiente de preservação[10]. Ou seja, o acervo custodiado pelo RDC-Arq não deverá ficar *on-line*.

Com isso, surge a necessidade de uma plataforma de acesso para que os consumidores possam interagir com o RDC-Arq por meio de solicitações. O acesso aos documentos arquivísticos digitais pode ser mediado por ferramentas como o Access to Memory (AtoM), um aplicativo de código aberto desenvolvido para descrição arquivística e acesso. Destaca-se que o AtoM é fundamentado em padrões para descrição preconizados pelo International Council on Archives (ICA). Ademais, o AtoM é multilíngue, pode ser usado de forma gratuita e implementado em diferentes plataformas tecnológicas. Para os consumidores é pertinente que os documentos arquivísticos sigam a hierarquia multinível, refletindo o quadro de arranjo.

Os consumidores precisam analisar e reconhecer a confiabilidade do processo que envolve o ciclo de vida dos documentos arquivísticos digitais, bem como a autoridade e a capacidade do custodiador proteger o acervo. Igualmente, o custodiador precisa demonstrar tais características e, assim, assegurar que os documentos que preserva são autênticos[36]. Ou seja, o RDC-Arq deve divulgar à sua comunidade designada o conjunto de práticas que adota, observando os principais padrões aceitos pela comunidade de preservação digital.

Cabe ao RDC-Arq identificar, avaliar e mensurar os riscos que o circundam, para então definir e implementar meios para que possam ser mitigados. Os riscos envolvidos não se restringem à tecnologia, envolvendo assim, a infraestrutura organizacional e os colaboradores. Ademais, o RDC-Arq poderá se beneficiar da análise e gestão de riscos para minimizar suas vulnerabilidades, bem como, apoiar a administração como um todo[37].

Fica compreendido que além de ser confiável, o RDC-Arq deverá demonstrar tal confiança ao público. As ações para mitigar seus riscos de segurança podem ser tomadas também no âmbito organizacional. Logo, deve-se pensar o RDC-Arq como um ambiente complexo e de segurança robusta, envolvido em uma cadeia de custódia ininterrupta capaz de monitorar todas as ações proferidas sobre os documentos arquivísticos digitais.

Nessa perspectiva, a cadeia de custódia ininterrupta deve contemplar a relação interoperável entre o SIGAD e o RDC-Arq. Com isso, o recolhimento de documentos arquivísticos se dará por meio do envio de SIPs que serão monitorados para evitar manipulações não autorizadas, inserção ou retirada de documentos e metadados durante as atividades de normalização. Além disso, a interoperabilidade deve se estender aos padrões de metadados utilizados no SIGAD e no RDC-Arq, seguindo respectivamente, e-Arq Brasil e OAIS[10].

Cabe à administração do RDC-Arq definir as especificações técnicas que descrevem em detalhes os formatos dos documentos arquivísticos, de modo que sejam interoperáveis e abertos. Pode-se destacar o projeto *eArchiving*, pelo qual é possível empacotar documentos e metadados para submissão, preservação de longo prazo e reuso. Nessa perspectiva, é pertinente manter 'especificações comuns' para os SIPs, AIPs e DIPs, a fim de estabelecer um entendimento dos requisitos necessários à interoperabilidade[38].

Com isso, desenvolve-se uma base comum de definições e ferramentas dos pacotes de informação, fundamentada em padrões amplamente utilizados no âmbito internacional, alcançando a interoperabilidade. Consequentemente, tais especificações podem ser adotadas por outras organizações sem a necessidade de modificações. As especificações técnicas elaboradas pelo *eArchiving* preconizam uma estrutura comum para SIPs, AIPs e DIPs, detalhando a localização de documentos, metadados e demais componentes do pacote[38]. Tais questões são compatíveis com o caráter abstrato do OAIS, de modo que facilitam o processo de recolhimento e corroboram com a confiabilidade do sistema informatizado como um todo.

O modelo OAIS não faz menções diretas à Arquivística, contudo, demonstra-se capaz de manter conformidade com pressupostos elementares como, por exemplo: princípio da proveniência, organicidade e autenticidade. Com isso, é possível preencher lacunas teóricas criadas pelos documentos digitais, visto que suas complexidades extrapolam os referenciais orientados aos documentos analógicos[39]. A longevidade do modelo OAIS reside em manter sua capacidade de ser flexível, amplo e abstrato. Tais características foram

fundamentais para a sua afirmação enquanto principal modelo de referência. Igualmente, a necessidade de implementar o OAIS resultou no desenvolvimento de outros padrões que reafirmam sua pertinência[40].

O modelo OAIS é amplo suficiente para ser implementado por arquivos, bibliotecas, centros de documentação, museus e outros que tenham a intenção de preservar documentos e informações no longo prazo. É compatível com as esferas pública e privada. Além disso, possui flexibilidade para ser implementado em repositórios institucionais ou temáticos. Logo, percebe-se que não há um pacote pré-definido de ferramentas ou plataformas específicas a seguir, o que proporciona liberdade para a organização buscar a solução que se mostre mais adequada ao contexto do seu acervo.

Com o modelo OAIS pode-se definir a tramitação e os modelos adequados aos documentos arquivísticos, tendo em vista a preservação em longo prazo, e criar, assim, um RDC-Arq. No entanto, a sua confiabilidade precisa ser verificada a fim de comprovar que o modelo está sendo seguido. Para sanar tal questão, surgiram padrões que abordam a auditoria do ambiente OAIS.

Auditoria

O processo de auditoria consiste em uma sistemática (conjunto de critérios) que é executada de forma independente para se obter evidências objetivas, a fim de sustentar a existência ou veracidade de um fato[41]. Auditoria se relaciona com controle, sendo necessária para identificar funções e atividades realizadas no ambiente organizacional, em um determinado período, com objetivo de verificar a conformidade com comportamentos adequados à organização[39,42]. Essencialmente, a necessidade de auditar surgiu em virtude do aumento da burocracia e da complexidade das organizações e busca verificar a conformidade das ações com os resultados obtidos.

Encontra-se na literatura, o termo 'auditoria de informação', que se concentra no estudo do ciclo de vida das informações com ênfase em aspectos como: produção, tramitação e uso da informação. Ademais, considera os custos envolvidos e o valor que determinadas informações agregam para uma organização. A auditoria de informação permite avaliar a qualidade dos serviços, além de contribuir para o planejamento estratégico organizacional[43].

Igualmente, há o termo 'auditoria arquivística', que consiste na análise dos procedimentos empregados no ciclo de vida dos documentos arquivísticos, assim, considera a legislação vigente e as teorias consolidadas da disciplina Arquivística. A auditoria arquivística visa monitorar as ações, fazer análises críticas e sugestões[42].

Percebe-se que o termo auditoria foi apropriado e devidamente adaptado para as abordagens informacional e arquivística. Assim, a auditoria passa a ser o processo de verificação dos fluxos da informação orgânica a fim de comprovar o uso de boas práticas no ciclo de vida dos documentos. Deste modo, podem-se auditar os sistemas informatizados para comprovar a sua conformidade com a teoria arquivística ou padrões específicos. A relação entre auditoria da informação e auditoria arquivística permite estabelecer métodos para mensurar a confiabilidade dos sistemas informatizados e presumir a autenticidade dos documentos arquivísticos digitais custodiados.

A auditoria permite verificar se os sistemas informatizados atendem aos interesses de sua comunidade designada, bem como, se os objetivos organizacionais estão sendo atingidos. Dessa forma, oferece indicadores que auxiliam no processo de adequação dos serviços para elevar a qualidade. Isso permite avaliar o sistema como um todo, contemplando os recursos utilizados e o estado de seus componentes, de modo que seja possível buscar soluções para os problemas observados[32].

Com relação ao RDC-Arq, observa-se que existem propostas de critérios para auditoria, a fim de comprovar sua confiabilidade. Dentre estas propostas destacam-se: Trustworthy Repository Audit & Certification: Criteria and Checklist (TRAC), Catalogue of Criteria for Trusted Digital Repositories da Network of Expertise in long-term STORage (NESTOR), Digital Repository Audit Method Based on Risk Assessment

(DRAMBORA) e Audit and Certification of Trustworthy Digital Repositories (ACTDR). Cada um desses conjuntos de critérios utiliza uma metodologia própria para avaliar a confiabilidade do repositório, de modo que possuem suas similaridades e diferenças.

O DRAMBORA possui limitação por se tratar de uma ferramenta para auditoria interna. Já o NESTOR mostra-se incipiente por não possuir reconhecimento da ISO. Observa-se que o TRAC teve sua última versão publicada em 2007, posteriormente, esse estudo foi continuado no âmbito do Consultative Committee for Space Data Systems (CCSDS), transformando-se no ACTDR. Cabe ressaltar que o ACTDR se firma com principal padrão para auditoria externa, tornando-se a ISO 16363:2012. Portanto, o modelo OAIS deve ser a referência para implementar um RDC-Arq, que, posteriormente, deverá ser auditado periodicamente por meio do padrão ISO 16363:2012 para atestar a confiabilidade do ambiente de preservação. Igualmente, um RDC-Arq precisa considerar os pressupostos elementares da disciplina Arquivística[39].

O objetivo da auditoria consiste em desenvolver um processo de melhoria contínua, no qual o resultado de uma auditoria não deve seguir uma lógica binária de sim ou não. O que se pretende é obter uma análise que aponte que áreas precisam ser melhoradas[44,45]. Sendo assim, além de manter conformidade com o OAIS e com os critérios de confiabilidade do ISO 16363:2012, o RDC-Arq precisa gerenciar documentos e metadados conforme os princípios e as práticas da Arquivística. Para tanto, deve-se preservar características do documento arquivístico, como, por exemplo, a autenticidade e a organicidade, além de fornecer instrumentos de pesquisa multinível aos consumidores[46].

Observa-se que a teoria da preservação digital vem sendo sistematizada, logo, têm-se ambientes definidos para gestão e preservação, bem como, os padrões a serem seguidos. De tal modo, a implementação de um RDC-Arq requer a conformidade com o modelo OAIS, e a sua confiabilidade fica condicionada aos resultados da auditoria externa realizada com o ISO 16363:2012. Tais apontamentos direcionam a preservação digital para uma abordagem sistêmica, que se fortalece, cada vez mais, na medida em que novos estudos surgem.

O padrão ISO 16363:2012 oferece uma série de critérios para a infraestrutura organizacional de um RDC-Arq, dos quais se destaca a necessidade de um planejamento estratégico para tomada de decisões tendo em vista a continuidade dos serviços de preservação. Para tanto, a administração do RDC-Arq precisa desenvolver planos de contingência para mitigar os riscos identificados. Entretanto, nos casos em que a organização não consiga minimizar os riscos ou mesmo encerre/interrompa suas atividades, deve-se ter um plano de sucessão para realizar a alteração da cadeia de custódia e, assim, garantir que os documentos armazenados sejam transferidos adequadamente. Logo, uma política de preservação deve considerar elementos da gestão de riscos, para desenvolver planos de contingência e de sucessão[47].

Nessa perspectiva, o RDC-Arq deve ser projetado em consonância com padrões amplamente aceitos para garantir a segurança dos materiais custodiados. A confiabilidade do RDC-Arq deve considerar o cumprimento de suas responsabilidades no longo prazo, bem como a presença de políticas que sejam mensuradas durante o processo de auditoria[11]. No entanto, atingir a confiança esperada pelo ISO 16363:2012 não é uma meta que possa ser esquecida após ser alcançada inicialmente. Assim, para manter a confiabilidade, é preciso realizar um ciclo regular de auditoria e certificação[44,45,48].

Ao considerar os apontamentos das auditorias, o repositório terá uma contínua evolução tecnológica, de modo que irá, sistematicamente, mitigar vulnerabilidades em sua infraestrutura técnica[49]. Desta forma, um RDC-Arq em conformidade com o OAIS deve ser auditado periodicamente por meio do ISO 16363:2012, visto que a confiança deriva da sequência de resultados positivos obtidos na avaliação. Portanto, a confiabilidade é uma construção fundamentada em um processo de melhoria contínua, que visa a aspectos relacionados à infraestrutura organizacional, ao gerenciamento de materiais digitais, e à infraestrutura de segurança e gestão de riscos.

Com as auditorias periódicas, o RDC-Arq poderá se firmar como 'confiável', adquirindo esse *status* diante da comunidade de preservação e de sua comunidade designada. Ademais, após obter êxito por meio

da auditoria, deve-se proceder a certificação, a fim de formalizar a confiabilidade. Contudo, as ações de auditoria e certificação devem ser contínuas, pois seus resultados não são definitivos[47]. Destaca-se que a iniciativa de comunicar os resultados da auditoria e da certificação eleva a confiança do público, que passa a compreender a evolução da segurança do RDC-Arq[48].

Observa-se a relação da auditoria com o plano organizacional, informacional, arquivístico e nos repositórios digitais. Os conceitos são convergentes e promovem a sinergia em sua abordagem, pois, ao auditar um RDC-Arq por meio do ISO 16363:2012, serão avaliadas questões de infraestrutura organizacional e o fluxo documental; igualmente, deve-se seguir princípios arquivísticos, configurando assim, uma visão holística, que além de considerar o ciclo de vida dos documentos arquivísticos, se estende ao âmbito organizacional. Ademais, pode-se reforçar a abordagem sistêmica, tendo em vista o uso de padrões como o OAIS e o ISO 16363:2012, bem como a necessidade de uma relação interoperável entre os ambientes de gestão e preservação.

Dessa forma, é reforçada a visão da preservação digital como um processo que precisa de constante atualização a fim de se adaptar às mudanças em seu contexto. Suas ações devem manter consonância com as demais políticas organizacionais, e atentar para questões como o planejamento, os recursos humanos e o financiamento. Ao estabelecer uma política organizacional que considere a preservação e o acesso, podem-se antecipar os efeitos da obsolescência tecnológica, e assim, buscar alternativas para preservar e garantir o acesso às informações digitais[50]. Sendo assim, destaca-se que cultura organizacional e preservação digital caminham lado a lado, de modo que as políticas de salvaguarda não devem se limitar ao acervo, precisam ser expandidas para todos os setores da organização.

CONSIDERAÇÕES FINAIS

Este estudo partiu de uma abordagem holístico-sistêmica da preservação de documentos arquivísticos digitais. Para tanto, foram perpassadas questões como a necessidade de uma cadeia de custódia ininterrupta e de sistemas informatizados que comportem os ambientes de gestão e preservação.

Reafirma-se uma relação de interdependência entre as cadeias de preservação e de custódia documental, motivada pelas complexidades e especificidades adquiridas pelos documentos arquivísticos em ambiente digital. Com isso, surge a necessidade de manter uma linha idônea que incorpore o ciclo de vida documental, de modo que as ações de custodiar e preservar tenham sempre as mesmas prioridades.

A confiabilidade começa com a implementação de procedimentos adequados na gestão de documentos, logo, é fundamental implementar um SIGAD em conformidade com o modelo e-Arq Brasil. Tais requisitos devem ser definidos em uma política organizacional que vislumbre a manutenção da autenticidade dos documentos arquivísticos digitais, bem como o seu reuso no longo prazo. Ademais, o SIGAD fica responsável pelos arquivos corrente e intermediário, isso comporta a captura dos documentos, a tramitação, avaliação e destinação. Logo, deve ser tanto capaz de eliminar documentos por meio de métodos seguros, quanto de promover o seu recolhimento para guarda permanente junto ao RDC-Arq.

O ambiente de preservação tem por finalidade preservar documentos arquivísticos e garantir acesso contínuo em longo prazo. Para tanto, deve-se implementar um RDC-Arq em conformidade com o modelo OAIS. Destaca-se a importância de manter níveis de interoperabilidade com o ambiente de gestão, de modo que o SIGAD enviará os documentos por meio de SIPs ao RDC-Arq, consequentemente, alterando a custódia. Ao receber o acervo, o RDC-Arq deve verificar a sua presunção de autenticidade e registrar a transferência da custódia por meio de metadados. Além de preservar documentos arquivísticos digitais, deve promover o acesso por meio de DIPs que serão disponibilizados para a comunidade designada, contendo documentos em formatos de fácil interpretação ao público geral.

Para que um RDC-Arq se firme como confiável, é preciso submetê-lo à auditoria por meio do padrão ISO 16363:2012, sendo realizada por terceiros. Dessa forma, pode-se verificar a conformidade do RDC-Arq com o modelo OAIS e mensurar os níveis de confiança com relação à infraestrutura organizacional, gestão de documentos digitais, infraestrutura de segurança e gestão de riscos. Ademais, o processo pode se estender, de modo a realizar uma auditoria arquivística a fim de comprovar que o SIGAD e o RDC-Arq seguem os fundamentos da disciplina Arquivística.

Ressalta-se que durante este estudo observou-se que a preservação deve ser pensada em todas as fases do ciclo de vida dos documentos. Tal ideia é reforçada pela interdependência entre cadeia de custódia, ambiente de gestão, ambiente de preservação e auditoria. Trata-se da necessidade de uma abordagem holística, capaz de implementar ações que contribuem com o sistema de arquivos como um todo. Há níveis de interoperabilidade a serem mantidos entre os sistemas informatizados a fim elevar a confiabilidade, especialmente no momento da alteração da custódia, que pode ser representada pelo recolhimento do acervo junto ao RDC-Arq. Os requisitos preconizados pelo SIGAD e pelo RDC-Arq precisam ser compatíveis, portanto, observa-se a inviabilidade de se pensar o ciclo vital de forma fragmentada.

A abordagem holística desperta a visão sistêmica da preservação digital, visto que SIGAD e RDC-Arq devem manter conformidade com padrões amplamente aceitos na literatura, com a legislação vigente e com os fundamentos da Arquivística. Essa visão sistêmica reflete o quanto a preservação digital tem evoluído, de modo que novos estudos são realizados e se incorporam aos existentes, formando assim, um arcabouço teórico cada vez mais sólido, que se fortalece quando aliado à visão macro do sistema de arquivos. Destaca-se que os documentos arquivísticos digitais são indispensáveis para quaisquer organizações contemporâneas, logo, a preservação digital deve começar no planejamento estratégico e estar enraizada na cultura organizacional.

Por fim, este estudo contribui para reafirmar a necessidade de uma abordagem holístico-sistêmica que contemple todo o ciclo de vida dos documentos arquivísticos digitais. Com isso, estima-se que a preservação digital será mais efetiva quando partir de uma política embasada em padrões pertinentes à literatura científica e em consonância com a legislação vigente. Ademais, observa-se uma preservação digital amadurecida, muito em virtude de modelos como o OAIS e o ISO 16363:2012, e igualmente fortalecida pela vasta bibliografia disponível que preenche antigas lacunas e gera novos questionamentos.

REFERÊNCIAS

1. Gil AC. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas; 2010.
2. Luna SV. Planejamento de pesquisa: uma introdução. São Paulo: Educ; 1997.
3. Silva EL, Menezes EM. Metodologia da pesquisa e elaboração de dissertação [Internet]. 4. ed. Florianópolis: UFSC; 2005 [acesso em 2020 jul. 16]. Disponível em: https://bit.ly/2CKHXuY.
4. Volpato GL, Barreto RE, Ueno HM, Volpato EDSN, Giaquinto PC, Freitas EGD. Dicionário crítico para redação científica. Botucatu: Best Writing; 2013.
5. Cordeiro AM, Oliveira GM, Rentería JM, Guimarães CA. Revisão sistemática: uma revisão narrativa. Rev Col Bras Cir [Internet]. 2007 dez. [citado em 2020 abr. 14];34(6):428-31. Disponível em: https://doi.org/10.1590/S0100-69912007000600012.
6. Santos VB. Preservação de documentos arquivísticos digitais. Ci Inf [Internet]. 2012 abr. [citado em 2020 abr. 14];41(1):114-26. Disponível em: http://revista.ibict.br/ciinf/article/view/1357.
7. Diretrizes do preservador: a preservação de documentos arquivísticos digitais: diretrizes para organizações [Internet]. Arquivo Nacional, Câmara dos Deputados, tradutores e revisores. Vancouver: Universidade da Colúmbia Britânica; 2007 [acesso em 2020 jul. 16]. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf.
8. Rondinelli RC. Gerenciamento arquivístico de documentos eletrônicos: uma abordagem teórica da diplomática arquivística contemporânea. 4. ed. Rio de Janeiro: FGV; 2005.

9. Ferreira M. Introdução à preservação digital: conceitos, estratégias e actuais consensos [Internet]. Portugal: Escola de Engenharia da Universidade do Minho; 2006 [acesso em 2020 jul. 16]. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf.

10. Flores D, Rocco BCB, Santos HM. Cadeia de custódia para documentos arquivísticos digitais. Acervo [Internet]. 2016 dez. [citado em 2020 abr. 14];29(2):117-32. Disponível em: http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717.

11. Luz CS, Flores D. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos [Internet]. In: Maringelli ICAS, organizadora. Anais do 4º Seminário Serviços de Informação em Museus: informação digital como patrimônio cultural; 2016 nov. 8-9; Sesc Bom Retiro, Brasil. São Paulo: Pinacoteca de São Paulo; 2017 [acesso em 2020 jul. 16]. p. 171-81. Disponível em: https://bit.ly/2OtOSLD.

12. Rousseau JY, Couture C. Os fundamentos da disciplina arquivística. Lisboa: Publicações Dom Quixote; 1998.

13. Heredia Herrera A. El debate sobre la gestión documental. Mét Inf [Internet]. 1998 marzo [citado en 2020 abr. 14];5(22):30-6. Disponible: https://core.ac.uk/download/pdf/11877283.pdf.

14. Rocha C, Ramos MHC, Silva M, Rondinelli RC. Gestão arquivísticas de documentos eletrônicos [Internet]. Gouget AG, revisora. Rio de Janeiro: Conselho Nacional de Arquivos, Câmara Técnica de Documentos Eletrônicos; 2004 [acesso em 2020 jul. 16]. Disponível em: https://bit.ly/2OxM8N6.

15. Conselho Nacional de Arquivos (BR). e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos [Internet]. Rio de Janeiro: O Conselho; 2011 [acesso em 2020 jul. 16]. Disponível em: https://bit.ly/32rvYNl.

16. Castro AM, Castro DM, Gasparian DMC. Arquivos: físicos e digitais. Brasília: Thesaurus; 2007.

17. Rocha CL. Repositórios para a preservação de documentos arquivísticos digitais. Acervo [Internet]. 2015 dez. [citado em 2020 abr. 14];28(2):180-91. Disponível em: http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/608/669.

18. Silva M. O arquivo e o lugar: custódia arquivística e a responsabilidade pela proteção aos arquivos. Niterói: Eduff; 2017.

19. Luz CS. A interoperabilidade na preservação da informação arquivística: os metadados e a descrição. Inf Arq [Internet]. 2016 jun. [citado em 2020 abr. 14];5(1):27-48. Disponível em: http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/139.

20. Innarelli HC. Preservação digital e seus dez mandamentos. In: Santos VB, organizador. Arquivística: temas contemporâneos: classificação, preservação digital, gestão do conhecimento. 3. ed. Brasília: Senac; 2009, p. 21-75.

21. Hedstrom M. The digital preservation research agenda [Internet]. Proceedings of The State of Digital Preservation: an International Perspective; 2002 April 24-25; Institutes for Information Science, United States. Arlington: Council on Library and Information Resources; 2002 [cited 2020 July 16]. p.32-7. Available from: https://bit.ly/3eBWxlJ.

22. Márdero Arellano MÁ, Andrade RS. Preservação digital e os profissionais da informação. DataGramaZero [Internet]. 2006 out. [citado em 2020 abr. 14];7(5):1-11. Disponível em: https://ridi.ibict.br/bitstream/123456789/259/1/MIGUELDgz2006.pdf.

23. Santos HM, Flores D. Políticas de preservação digital para documentos arquivísticos. Perspect Ci Inf [Internet]. 2015 Dez [citado 2020 mai 06];20(4):197-217. Disponível em: http://dx.doi.org/10.1590/1981-5344/2542.

24. Márdero Arellano MÁ. Preservação de documentos digitais. Ci Inf [Internet]. 2004 ago. [citado 2020 abr. 14];33(2):15-27. Disponível em: http://revista.ibict.br/ciinf/article/view/1043.

25. Thomaz KP, Soares AJ. A preservação digital e o modelo de referência Open Archival Information System (OAIS). DataGramaZero [Internet]. 2004 fev. [citado em 2020 abr. 14];5(1):1-17. Disponível em: http://www.brapci.inf.br/index.php/res/download/45229.

26. Conselho Nacional de Arquivos (BR). Carta para a preservação do patrimônio arquivístico digital [Internet]. Rio de Janeiro: O Conselho; 2004. Disponível em: http://conarq.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf.

27. Silva Junior LP, Borges MM. Preservação digital no repositório científico de acesso aberto de Portugal. Rev Eletron Comun Inf Inov Saúde [Internet]. 2014 dez. [citado em 2020 abr. 14];8(4):567-74. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/441.

28. Conselho Nacional de Arquivos (BR). Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis: RDC-Arq [Internet]. Rio de Janeiro: O Conselho; 2015 [acesso em 2020 jul. 16]. Disponível em: https://bit.ly/2B5Yglo.

29. Thomaz KP. Repositórios digitais confiáveis e certificação. Arquivística.net [Internet]. 2007 jun. [citado em 2020 abr. 14];3(1):80-89. Disponível em: https://bit.ly/30fQRIY.

30. Smith A. Digital preservation research and developments. Russ Dig Libraries J [Internet]. 2000 June [cited 2020 Apr 14];3(3):1-6. Available from: https://elbib.ru/ru/article/77.

31. Barbedo F. Arquivos digitais: da origem à maturidade. Cad BAD [Internet]. 2016 dez. [citado em 2020 abr. 14];1(2):6-18. Disponível em: https://bit.ly/3h4UBDM.

32. Ravelo Díaz G, Mena Mugica MM, Del Castillo Guevara J. Requisitos para la valoración de riesgos de preservación en repositorios digitales. Biblios [Internet]. 2019 jul. [citado en 2020 abr. 14];75(2):25-34. Disponible: https://doi.org/10.5195/biblios.2019.484.

33. Associação Brasileira de Normas Técnicas. Sistemas espaciais de dados e informações: modelo de referência para um sistema aberto de arquivamento de informação. Rio de Janeiro: A Associação; 2007. NBR 15472/2007.

34. Consultative Committee for Space Data System. Reference Model for an Open Archival Information System (OAIS): recommendation for space data system practices. Recommended practice: CCSDS 650.0-M-2 [Internet]. Magenta Book. Washington: The Committee; 2012 [cited 2020 July 16]. Available from: http://public.ccsds.org/publications/archive/650x0m2.pdf.

35. International Organization for Standardization. Space data and information transfer systems: Open archival information system: reference model. Genebra: The Organization; 2012. ISO 14721/2012.

36. Voutssás Márquez J. La cadena de preservación en archivos digitales. In: Barnard AA., organizadora. Archivos electrónicos: textos y contextos. México: Red Nacional de Archivos de Educación Superior y Archivo Histórico de la Universidad Nacional Autónoma de Puebla; 2010. p. 143-67.

37. Digital Curation Centre; Digital Preservation Europe. Digital repository audit method based on risk assessment. Edinburgh: The Centre; 2007 [cited 2020 July 16]. Available from: http://www.repositoryaudit.eu/download.

38. eArchiving Services: technical specifications [Internet]. [place unknown]: CEF Digital Connecting Europe; 2020 [cited 2020 July 16]. Available from: https://bit.ly/3eDN11j.

39. Santos HM. Auditoria de repositórios arquivísticos digitais confiáveis. Inf Pauta [Internet]. 2019 dez [citado em 2020 abr. 14];4(2):156-72. Disponível em: https://bit.ly/32o4WGQ.

40. Cruz Mundet JR, Díez-Carrera C. Sistema de Información de Archivo Abierto (OAIS): luces y sombras de um modelo de referencia. Investig Bibliotecol [Internet]. 2016 dic. [citado en 2020 abr 14];30(70):221-47. Disponible: http://dx.doi.org/10.1016/j.ibbai.2016.10.010.

41. Associação Brasileira de Normas Técnicas. Diretrizes para auditoria de sistemas de gestão. Rio de Janeiro: A Associação; 2018. NBR ISO 19011/2018

42. Batista DA, Oliveira EB. Auditoria arquivística: uma proposta de requisitos. Inf Soc [Internet]. 2019 mar [citado em 2020 abr. 14];29(1):159-80. Disponível em: https://bit.ly/2Wt8Ev1.

43. Pestana O. Auditoria de informação: definição e evolução da atividade no contexto da gestão da informação e das organizações. Pág A&B [Internet]. 2014 dez. [citado em 2020 abr. 14];3(2):49-64. Disponível em: http://ojs.letras.up.pt/index.php/paginasaeb/article/view/599/579.

44. Consultative Committee for Space Data System. Audit and certification of trustworthy digital repositories: recommendation for space data system practices. Recommended practice: CCSDS 652.0-M-1. Magenta Book. Washington: The Committee; 2011 [cited 2020 July 16]. Available from: https://public.ccsds.org/pubs/652x0m1.pdf.

45. International Organization for Standardization. Space data and information transfer systems: Audit and certification of trustworthy digital. Geneva: The Organization; 2013. ISO 16363/2012.

46. Conselho Nacional de Arquivos (BR). Cenários de uso de RDC-Arq em conjunto com o SIGAD [Internet]. Rio de Janeiro: O Conselho; 2015 [acesso em 2020 jul. 16]. Disponível em: https://bit.ly/391rjmM.

47. Santos HM, Flores D. Infraestrutura organizacional necessária ao repositório arquivístico digital confiável: um diálogo com a ISO 16363. Rev Bras Biblio Doc [Internet]. 2020 jan [citado em 2020 abr 14];16(1):1-29. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/1305.

48. Trustworthy repositories audit and certification [Internet]. Chicago: The Center for Research Libraries, Online Computer Library Center; 2007 [cited 2020 July 16]. Available from: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf.

49. Rezende LVR, Cruz-Riascos AS, Hott DFM. Em busca de repositórios digitais confiáveis no Brasil: análise da infraestrutura organizacional conforme a norma ISO 16363/2012. Rev Eletron Comun Inf Inov Saúde [Internet]. 2017 nov. [citado em 2020 abr. 14];11:1-12. Disponível em: http://dx.doi.org/10.29397/reciis.v11i0.1390.

50. Márdero Arellano MÁ, Tavares MFD. Preservação digital, gestão de dados de pesquisa e biodiversidade. Cad BAD [Internet]. 2018 out. [citado em 2020 abr. 14];1(1):180-89. Disponível em: https://www.bad.pt/publicacoes/index.php/cadernos/article/view/1930.