Preservação sistêmica de documentos arquivísticos digitais: uma perspectiva holística

Systemic preservation of digital archival records: a holistic perspective

Santos, Henrique Machado dos; Mazuco, Fabiana Ciocheta; Flores, Daniel

Henrique Machado dos Santos
henrique.hms.br@gmail.com
Universidade Federal de Santa Maria, Brasil
Universidade Federal do Rio Grande, Brasil
Fabiana Ciocheta Mazuco
fabianamazuco@gmail.com
Universidade Federal de Santa Maria, Brasil
Arquivo Público Municipal de São Francisco de Assis-RS, Brasil
Daniel Flores
dfloresbr@gmail.com
Universidad de Salamanca , España
Universidade Federal Fluminens, Brasil

Percursos
Universidade do Estado de Santa Catarina, Brasil
ISSN-e: 1984-7246
Periodicidade: Cuatrimestral
vol. 21, núm. 46, 2020
revistapercursos.faed@udesc.br

Recepção: 07 Abril 2020
Aprovação: 17 Setembro 2020

URL: http://portal.amelica.org/ameli/journal/815/8154526012/

DOI: https://doi.org/10.5965/1984724621462020244

Resumo: A preservação de documentos digitais tem sido um tema de constante discussão na literatura científica. Consequentemente, diversas estratégias e métodos vêm sendo empregados a fim de garantir o acesso em longo prazo. No âmbito da Arquivística tem-se discutido sobre os sistemas informatizados responsáveis por gerenciar e preservar tais documentos. Igualmente, a reformulação de conceitos como as cadeias de custódia e de preservação trazem novos questionamentos. Dessa forma, tem-se por objetivo discutir a abordagem sistêmica da preservação digital, pautada em normas e padrões amplamente aceitos, aliados à visão holística do ciclo de vida dos documentos arquivísticos, para, assim, planejar a preservação já na fase da gestão de documentos. Para apoiar o ponto de vista apresentado neste artigo, utiliza-se um levantamento bibliográfico composto por livros, publicações técnicas, leis e artigos científicos. Observa-se que os ambientes de gestão e preservação devem manter níveis de interoperabilidade para adicionar confiança às transferências e recolhimentos. Com isso, mantém-se uma cadeia de custódia ininterrupta, que irá assegurar a autenticidade dos documentos arquivísticos. Sendo assim, entende-se que a abordagem holístico-sistêmica permite compreender a visão macro do sistema de arquivos, e assim, identificar a legislação, as normas e os padrões envolvidos.

Palavras-chave: Preservação sistêmica, Documentos digitais, Arquivística, Cadeia de custódia, Cadeia de preservação, Confiabilidade.

Abstract: The preservation of digital documents has been a topic of constant discussion in the scientific literature. Consequently, several strategies and methods have been employed to guarantee long-term access. In the scope of Archivistics, computerized systems responsible for managing and preserving such documents have been discussed. Likewise, the reformulation of concepts such as chains of custody and preservation raises new questions. Thus, the objective is to discuss the systemic approach to digital preservation based on widely-accepted norms and standards, combined with the holistic view of the life cycle of archival documents, to plan the preservation already in the document management phase. To support this article's point of view, a bibliographic survey composed of books, technical publications, laws, and

scientific articles are used. It is observed that the management and preservation environments must maintain levels of interoperability to add confidence to transfers and collections. Thus, an uninterrupted chain of custody is maintained, which will ensure the authenticity of archival documents. Thus, it is understood that the holistic-systemic approach allows understanding the macro view of the file system and, thus, identifying the legislation, norms, and standards involved.

Keywords: Systemic preservation, Digital records, Archival science, Chain of custody, Chain of preservation, Reliability.

Introdução

Com o início do século XXI, observa-se que as organizações, governos e indivíduos estão cada vez mais dependentes dos documentos arquivísticos digitais (BRASIL, 2004a). As ferramentas de tecnologias da informação simplificaram a produção e a disseminação de documentos digitais[1] por meio das modernas redes de comunicação (FERREIRA, 2006). A informação digital transformou os custos de produção, de modo que, quando as quantidades de produtos aumentam, os custos sofrem pouca variação. A economia da informação digital extingue os tradicionais custos fixos[2] de produção (BARRETO, 2009).

Uma parcela significativa das informações produzidas no mundo tem sua origem no ambiente digital, de modo a representar textos, imagens, áudios, vídeos e bancos de dados. Paralelamente, *hardware, software* e suporte são, constantemente, substituídos por novas gerações tecnológicas, criando assim, ciclos de obsolescência que geram incompatibilidades (THOMAZ, 2006).

Além disso, há um crescente risco de perda de informações em virtude das dificuldades na gestão e na preservação, sobretudo de documentos arquivísticos (GUEDES, 2012). Tal risco é catalisado pelos acelerados ciclos de obsolescência tecnológica que agravam o desafio da preservação digital. Essa constante evolução das tecnologias da informação tende a ocorrer de forma cada vez mais acelerada e dificultar as ações de preservação digital (GRANGER, 2000). Logo, a obsolescência tecnológica aliada à falta de políticas de gestão e preservação de documentos digitais eleva o risco da perda de informações. Tais impactos podem ser minimizados por meio de padrões recomendados para gestão e preservação, além de considerar a legislação arquivística.

É inegável que os documentos digitais trazem novos horizontes de atuação à Arquivística/Arquivologia; no entanto, surgem desafios, riscos e incertezas que passam a rodear os acervos. O modesto domínio que o arquivista tem sobre as tecnologias, reforça a necessidade de pesquisas em torno da preservação, acesso e manutenção da autenticidade. Sua formação profissional evoluiu tanto quanto as novas tecnologias, no entanto, há profissionais que carecem de atualização sobre o tema.

A informação digital é vulnerável por natureza, de modo que está sujeita a intervenções não autorizadas, obsolescência e degradação física dos suportes (CDs, DVDs, HDs e Pen Drives), tendo por consequência a corrupção da sequência de *bits* do documento arquivístico digital, que acaba por comprometer a sua autenticidade. Com isso, emerge a necessidade de as organizações adotarem políticas e procedimentos tendo em vista produzir e manter documentos autênticos e acessíveis, de modo que tal autenticidade possa ser comprovada (BRASIL, 2004b).

Os documentos arquivísticos digitais correm risco constante de perda ou adulteração em virtude da facilidade de serem modificados sem deixar vestígios aparentes, bem como pelas fragilidades das mídias de armazenamento. Para tanto, devese definir uma série de procedimentos para protegê-los de tais intempéries. Sendo assim, a preservação desses documentos requer uma visão holística, capaz de estabelecer uma cadeia

de preservação que contemple todo o seu ciclo de vida. Ou seja, com monitoramento contínuo que objetiva protegê-lo desde o ato da produção, perpassando todas as etapas de sua tramitação.

Destaca-se que os métodos para conservação e preservação de informações em suportes analógicos chegaram a patamares avançados. Em contrapartida, os métodos para preservar informações em ambiente digital estão em fase de desenvolvimento. Além de implementar uma série de soluções tecnológicas, é preciso definir políticas de preservação digital e requisitos informacionais como, por exemplo, padrões de metadados e formatos de arquivo recomendados para a preservação em longo prazo (CLOONAN, 2016).

A complexidade da preservação digital, aliada às diversas ações que devem ser tomadas, reforça a necessidade de uma abordagem sistêmica, de modo que seja pautada em normas e padrões amplamente aceitos pela literatura. Com isso, pode-se reunir um sólido *corpus* teórico para orientar o planejamento e as intervenções necessárias para preservar documentos autênticos com garantia de acesso ininterrupto no longo prazo.

Metodologia

Tendo em vista o contexto apresentado, este artigo tem por objetivo realizar uma abordagem sistêmica da preservação digital, que se fundamenta em padrões reconhecidos pela literatura, para que assim, possam orientar a implementação dos sistemas informatizados. Ademais, faz-se uso de uma abordagem holística do ciclo de vida dos documentos arquivísticos digitais, de modo que a sua preservação é pensada durante todas as etapas de tramitação dos documentos, até mesmo antes de serem produzidos.

Estima-se que uma abordagem holístico-sistêmica possibilita compreender a necessidade de normatizar a preservação digital e pensar suas ações em todo o ciclo de vida dos documentos. Logo, permite implementar sistemas de informação interoperáveis para os ambientes de gestão e preservação, de modo a manter as cadeias de preservação e de custódia documental.

O método utilizado para apoiar o ponto de vista deste artigo parte do levantamento bibliográfico, composto essencialmente por livros, publicações técnicas e artigos científicos. Para os livros, buscou-se contemplar temáticas como: custódia, autenticidade, preservação digital e gestão de documentos arquivísticos. As publicações técnicas consistem em: diretrizes do Conselho Nacional de Arquivos, normas e estudos internacionais, e a legislação vigente.

Já os artigos foram recuperados por meio da ferramenta de pesquisa *Google Scholar*, capaz de localizar materiais em diversas fontes de informação. Para tanto, utilizaram-se combinações com as seguintes palavras-chave: "repositórios arquivísticos digitais", "confiabilidade", "preservação digital" e "custódia". Foi privilegiado o intervalo entre os anos de 2017-2020, e utilizam-se outros artigos fora do período, recuperados a partir de suas referências a fim de apoiar a fundamentação teórica.

Os dados coletados foram analisados pela abordagem sistêmica (normas, padrões e legislação), aliada à abordagem holística (ciclo de vida documental). Ademais, caracteriza-se pela subjetividade da interpretação, de modo que a discussão dos resultados segue a lógica dedutiva e busca salientar o ponto de vista dos autores (GIL, 2010; LUNA, 1997;SILVA; MENEZES, 2005; VOLPATO, BARRETO, UENO, VOLPATO, GIAQUINTO; FREITAS, 2013).

Logo, obtém-se um artigo de revisão assistemática/narrativa que parte de uma temática aberta, guiada pelos referenciais da Arquivística e da preservação digital, buscando assim, estabelecer relações com normas e padrões pertinentes para orientar a implementação dos sistemas informatizados (CORDEIRO, OLIVEIRA, RENTERÍA; GUIMARÃES, 2007).

A autenticidade ante produtores e preservadores

Na Arquivística há dois indivíduos responsáveis pela gestão e preservação dos documentos, que são respectivamente, produtor e preservador. A posse desses documentos imputa a responsabilidade, daí deriva o conceito de custódia documental, que assume duas abordagens: custodial e pós-custodial.

Na perspectiva custodial, o produtor é responsável tanto pela criação quanto pela preservação em longo prazo. Ou seja, os documentos arquivísticos são geridos e preservados por um mesmo indivíduo

ou instituição. Já a visão pós-custodial traz reformulações à visão de custódia tradicional, de modo que a documentação pode ser transferida para um terceiro (o preservador), fato que provoca a alteração da custódia. Dessa forma, a responsabilidade pelos documentos arquivísticos pode ser delegada para indivíduo ou instituição que possui expertise em preservação, bem como a devida regulamentação. A transferência de custódia pode ser, por exemplo, de uma instituição para um arquivo público; ou para uma empresa do setor privado que presta tais serviços.

Desse modo, surge a necessidade do preservador ser um custodiador confiável, entendido como pessoa física ou jurídica que assume a custódia e as responsabilidades decorrentes desde a fase de gestão documental. A partir do momento em que é produzido, o documento digital é classificado, descrito e identificado com os metadados, de modo que está pronto para arquivamento, perpassando ambientes de preservação e acesso (SILVA, 2017). No caso da alteração de custódia, cabe ao preservador manter a autenticidade que os documentos possuem junto ao produtor no ambiente de gestão.

Deve-se ressaltar que alterar a custódia não significa negligenciá-la, e sim buscar o meio mais adequado para prolongá-la (ARAÚJO, 2014). Ao delegar tal responsabilidade ao custodiador confiável entende-se que este irá proteger a documentação para mantê-la autêntica no longo prazo.

A cadeia de custódia é um dos pilares da autenticidade; seu ambiente envolve pessoas, sistemas, normas, políticas e o acervo propriamente dito. Trata-se de uma linha ininterrupta que se estende desde a gestão, perpassa a preservação até chegar ao acesso à informação. Nesse trajeto, são registradas questões como: sequência de custodiadores, controle de transferências e evidências.

Tradicionalmente, o conceito arquivístico de cadeia de custódia está relacionado à qualidade dos documentos públicos para que possam ser válidos enquanto prova administrativa. De modo que esse valor está fortemente ligado ao caráter único, autêntico e imparcial dos arquivos (JENKINSON, 1922). Logo, visa demonstrar a sucessão de entidades coletivas ou pessoas que tiveram posse, custódia e controle sobre a documentação. Esse conceito nasce ligado ao ambiente analógico, portanto, à cadeia de custódia tradicional, que não é suficiente para garantir a proteção dos documentos digitais, dada a sua facilidade de efetuar falsificações em seu conteúdo. As adulterações em documentos digitais não deixam vestígios, já em documentos analógicos, registrados em suportes como o papel, podem ser identificadas por métodos baseados na análise do suporte e da assinatura.

Dessa forma, a facilidade de adulterar os documentos arquivísticos digitais desperta a importância de uma preservação ativa, ou seja, um conjunto de sistemas que monitorem continuamente as ações proferidas sobre os documentos. Com isso, estima-se criar um histórico para fundamentar a presunção de autenticidade.

Na cadeia de custódia tradicional, a presunção de autenticidade dos documentos arquivísticos analógicos sempre fez parte do processo, sendo fortemente apoiada pela análise de forma fixa e conteúdo estável. Além disso, o conteúdo é inseparável do suporte. Logo, a presunção de autenticidade desses documentos baseia-se na presença de uma cadeia de custódia ininterrupta.

A presunção de autenticidade deve ser apoiada pela evidência de que o documento não foi alterado ou corrompido em seus aspectos essenciais durante sua tramitação, transferência ou recolhimento (DURANTI, 1994). Então, a autenticidade é a qualidade de um documento ser exatamente aquele que foi produzido, de modo que não tenha sofrido alterações, corrupção de dados e adulteração de conteúdo. Logo, a autenticidade é composta por identidade e integridade (BRASIL, 2012).

Observa-se que a autenticidade está condicionada aos processos de produção, manutenção e custódia dos documentos a fim de garantir que não foram adulterados. Com isso, tais documentos irão transmitir o mesmo sentido, sendo capaz de atestar as funções/atividades para as quais foram produzidos (JARDIM; FONSECA, 2008;RONDINELLI, 2005). Sendo assim, as transferências e os recolhimentos do ambiente de gestão para o ambiente de preservação devem ser controlados por meio de auditorias para comprovar que são utilizadas recomendações preconizadas pela Arquivística.

Cadeia de custódia digital arquivística

Uma cadeia de custódia digital arquivística demanda cuidados específicos com a gestão e a preservação como, por exemplo, a migração de suportes e formatos de arquivo, de modo a registrar tais ações em metadados. Esse controle faz-se necessário para evitar possíveis manipulações, e assim manter a presunção de autenticidade dos documentos digitais. Dessa forma, destaca-se a importância da interoperabilidade entre os ambientes de gestão e preservação, permitindo que os documentos sejam recolhidos ao arquivo permanente sem interromper a cadeia de custódia.

A custódia consiste em assumir responsabilidade jurídica, seja ela temporária ou definitiva, de modo ao custodiador tornar-se responsável pela guarda e proteção de tais documentos (CAMARGO; BELLOTTO, 2012). A custódia inclui uma cadeia de responsabilidade que independe do vínculo de propriedade. Com isso, estima-se garantir que os documentos mantenham questões como: a forma fixa, o conteúdo estável, a organicidade e o contexto (LUZ, 2018).

Para que o documento arquivístico digital possa ser utilizado como fonte de prova, testemunho, memória, patrimônio e cidadania plena, precisa ser autêntico. Tal característica deve ser mantida tanto no ambiente de gestão quanto no de preservação, seja abordagem custodial ou pós-custodial. Caso a cadeia de custódia seja interrompida, o tempo em que os documentos não estiveram sob a proteção do seu produtor ou sucessor, será suficiente para causar dúvidas com relação a sua autenticidade.

A abordagem da cadeia de custódia digital arquivística continua associada à proteção do acervo; no entanto, a posse física não é suficiente para manter sua autenticidade, dadas as vulnerabilidades dos documentos digitais (DURANTI, 1994). Assim, a custódia deverá contemplar toda a informação manifestada em suporte, registrada na decorrência das funções e atividades do órgão, que poderão constituir fonte de prova ou imputar algo na vida das pessoas. Essa perspectiva inclui e-mails, *websites*, documentos digitais, sistemas informatizados para gestão e preservação, redes sociais, dados de pesquisa, filmagens de câmeras de vídeo-monitoramento, entre outros. Ou seja, deve-se gerir a informação orgânica produzida e registrada pelos gestores.

No contexto do serviço público, é preciso entender quem está efetivamente com a custódia dos documentos arquivísticos digitais e se os setores de arquivo estão recolhendo e arquivando esses documentos de forma adequada. Além disso, é preciso ponderar se a custódia de tais documentos é de responsabilidade dos profissionais de tecnologia de informação ou dos arquivistas. Acredita-se que o arquivista deve trabalhar com a cadeia de custódia, tendo em vista que é devidamente qualificado para receber a atribuição de preservar documentos arquivísticos. Já o profissional de tecnologia de informação é qualificado para especificar requisitos, desenvolver sistemas, elevar a segurança, e assim, contribuir para a custódia em ambiente digital.

A infraestrutura será fundamental para alcançar o nível de confiabilidade do repositório digital e demais sistemas de informação responsáveis por armazenar, preservar e recuperar documentos digitais. Assim, as organizações e os cidadãos (público em geral), podem confiar na preservação e garantia de acesso a documentos autênticos no longo prazo (THIBODEAU, 2002;THOMAZ, 2007).

Nesse contexto, a validade legal dos documentos digitais está condicionada à capacidade dos sistemas garantirem a sua autenticidade. Conforme o desenvolvimento dessas soluções tecnológicas, os legisladores podem começar um processo de regularização do uso de documentos digitais (MÁRDERO ARELLANO; ANDRADE, 2006).

A custódia arquivística requer a implementação de um Repositório Arquivístico Digital Confiável (RDC-Arq), preconizado por diversos estudos como: Brasil (2015), Flores, Pradebon e Cé (2017), Gonçalez (2017), Luz (2018), Santos (2019) e Santos e Flores (2020). Sendo assim, o RDC-Arq deve manter interoperabilidade com o Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e demais sistemas de negócio. No caso de documentos de valor permanente, o RDC-Arq requer ênfase em ações como a descrição arquivística, utilizando-se de normas como:

- Norma Geral Internacional de Descrição Arquivística (ISAD (G));
- Norma Brasileira de Descrição Arquivística (NOBRADE);

• Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias (ISAAR (CPF));

• Norma Internacional para Descrição de Instituições com Acervo Arquivístico (ISDIAH);

• Norma Internacional para Descrição de Funções (ISDF).

Para custodiar documentos arquivísticos digitais há uma série de normas e padrões que devem ser levados em consideração. Logo, surge a necessidade de promover o diálogo entre os profissionais de arquivo e de tecnologia da informação.

Cadeia de preservação arquivística

A estrutura de uma cadeia de preservação contempla elementos como estratégias, políticas e metodologias que são necessárias ao gerenciamento dos documentos digitais. Idealmente, essa cadeia começa na produção, portanto, os preservadores devem fornecer orientações para produção e manutenção de documentos arquivísticos digitais (INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS, 2007b).

A cadeia de preservação pode ser entendida como um sistema de controle que comporta todo o ciclo de vida dos documentos com o objetivo de protegê-los e assegurar sua autenticidade ao longo do tempo. Trata-se de um complemento à cadeia de custódia digital arquivística, que representa as atividades de produção, manutenção, avaliação e preservação digital.

A cadeia de custódia trata-se de um conceito jurídico que fortalece a confiança com relação à autenticidade, guarda e proteção dos documentos. Já a cadeia de preservação concentra-se nas atividades de produção, manutenção, avaliação e preservação digital, de modo a envolver todo o ciclo de vida dos documentos (LUZ; FLORES, 2018). Na cadeia de preservação e na de custódia digital, os documentos arquivísticos necessitam de cuidados especiais levando em consideração conceitos e legislação que garantam a preservação e acesso em longo prazo (FLORES; PRADEBON; CÉ, 2017).

Prover o acesso aos documentos preservados é uma das funções essenciais da cadeia de preservação. O preservador deve gerir o acesso com o mesmo senso de responsabilidade e competência técnica/profissional empregados no processo de avaliação, recebimento/transferência, descrição e armazenamento da documentação (INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS, 2007a).

Com isso, a cadeia de preservação consiste em uma linha de monitoramento contínuo que promove intervenções, devidamente justificadas, que têm por objetivo a preservação de documentos arquivísticos digitais autênticos (SANTOS; FLORES, 2020).

Observa-se certo grau de atuação conjunta com a cadeia de custódia, logo, haverá uma relação de interdependência entre as cadeias em prol da preservação e manutenção da autenticidade no longo prazo.

Sendo assim, o RDC-Arq assegura a manutenção dessas cadeias, tendo em vista a sua capacidade de lidar com as complexidades, as especificidades e as vulnerabilidades inerentes aos documentos arquivísticos digitais (LUZ; FLORES, 2018). Para tanto, as políticas de preservação que regem o SIGAD e o RDC-Arq devem considerar os padrões relevantes na literatura técnica.

Visão holística do ciclo de vida dos documentos

A separação dos documentos, por meio dos ambientes de gestão e preservação, se dá nos países que praticam as correntes arquivísticas tradicional, integrada e *records management*. Maiores detalhes sobre as correntes arquivísticas são apresentados por Lopes (2014).

Nessa perspectiva, os documentos em que predomina o valor administrativo ficam nas fases corrente e intermediária, de modo que aqueles onde predomina o valor histórico e probatório, depois de cumprirem a temporalidade de guarda, são recolhidos ao arquivo permanente. Há de se ressaltar que essa distinção toma por base a predominância de valor, logo, não impede os documentos em fase corrente e intermediária de possuir valor histórico e probatório, bem como os documentos em fase permanente de possuir valor administrativo.

Gestão de documentos digitais

O ambiente de gestão documental será responsável por produzir e tramitar os documentos arquivísticos digitais de forma confiável. Além disso, terá de avaliá-los para que os documentos em que predominam o valor histórico e probatório sejam recolhidos ao arquivo permanente.

Com a evolução do modo de gerir os documentos na fase corrente, não se pode mais comparar a produção dos documentos como um controle de estoques. Atualmente, o cuidado está em gerenciar os fluxos de produção das informações (LE COADIC, 2004). Para tanto, é preciso normatizar a gestão de documentos, logo, é pertinente seguir normas e padrões em arquivos correntes e intermediários. Dentre estes se destacam: DOD 5015.02, nos Estados Unidos; e *Modular Requirements for Records Systems* (MoReq), na Europa.

Já no contexto brasileiro, há o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil), que contempla um conjunto de requisitos para implementar um SIGAD (BRASIL, 2007). Dessa forma, o SIGAD será responsável pela gestão de documentos digitais e analógicos. No caso dos documentos analógicos, um representante digital (cópia digitalizada do documento) é capturado pelo SIGAD, e para sua identificação deve-se inserir metadados.

Um SIGAD em conformidade com o e-Arq Brasil deve contemplar requisitos como, por exemplo: capturar, armazenar, indexar os documentos arquivísticos e seus respectivos componentes digitais[3]; organizar a documentação conforme o plano de classificação a fim de manter a lógica da relação orgânica entre os documentos; de modo a possibilitar a sua busca e recuperação; executar a avaliação com base na tabela de temporalidade para promover o recolhimento dos documentos que serão preservados, bem como eliminar os documentos que não possuem valor administrativo, histórico, probatório ou informativo; implementar esquemas de metadados para descrever o contexto jurídico-administrativo dos documentos; e atribuir restrições de acesso para proteger a confidencialidade da informação (BRASIL, 2011a).

Com adesão ao e-Arq Brasil, as instituições podem acelerar o controle de produção de documentos digitais e normalizar a metodologia de uso (ROCHA; SILVA, 2007). Assim, o SIGAD deve tratar o documento arquivístico desde o momento de sua produção ou recebimento, independente do suporte (LUZ, 2016). Ressalta-se que o SIGAD poderá ser desenvolvido a partir de um ou vários sistemas de negócios integrados (BRASIL, 2011a). Dessa forma, sendo o SIGAD responsável pela captura, tramitação, classificação, avaliação e destinação dos documentos, também poderá interoperar com os demais sistemas de negócio que a organização utiliza, como, por exemplo: *Customer Relationship Management* (CRM), *Enterprise Resource Planning* (ERP) e *Business Intelligence* (BI).

O SIGAD atende os requisitos de gestão dos documentos a partir do plano de classificação e da tabela de temporalidade e destinação de documentos. Ele gerencia o ciclo de vida dos documentos de acordo com as atividades e funções (LUZ, 2016). Ademais, o SIGAD pode ser implementado por meio de *softwares* como: *Nuxeo DM, Alfresco, Archivista Box, Maarch, Orfeo LIBRE*, entre outros. Com isso, desenvolve-se uma plataforma que engloba um conjunto de funcionalidades e métodos que promovem a eficiência administrativa.

A implementação de um SIGAD que contemple e-Arq Brasil é fundamental para manter conformidade com legislação vigente, como, por exemplo, a Lei nº 8.159/1991, que em seu art. 25 dispõe sobre a responsabilidade penal, civil e administrativa, daquele que desfigurar ou destruir documentos de valor permanente, de interesse público e social (BRASIL, 1991). Destaca-se também a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento dos dados pessoais, inclusive digitais, exigindo dos profissionais da informação, manutenção, sigilo e segurança jurídica (BRASIL, 2018). Nessa perspectiva, observa-se a pertinência de utilizar sistemas confiáveis como o SIGAD, para assim, assegurar a perenidade das informações de interesse público, bem como a confidencialidade e o sigilo.

Para serem autênticos, os documentos digitais precisam receber seus metadados de gestão conforme o e-Arq. Posteriormente, devem-se inserir os metadados de representação/descrição arquivística para facilitar a busca e recuperação da informação. Portanto, os desafios proporcionados pelos documentos digitais

demandam a definição de políticas com base na literatura de gestão eletrônica e preservação digital, além de considerar os fundamentos da disciplina Arquivística. Sendo assim, o arquivista precisa vislumbrar a implementação de sistemas informatizados com capacidade para produzir, capturar e armazenar os documentos digitais com alto grau de confiabilidade.

Preservação e acesso em longo prazo

Os principais métodos de preservação podem ser agrupados em duas categorias: estruturais e operacionais. Assim, os estruturais consistem nos investimentos iniciais, como infraestrutura, visando implementar procedimentos de preservação. Já os métodos operacionais são intervenções aplicadas aos documentos e seus respectivos componentes digitais (MÁRDERO ARELLANO, 2004).

No entanto, as estratégias de preservação digital não podem ser implementadas de forma isolada/aleatória. Devem-se sistematizar as ações, para obter controle sobre as modificações por meio de uma estrutura de metadados. Para tanto, surge a necessidade de implementar um RDC-Arq, o qual atua como um arquivo permanente digital, voltado para guarda, proteção e custódia de documentos arquivísticos autênticos no longo prazo.

O RDC-Arq poderá contemplar as fases corrente, intermediária e permanente, sendo capaz de preservar os documentos de forma autêntica, bem como garantir o acesso em longo prazo. Seu uso nas fases corrente e intermediária ocorre devido a questões de preservação e casos específicos, como, por exemplo, documentos de longa temporalidade, elevado nível de complexidade e/ou sigilosos (BRASIL, 2015).

Dentre os documentos de longa temporalidade podem-se citar, por exemplo, o assentamento funcional digital e o prontuário eletrônico de paciente. Igualmente, os documentos sensíveis, que ferem a privacidade, precisam ser preservados e protegidos, cumprindo a Lei nº 13.709/2018 (LGPD), que estabelece normas rigorosas para a proteção de dados pessoais. Já entre os documentos complexos, destacam-se aqueles com multicomponentes, como por exemplo, o *website* e o e-mail, que necessitam de um conjunto de objetos digitais para representar um documento digital.

Ressalta-se que a questão da autenticidade deve estar apoiada em sistemas de informação confiáveis, isso inclui os sistemas de negócio, o SIGAD e o RDC-Arq, então desenvolvidos a partir de padrões relevantes. Logo, o RDC-Arq deve estar em conformidade com o modelo *Open Archival Information System* (OAIS), que corresponde à norma *International Organization for Standardization* (ISO) 14721:2012, principal referência em preservação digital. Essa norma foi traduzida no Brasil pela Associação Brasileira de Normas Técnicas (ABNT) como Norma Brasileira Recomendada (NBR), tornando-se a ABNT/NBR 15472:2007, Sistema Aberto de Arquivamento de Informação (SAAI).

O modelo OAIS/SAAI contempla uma série de funções para preservar a informação, sendo responsável por questões como: admissão, armazenamento arquivístico, gerenciamento de dados, acesso e disseminação. Esse modelo perpassa a migração da informação digital para novos formatos de arquivo e suportes, além de propor um modelo para representar a informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2007; CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM, 2012;INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012a).

Documentos não devem ser entregues ao preservador em mídias de armazenamento, e sim em pacotes de informação, de modo que as cadeias de custódia e preservação não sejam interrompidas. Portanto, os pacotes de informação serão utilizados para mediar as trocas de informação do ambiente OAIS (RDC-Arq) com os produtores e consumidores. Logo, o OAIS estabelece três tipos de pacotes: Pacote de Informação para Submissão (*Submission Information Package* - SIP); Pacote de Informação para Arquivamento (*Archival Information Package* - AIP) e Pacote de Informação para Disseminação (*Dissemination Information Package* - DIP). Cada pacote é utilizado para funções distintas:

- SIP: entregue pelo produtor ao OAIS para ser armazenado e preservado;
- AIP: consiste no objeto de preservação que reúne todas as informações necessárias para manutenção de sua autenticidade;

• DIP: é derivado de um ou mais AIPs, entregue pelo OAIS ao consumidor em resposta a uma solicitação de pesquisa.

Os pacotes SIP, AIP e DIP comportam o documento e seus metadados, distribuídos em: informação descritiva de preservação, informação de empacotamento e a descrição do pacote. Ademais, o RDC-Arq que segue os requisitos do OAIS não se trata de um *software* específico, e sim de um conjunto composto por: sistemas informatizados, pessoas, políticas, procedimentos e o próprio acervo.

O êxito do RDC-Arq está condicionado às boas práticas da produção e preservação, de modo que a inserção de metadados esteja prevista em todo o ciclo de vida dos documentos digitais (SARAMAGO, 2002). Um RDC-Arq bem sucedido é aquele que cumpre com o propósito para o qual foi criado, de modo que os critérios para avaliálo serão derivados da declaração de propósito e compromisso (THIBODEAU, 2007). Com base nessas questões deve-se moldar a infraestrutura, bem como capacitar a equipe responsável conforme as demandas tecnológicas surjam.

Há de se ressaltar que apenas duas categorias de profissionais devidamente regulamentados devem ter acesso ao ambiente de preservação, o arquivista/cientista da informação e o profissional de tecnologia da informação. Esses profissionais irão compartilhar as responsabilidades pela cadeia de custódia digital arquivística, logo observa-se uma possível ruptura paradigmática ante a ideia tradicional de cadeia de custódia.

A confiabilidade do RDC-Arq está condicionada ao processo de auditoria, que verifica a sua conformidade com o modelo OAIS, com ênfase em questões como: responsabilidade administrativa, viabilidade organizacional, respaldo financeiro, adequação tecnológica, segurança da informação e transparência em sua prestação de contas.

No âmbito do *Consultative Committee for Space Data Systems* (CCSDS), recomendase que os repositórios digitais que seguem o OAIS sejam auditados por meio do *Audit and Certification of Trustworthy Digital Repositories* (ACTDR). Esse padrão tornou-se a norma ISO 16363:2012; possui áreas potenciais de preocupação de segurança, como, por exemplo, a possibilidade do repositório ser enganado no processo de auditoria por indivíduo não qualificado ou mal-intencionado, bem como o possível vazamento de informações confidenciais a que o auditor terá acesso (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM, 2011;INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012b). A auditoria irá demonstrar que um RDC-Arq mantém conformidade com o OAIS e comporta os princípios da Arquivística.

Com auditorias periódicas, verificam-se as vulnerabilidades e o cumprimento das políticas de preservação com o objetivo de buscar soluções para elevar o nível de confiabilidade do RDC-Arq. Em caráter complementar à auditoria, deve-se proceder à certificação para demonstrar que o RDC-Arq atingiu os níveis esperados, e que pode ser considerado "confiável" (SANTOS, 2019). Destaca-se que a auditoria e a certificação devem ser realizadas por meio de terceiros a fim de agregar credibilidade ao processo como um todo.

Além de preservar documentos arquivísticos autênticos, é preciso disponibilizar plataformas de acesso e disseminação da informação para que os cidadãos possam usufruir dos conteúdos. Já para contribuir com a transparência ativa é preciso desenvolver uma interface amigável, intuitiva, que permita gerar instrumentos de pesquisa, disponha de navegação multinível, bem como permita realizar o *download* dos pacotes DIP disponíveis.

A navegação multinível permite estabelecer uma clara distinção dos níveis hierárquicos, de modo que o usuário tem a percepção clara da organização interna dos documentos, capaz de refletir o quadro de arranjo elaborado pelos arquivistas. Com a navegação multinível é possível identificar, por exemplo, a qual setor ou departamento da instituição pertence determinado documento.

Tais aspectos corroboram a Lei 12.527/2011, Lei de Acesso à Informação (LAI), válida para os três Poderes da União, Estados, Distrito Federal, Municípios e entidades privadas sem fins lucrativos que receberam ou destinaram recursos ao poder público. Para efetividade da LAI, as organizações necessitam disponibilizar em

seus *sites* os seguintes itens: ferramentas de pesquisa; relatórios em formatos de arquivo que não dependem de *softwares* específicos com licenças de uso para serem interpretados; acesso via sistemas; método em que a informação é estruturada; garantir a autenticidade; manter a informação atualizada; indicar seus meios para comunicação; e ter mecanismos para garantir a acessibilidade (BRASIL, 2011b).

Ainda há de se mencionar a consonância do ambiente de preservação e acesso com o uso de dados abertos. Pode-se disponibilizar o plano de classificação de documentos, a tabela de temporalidade, guias e inventários em formatos como: *Encoded Archival Description* (EAD), *Extensible Markup Language* (XML), *Comma-Separated Values* (CSV) e outros. Igualmente, o RDC-Arq pode disponibilizar dados brutos como, por exemplo: extratos dos documentos, cruzamentos, sínteses, análises, planificações, sumarização e estatísticas.

Para mediar o acesso, pode-se acoplar a plataforma *Access to Memory* (AtoM) para interagir com o RDC-Arq e possibilitar o acesso à informação, transparência ativa e exercício da cidadania plena. Destaca-se que o AtoM é um *software* livre e de código aberto, que pode ser personalizado para cada instituição. Sua interface de acesso reflete a organização hierárquica interna do fundo documental, além de permitir buscas de documentos por meio de palavras-chave relacionadas, por exemplo, ao assunto e aos indivíduos.

Além disso, é preciso que o RDC-Arq disponibilize em sua plataforma de acesso (AtoM) os documentos em padrões abertos, ou seja, de modo que possam ser interpretados em diferentes plataformas tecnológicas sem restrições de uso, e sem a necessidade de adquirir determinado *software* ou licença. Dessa forma, ao preservar documentos digitais nesses formatos, o RDC-Arq otimiza suas ações, pois irá minimizar o potencial de obsolescência; e ao disponibilizar os documentos para o público geral nesses formatos, o AtoM irá facilitar o acesso à informação e a interpretação dos documentos disponibilizados via pacote DIP.

A liberdade proporcionada por esses formatos possibilita adaptações, tendo em vista o aperfeiçoamento das atividades de preservação digital. Com isso, busca-se aumentar as perspectivas de longevidade das informações disponibilizadas para garantir acesso em longo prazo (ALMEIDA; NASCIMENTO, 2011).

A dependência de *softwares* e formatos proprietários específicos é um entrave significativo para a preservação digital. Consequentemente, as estratégias de migração tendem a ser executadas com mais frequência, de modo que podem ocasionar perdas de informação, pois, não há domínio sobre o formato fechado (CAMPOS; SARAMAGO, 2007; INNARELLI, 2009).

A informação digital é complexa por natureza, e o excesso de intervenção humana aumenta, paradoxalmente, a sua complexidade, em especial por causa do seu caráter recursivo. Logo, será necessário, reunir cada vez mais informações digitais para representar e preservar uma determinada informação digital. Tais estratégias, que deveriam ser as pontes para o acesso à informação, tornar-se-ão muralhas, um óbice a ser superado. (SANTOS; KRAWSZUK, 2019, p. 11)

Observa-se a necessidade de o preservador orientar os produtores com relação aos formatos de arquivo que devem ser priorizados. Com isso, é possível diminuir a quantidade de migrações realizadas sobre os documentos arquivísticos digitais, evitando possíveis perdas de informação. Mesmo que um formato se torne obsoleto, poderá ser reconstruído pela equipe de tecnologia da informação e programadores, bastando haver acesso ao seu código fonte. Com isso, ao escolher sistemas, *softwares* e formatos de arquivo com base em padrões abertos, minimizam-se as perspectivas de obsolescência tecnológica.

Considerações finais

No decorrer deste artigo defendeu-se a pertinência de uma abordagem holísticosistêmica para comportar as complexidades e especificidades dos documentos arquivísticos digitais. Com isso, a preservação de tais documentos precisa vislumbrar as ações executadas por produtores e preservadores, de modo a incorporar todo o ciclo de vida documental.

É preciso que os documentos arquivísticos sejam gerenciados por sistemas informatizados, constituindo assim, os ambientes de gestão e preservação. Ressalta-se que esses ambientes devem ser envolvidos em uma cadeia de custódia ininterrupta, a fim de agregar confiabilidade às ações proferidas. Igualmente, deve-

se manter uma cadeia de preservação para monitoramento contínuo da documentação, tendo em vista a manutenção da autenticidade e garantia de acesso contínuo em longo prazo.

As cadeias de custódia e preservação se demonstram interdependentes, seja na perspectiva custodial ou na pós-custodial. Além disso, sua abordagem em ambiente digital requer o compartilhamento da custódia, de modo a envolver os profissionais de arquivo e tecnologia da informação. Assim, ambos os profissionais precisam discutir a elaboração das políticas de preservação, bem como escolher as estratégias a serem executadas.

No caso brasileiro, o ambiente de gestão requer a implementação de um SIGAD em conformidade com o modelo e-Arq Brasil, que seja capaz de capturar, inclusive, os documentos produzidos e armazenados em sistemas de negócio da organização (ERP, CRM, BI e outros). Já para o ambiente de preservação, deve-se implementar um RDC-Arq em conformidade com o modelo OAIS, e que seja periodicamente auditado por terceiros através do padrão ACTDR, tendo em vista obter a certificação.

Sendo assim, um RDC-Arq deve possuir instrumentos de pesquisa multiníveis a fim de facilitar o acesso à informação custodiada. Para tanto, é essencial observar a descrição por meio de normas como NOBRADE, ISAD(G), ISAAR(CPF), ISDIAH e ISDF; bem como padrões de metadados que otimizem o processo de busca precisa e recuperação da informação. Tais elementos auxiliam no cumprimento da LAI, além de melhorar a prestação de serviços ao cidadão.

Ressalta-se que SIGAD e RDC-Arq devem ser interoperáveis a fim de facilitar a transferência/recolhimento, bem como contemplar todo o ciclo de vida dos documentos. Sua abordagem torna-se holística quando inseridos no âmbito das cadeias de preservação e de custódia, de modo que a preservação e a autenticidade são pensadas antes mesmo da produção documental. Igualmente, sua abordagem adquire caráter sistêmico quando os elementos que compõem o sistema de arquivos são implementados com base em normas, padrões relevantes e na legislação vigente.

Observa-se um novo horizonte para a preservação digital, que passa a ser pensada já no momento da produção, mediada por políticas organizacionais e com uso de padrões abertos. Além disso, a aproximação do SIGAD junto aos sistemas de negócio integra e potencializa a gestão da informação orgânica. Ao passo em que os documentos são devidamente capturados e geridos pelo sistema de arquivos, cria-se uma sinergia, permitindo assim, o reuso da informação estratégica que foi devidamente preservada.

Por fim, as cadeias de preservação e custódia mostram-se interdependentes, especialmente quando abordadas na perspectiva dos documentos arquivísticos digitais. Ao ressignificar seus conceitos na perspectiva da preservação holístico-sistêmica, chegase ao conceito de Cadeia de Custódia Digital Arquivística: uma abordagem que considera as complexidades advindas dos ambientes digitais, bem como as especificidades dos documentos arquivísticos. Essa abordagem se fundamenta em padrões nacionais e internacionais, e comporta todo o ciclo de vida dos documentos.

Referências

ALMEIDA, Ana Cláudia Lopes de; NASCIMENTO, Genoveva Batista do. Considerações sobre a preservação de documentos em formato digital. **Biblionline**, João Pessoa, v. 7, n. 2, 2011. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/biblio/article/view/10422. Acesso em: 13 set. 2020.

ARAÚJO, Carlos Alberto Ávila. **Arquivologia, biblioteconomia, museologia e ciência da informação**: o diálogo possível. Brasília: Briquet de Lemos; São Paulo: ABRAINFO, 2014.

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

BARRETO, Aldo de Albuquerque. Os documentos de amanhã: a metáfora, a escrita e a leitura nas narrativas em formato digital. **DataGramaZero**, Rio de Janeiro, v. 10, n. 1, 2009. Disponível em: http://ridi.ibict.br/handle/123456789/159. Acesso em 05 abr. 2020.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Carta para a preservação do patrimônio arquivístico digital**. Rio de Janeiro: Arquivo Nacional, 2004a. Disponível em: http://conarq.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf. Acesso em: 03 abr. 2020.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis - RDC-Arq**. Rio de Janeiro: Arquivo Nacional, 2015. Disponível em: http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf. Acesso em: 23 mar. 2020.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: http://conarq.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_completa.pdf. Acesso em: 23 mar. 2020.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **e-ARQ Brasil**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011a. Disponível em: http://www.siga.arquivonacional.gov.br/images/publicacoes/earq.pdf. Acesso em: 23 mar. 2020.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). **Gestão arquivística de documentos eletrônicos.** Rio de Janeiro: Arquivo Nacional, 2004b. Disponível em: http://pt.scribd.com/doc/37174068/Gestao-Arquivistica-de-Documentos-EletronicosCONARQ-Por-Claudia-Rocha. Acesso em: 03 abr. 2020.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 25, de 27 de abril de 2007**. Rio de Janeiro: Arquivo Nacional, 2007. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucaono-25-de-27-de-abril-de-2007. Acesso em: 01 abr. 2020.

BRASIL. Lei n. 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial**: República Federativa do Brasil: seção 1, Brasília, DF, ano 1991, n. 4, p. 4, 8 jan. 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm. Acesso em: 01 abr. 2020.

BRASIL. Lei, n. 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação (LAI). Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial**: República Federativa do Brasil: seção 1, Brasília, DF, ano 2011b, n. 33, p. 1, 18 nov. 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em: 01 abr. 2020.

BRASIL. Lei n. 13.709, de 15 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. **Diário Oficial**: República Federativa do Brasil: seção 1, Brasília, DF, ano 2018, n. 28, p. 1, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 abr. 2020.

CAMARGO, Ana Maria de Almeida; BELLOTTO, Heloísa Liberalli. **Dicionário de terminologia arquivística**. 3. ed. São Paulo: ARQ-SP, 2012.

CAMPOS, Fernanda Maria Guedes de; SARAMAGO, Maria de Lurdes. Preservação digital de longo prazo em instituições patrimoniais: reutilização e adaptação de metadados. *In*: **Actas dos congressos nacionais de bibliotecários, arquivistas e documentalistas**, v. 9, n. 1, p. 1-7, Lisboa, 2007. Disponível em: http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/540/330. Acesso em: 30 mar. 2020.

CLOONAN, Michèle. Preservando documentos de valor permanente. *In*: EASTWOOD, Terry; MACNEIL, Heather. (org.). **Correntes atuais do pensamento arquivístico**. Belo Horizonte: Editora UFMG, 2016, p. 107-134.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Audit and certification of trustworthy digital repositories (ACTDR)**: magenta book. Washington: CCSDS, 2011. Disponível em: http://public.ccsds.org/publications/archive/652x0m1.pdf. Acesso em: 06 abr. 2020.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Reference model for an open archival information system (oais)**: magenta book. Washington: CCSDS, 2012. Disponível em: http://public.ccsds.org/publications/archive/650x0m2.pdf. Acesso em: 23 mar. 2020.

CORDEIRO, Alexander Magno; OLIVEIRA, Glória Maria de; RENTERÍA, Juan Miguel; GUIMARÃES, Carlos Alberto. Revisão sistemática: uma revisão narrativa. **Rev. Col. Bras. Cir.**, Rio de Janeiro, v. 34, n. 6, p. 428-431, 2007. Disponível em: http://dx.doi.org/10.1590/S0100-69912007000600012. Acesso em: 23 mar. 2020.

DURANTI, Luciana. Registros documentais contemporâneos como provas de ação. **Estudos Históricos**, Rio de Janeiro, v. 7, n. 13, p. 49-64, 1994. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/reh/article/view/1976. Acesso em 30 mar. 2020.

FERREIRA, Miguel. **Introdução à preservação digital**: conceitos, estratégias e actuais consensos. Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf. Acesso em: 03 abr. 2020.

FLORES, Daniel; PRADEBON, Daiane Segabinazzi; CÉ, Graziella. Análise do conhecimento teórico-metodológico da preservação digital sob a ótica da OAIS, SAAI, ISO 14721 e NBR 15472. **Brazilian Journal of Information Science**: research trends, Marília, v. 11, n. 4, p. 7280, 2017. Disponível em: https://doi.org/10.36311/1981-1640.2017.v11n4.11.p73. Acesso em: 23 mar. 2020.

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

GUEDES, Mário Augusto Muniz. Fatores de risco da perda de documentos eletrônicos de caráter arquivístico em uma instituição pública. *In*: RODRIGUES, Georgete Medleg; COSTA, Marli Guedes da (org.). **Arquivologia**: configurações da pesquisa no Brasil: epistemologia, formação, preservação, uso e acesso. Brasília: Editora Universidade de Brasília, 2012. p. 153-171.

GONÇALEZ, Regina Ventura Amorim Gonçalez. Recomendações para certificação ou medição de confiabilidade de repositórios arquivísticos digitais com ênfase no acesso à informação. **Informação & Informação**, Londrina, v. 22, n. 1, p. 215-241, 2017. Disponível em: http://dx.doi.org/10.5433/1981-8920.2017v22n1p215. Acesso em: 23 mar. 2020.

GRANGER, Stewart. Emulation as a digital preservation strategy. **D-Lib Magazine**, v. 6, n. 10, 2000. Disponível em: http://www.dlib.org/dlib/october00/granger/10granger.html. Acesso em: 03 abr. 2020.

INNARELLI, Humberto Celeste. Preservação digital e seus dez mandamentos. *In:* SANTOS, V. B. (org.). **Arquivística**: temas contemporâneos - classificação, preservação digital, gestão do conhecimento. 3. ed. Distrito Federal: SENAC, 2009, p. 21-75.

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

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

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (INTERPARES 2 PROJECT). **Diretrizes do preservador**. A preservação de documentos arquivísticos digitais: diretrizes para organizações. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. [Brasília: Conarq], 2007a. Disponível em: http://conarq.gov.br/images/publicacoes_textos/Diretrizes_produtor_preservador.pdf. Acesso em: 23 mar. 2020

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (INTERPARES 2 PROJECT). **Diretrizes do Produtor**. A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. [Brasília: Arquivo Nacional], 2007b. Disponível em: http://www.siga.arquivonacional.gov.br/images/publicacoes/diretrizes_produtor_digital.pdf . Acesso em: 23 mar. 2020.

JARDIM, José Maria; FONSECA, Maria Odila. O. Arquivos. *In*: CAMPELLO, Bernadete; CALDEIRA, Paulo da Terra (org.). **Introdução às fontes de informação**. 2. ed. Belo Horizonte: Autêntica Editora, 2008. p. 121-139.

JENKINSON, Hilary. **A manual of archive administration including the problems of war archives and archive making**. Oxford: Clarendon Press, 1922.

LE COADIC, Yves-François . **A ciência da informação**. 2. ed. Brasília: Briquet de Lemos, 2004.

LOPES, Luís Carlos. **A nova arquivística na modernização administrativa**. 3. ed. Brasília: Annabel Lee, 2014.

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

LUZ, Charlley dos Santos. A interoperabilidade na preservação da informação arquivística: os metadados e a descrição. **Informação Arquivística**, Rio de Janeiro, v. 5, n. 1, jun. 2016. Disponível em: http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/139. Acesso em: 01 abr. 2020.

LUZ, Charlley dos Santos. Curadoria digital, custódia arquivística e preservação digital: relações possíveis. **Páginas a&b**, Porto, v. 3, n. 10, p. 92-103, 2018. Disponível em: https://doi.org/10.21747/21836671/pag10a7. Acesso: 23 mar. 2020.

LUZ, Charlley dos Santos; FLORES, Daniel. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos. *In*: **Seminário Serviços de Informação em Museus**. [S. l. : s. n.], p. 171-181, 2018. Disponível em: https://www.researchgate.net/publication/325225229. Acesso: 23 mar. 2020.

MÁRDERO ARELLANO, Miguel Ángel. Preservação de documentos digitais, **Ciência da Informação**, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: http://revista.ibict.br/ciinf/article/view/1043. Acesso em: 01 abr. 2020.

MÁRDERO ARELLANO, Miguel Ángel; ANDRADE, Ricardo Sodré. Preservação digital e os profissionais da informação. **DataGramaZero**, Rio de Janeiro, v.7 n. 5, out. 2006. Disponível em: https://repositorio.ufba.br/ri/handle/ri/3039. Acesso em: 01 abr. 2020.

ROCHA, Claudia Lacombe; SILVA, Margareth da. Padrões para garantir a preservação e o acesso aos documentos digitais. **Acervo**, Rio de Janeiro, v. 20, n. 1-2, p. 113-124, 2007. Disponível em: http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/76/76. Acesso em: 06 abr. 2020.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos**: uma abordagem teórica da diplomática arquivística contemporânea. 4. ed. Rio de Janeiro: FGV, 2005.

SANTOS, Henrique Machado dos. Auditoria de repositórios arquivísticos digitais confiáveis. **Informação em Pauta**, Fortaleza, v. 4, n. 2, p. 156-172, 2019. Disponível em: https://doi.org/10.32810/2525-3468.ip.v4i2.2019.41787.156-172. Acesso em 17 mar. 2020.

SANTOS, Henrique Machado dos; FLORES, Daniel. Infraestrutura organizacional necessária ao repositório arquivístico digital confiável: um diálogo com a ISO 16363. **Revista Brasileira de Biblioteconomia e Documentação**, São Paulo, v. 16, p. 1-29, 2020. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/1305. Acesso em: 17 mar. 2020.

SANTOS, Henrique Machado dos; KRAWSZUK, Gabriela Luísa. O documento arquivístico digital no processo de tomada de decisão administrativa: uma breve reflexão. **BIBLOS**, Rio Grande, v. 33, n. 1, p. 4-22, jan./jun., 2019. Disponível em: https://doi.org/10.14295/biblos.v33i1.8659. Acesso em: 03 abr. 2020.

SARAMAGO, Maria de Lurdes. Preservação digital a longo prazo: boas práticas e estratégias. **Cadernos BAD**, Lisboa, n. 2, p. 54-68, 2002. Disponível em: http://www.bad.pt/publicacoes/index.php/cadernos/article/view/866. Acesso em: 02 abr. 2020.

SILVA, Edna Lúcia da; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005. Disponível em: http://www.portaldeconhecimentos.org.br/index.php/por/Conteudo/Metodologia-dapesquisa-e-elaboracao-de-dissertacao. Acesso em: 23 mar. 2020.

SILVA, Margareth da. **O arquivo e o lugar**: custódia arquivística e a responsabilidade pela proteção aos arquivos. Niterói: Eduff, 2017.

THIBODEAU, Kenneth. If you build it, will it fly? Criteria for success in a digital repository. **JoDI**: Journal of Digital Information, Texas, v. 8, n. 2, 2007. Disponível em: https://journals.tdl.org/jodi/index.php/jodi/article/view/197/174. Acesso em: 02 abr. 2020.

THIBODEAU, Kenneth. Overview of technological approaches to digital preservation and challenges in coming years. *In*: **The state of digital preservation:** an international perspective. Washington: CLIR and Library of Congress, 2002. p. 4-31. Disponível em: https://www.clir.org/pubs/reports/pub107/pub107.pdf#page=10. Acesso em: 01 abr. 2020.

THOMAZ, Kátia de Pádua. Gestão e preservação de documentos eletrônicos de arquivo: revisão de literatura - parte 2. **Arquivística.net**, Rio de Janeiro, v. 2, n. 1, p. 114-131, jan./jun., 2006. Disponível em: https://www.brapci.inf.br/index.php/article/download/6733. Acesso em: 03 abr. 2020.

THOMAZ, Kátia de Pádua. Repositórios digitais confiáveis e certificação. **Arquivística.net**, Rio de Janeiro, v. 3, n. 1, p. 80-89, jan./jun. 2007. Disponível em: http://www.brapci.inf.br/_repositorio/2010/05/pdf_fed0720dbb_0010726.pdf. Acesso em: 01 abr. 2020.

VOLPATO, Gilson Luiz; BARRETO, Rodrigo Egydio; UENO, Helene Mariko; VOLPATO, Enilze de Souza Nogueira; GIAQUINTO, Percília Cardoso; FREITAS, Eliane Gonçalves de. **Dicionário crítico para redação científica**. Botucatu: Best Writing, 2013.

Notas

1 Tais documentos podem ser naturalmente produzidos em ambiente digital (nato-digitais) ou representados nesse ambiente (processo de digitalização). Cabe ressaltar que este artigo levanta vulnerabilidades e lança recomendações aplicáveis para ambos.

2 Por exemplo, no modelo tradicional, a impressão de documentos possui um custo fixo por unidade, de modo que o custo total deriva da quantidade de cópias impressas. Já no ambiente digital, esse custo não segue a mesma lógica, pois o custo para produzir um ou dez documentos em formato digital será igual. Este mesmo exemplo também pode ser aplicado para livros ou jornais.

3 Objetos digitais que compõem um documento, contribuindo para a sua correta representação. Uma página web, por exemplo, pode conter imagens e vídeos relacionados ao documento principal.