DOI: https://doi.org/10.30749/2594-8261.v4n2p108-139

CADEIA DE CUSTÓDIA DIGITAL ARQUIVÍSTICA

ARCHIVAL DIGITAL CHAIN OF CUSTODY

Henrique Machado dos Santos[*]
Daniel Flores[**]

Resumo: Este estudo realiza uma reflexão em torno da cadeia de custódia, de modo que vislumbra propor uma abordagem para mitigar as vulnerabilidades dos documentos arquivísticos em ambiente digital. Para tanto, parte-se de um levantamento bibliográfico, sedimentado nos referenciais da Arquivística e da preservação digital. Ademais, recorre-se ao Direito para fundamentar a cadeia de custódia. Essa triangulação de ideias resulta em um artigo de revisão assistemática, que segue a lógica dedutiva para discorrer sobre o objeto de investigação. A discussão consiste em formular uma cadeia de custódia digital arquivística, pautada em padrões reconhecidos pela literatura, e capaz de comportar todo o ciclo de vida dos documentos. Tal abordagem corrobora com a manutenção da autenticidade, proteção do sigilo, preservação e garantia de acesso à informação, e consequentemente, eleva a confiabilidade das fontes de prova. Igualmente, fortalece a segurança jurídica e possibilita o exercício da cidadania plena.

Palavras-chave: Documentos digitais. Arquivos digitais. Cadeia de custódia. Autenticidade. Preservação digital.

Abstract: This study reflects on the chain of custody, to propose an approach to mitigate the vulnerabilities of archival records in the digital environment. For this, part of a bibliographic survey, based on references of Archival science and digital preservation. Also, recover the Law to establish a chain of custody. This triangulation of ideas results in a no systematic review article, which follows a deductive logic to discuss the object of investigation. The discussion consists of an archival digital chain of custody, based on standards recognized by the literature and capable of supporting the entire life cycle of records. Such an approach corroborates the maintenance of authenticity, the protection of confidentiality, the preservation and guarantee of access to information, and consequently, increases the sources of evidence. It also strengthens legal security and enables the exercise of full citizenship.

[*] Mestre em Patrimônio Cultural e Bacharel em Arquivologia pela Universidade Federal de Santa Maria. Arquivista do Arquivo Geral da Universidade Federal do Rio Grande. Integrante do grupo de pesquisa CNPq UFF Ged/A - Documentos Digitais: Gestão, Preservação, Acesso e Transparência Ativa. E-mail: henrique.hms.br@gmail.com

[**] Docente do Curso de Graduação em Arquivologia e do Programa de Pós-Graduação em Ciência da Informação - PPGCI, Mestrado e Doutorado, da Universidade Federal Fluminense - UFF, Niterói, Rio de Janeiro - Brasil. Líder do Grupo de Pesquisa CNPq UFF Ged/A - Documentos Digitais: Gestão, Preservação, Acesso e Transparência Ativa. Pesquisador do Grupo de Pesquisa da Universidade de Brasília - UnB: Fundamentos históricos, epistemológicos e teóricos da Arquivologia - FHETA. Bacharel em Arquivologia pela UFSM, Especialista em Organização de Arquivos pela USP, Mestre em Engenharia da Produção - Tecnologia da Informação pela UFSM, Doutor em Documentação pela USAL/Espanha - revalidado pela UFRJ como Doutor em Ciência da Informação no Brasil.

Keywords: Digital records. Digital archives. Chain of custody. Authenticity. Digital preservation.

Recebido em: 19/07/2020
Aceito em: 20/08/2020

1 INTRODUÇÃO

Os constantes e desenfreados avanços das tecnologias da informação atrelados à necessidade de automação organizacional, originaram uma nova demanda informacional, os documentos digitais. A adesão a tais registros se propagou rapidamente, de modo que ultrapassaram os limites do ambiente de trabalho e já fazem parte do cotidiano das pessoas.

As tecnologias da informação e os documentos digitais são uma realidade cada vez mais sedimentada, e trazem consigo, uma dependência em virtude das facilidades proporcionadas ante os meios tradicionais de comunicação. Dessa forma, se os documentos digitais fazem parte da vida de pessoas e organizações, é notável que passem a compor os arquivos.

Destaca-se que a Arquivística/Arquivologia, em sua trajetória, concentrou-se na gestão e na preservação de documentos analógicos/não digitais, de modo que o advento do documento arquivístico digital exigiu a ressignificação de conceitos e princípios da disciplina. Dentre os principais motivos para lançar um novo olhar sobre a teoria tradicional estão: as vulnerabilidades apresentadas pelos documentos digitais; e a sua relevância para a sociedade.

A informatização *per si* não é capaz de resolver problemas de natureza arquivística, apenas expõe a necessidade de definir políticas de gestão e preservação *a priori*. Os sistemas informatizados são necessários, todavia, precisam seguir padrões e manter a consonância com os pressupostos teóricos da Arquivística. Conceitos elementares como a autenticidade passam a ser ameaçados pelas fragilidades do ambiente digital, fato que torna necessário reformular a cadeia de custódia, até então, pensada para documentos arquivísticos analógicos.

Destaca-se que o valor incomensurável que pode ser atribuído à informação fez a preservação digital ganhar relevância, se desenvolver de forma interdisciplinar, de modo que já conta com vasta bibliografia especializada sobre o tema. Tais conhecimentos têm contribuído para compreender a problemática dos documentos arquivísticos em ambiente digital. Ademais, o surgimento de estudos sobre gestão, preservação, autenticidade e acesso à informação tem fortalecido o *corpus* teórico da Arquivística.

Tendo em vista o exposto, tem-se por objetivo realizar uma reflexão sobre a cadeia de custódia para documentos arquivísticos digitais. Para tanto, considera-se a perspectiva sistêmico-holística da preservação, sedimentada em padrões recomendados na literatura científica, e contemplando todo o ciclo de vida dos documentos. Com isso, pretende-se demonstrar as vulnerabilidades implícitas à natureza dos documentos digitais e discorrer sobre uma abordagem capaz de protegê-los contra eventuais adulterações.

Ressalta-se que a confiabilidade das fontes de informação digital será pautada na adoção de procedimentos de gestão e preservação, controlados por sistemas informatizados. Consequentemente, as fontes digitais passam a auxiliar no processo de (re)construção da História. Logo, é fundamental manter a autenticidade dos documentos arquivísticos digitais, permitindo o resgate da memória social, além de permitir o exercício da cidadania plena pelos cidadãos. Dessa forma, pretende-se demonstrar que a abordagem da cadeia de custódia em ambiente digital pode ser expandida além dos horizontes da Arquivística, de modo a ser considerada no âmbito do Direito e da História.

2 METODOLOGIA

Este estudo assume um caráter descritivo, pois objetiva discorrer sobre as características do objeto de investigação: a cadeia de custódia (GONÇALVES, 2011). O método utilizado consiste no levantamento bibliográfico de livros, publicações técnicas e artigos científicos (GIL, 2010; LUNA, 1997).

Os artigos são recuperados por meio da ferramenta de pesquisa *Google Scholar*, da Base de Dados em Ciência da Informação (BRAPCI) e das redes sociais de pesquisa *Academia.edu* e *ResearchGate*. Tais os artigos são escolhidos por meio da análise do resumo; e outras obras são selecionadas a partir de suas referências.

Destaca-se que o *Google Scholar*, o *Academia.edu* e o *ResearchGate* possuem viés multidisciplinar, e possibilitam recuperar materiais de diversas bases de dados. Já a BRAPCI concentra-se na área de Ciência da Informação e indexa diversos periódicos do Brasil e do exterior.

Os dados coletados estão sujeitos à subjetividade da interpretação, de modo que a discussão do tema segue a lógica dedutiva (SILVA; MENEZES, 2005;

VOLPATO *et al*., 2013). Obtém-se um artigo de revisão assistemática/narrativa que parte da temática aberta, fundamentada pelos referenciais da Arquivística e da preservação digital (CORDEIRO *et al*., 2007). A cadeia de custódia é a categoria norteadora, e para conceituá-la, recorre-se aos referenciais do Direito.

Essa triangulação estabelece uma abordagem interdisciplinar sobre o tema, no entanto, não há pretensão de fazer uma abordagem exaustiva do mesmo. Dessa forma, este estudo limita-se em compreender e expor os pressupostos elementares de uma cadeia de custódia para documentos arquivísticos digitais.

3 O PATRIMÔNIO DOCUMENTAL ANTE À EVOLUÇÃO DAS TECNOLOGIAS

O ato de escrever é considerado um marco que define a civilização, embora não seja fundamental, como a comunicação oral; pois as civilizações não existiriam sem a língua falada, o que faz da escrita uma habilidade secundária. Entretanto, a ausência da escrita impossibilita o registro, em longa escala, dos conhecimentos acumulados, bem como o registro da História, de modo a limitar o avanço da Ciência (ROBINSON, 2016). Nessa perspectiva, a existência das civilizações teve por base a comunicação oral, já o seu desenvolvimento foi impulsionado pela comunicação escrita. Ambas as formas de comunicação propiciaram o surgimento da cultura e do patrimônio.

Observa-se que a cultura pode ser transmitida por meio da comunicação, assim, a experiência de um indivíduo é transmitido aos demais, criando ciclo de acumulação interminável (LARAIA, 2001). Sendo assim, a cultura consiste no conjunto de traços materiais e imateriais capazes de caracterizar e identificar uma sociedade (DIAS, 2012).

Com o surgimento da escrita, a memória se separa dos indivíduos, sendo considerada como uma mnemotécnica, e começa a ser disponibilizada para consultas e comparações. Trata-se de uma memória objetiva, impessoal, vindo a constituir uma verdade independente dos sujeitos. Desta forma, o conhecimento é separado da identidade pessoal, seja do indivíduo ou da comunidade. O conhecimento deixa de ser aquilo que é útil no dia a dia, e passa a ser aquilo que está registrado, tornando-se suscetível à avaliação e formalização. A escrita tenta representar a memória social por intermédio de uma rede de signos, a qual lhe confere um significado (LÉVY, 2010).

A memória cultural não oferece a exatidão histórica, mesmo assim, é valorizada em virtude de sua capacidade de relacionar passado e presente (HEDSTROM, 2016). Destaca-se que a preservação do patrimônio cultural se relaciona com a preservação da memória social, ou seja, saberes, fazeres, comportamentos e experiências que são derivados de uma série de objetos e registros, que foram produzidos conforme a evolução da sociedade (BELLOTTO, 2014). Em linhas gerais, a memória evoca fatos e atos que permitem a "construção" do saber histórico, por meio da análise crítica das fontes, bem como a sua transmissão para as gerações seguintes.

Atualmente, os documentos custodiados pelos Arquivos integram com o patrimônio cultural brasileiro, além de possuírem tutela jurídica, conforme ressaltado pelo artigo nº 216 da Constituição Federal de 1988:

> Art. 216 Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:
> I - as formas de expressão;
> II - os modos de criar, fazer e viver;
> III - as criações científicas, artísticas e tecnológicas;
> IV - as obras, objetos, documentos, edificações e demais espaços destinados às manifestações artístico-culturais;
> V - os conjuntos urbanos e sítios de valor histórico, paisagístico, artístico, arqueológico, paleontológico, ecológico e científico (BRASIL, 1988).

A Constituição Federal inicia uma preocupação com a preservação dos documentos, embora não explicite se estes registros são arquivísticos, biblioteconômicos ou museológicos, ressalta-se sua importância como um marco na preservação do patrimônio documental. Sendo assim, dentre os objetos do patrimônio histórico e cultural, está o documento arquivístico:

> O documento arquivístico nasce como resultado do cumprimento de uma atividade e é mantido como prova dela. E, também, com o objetivo de decidir, de agir e controlar as decisões e as ações empreendidas e, ainda, para efetuar pesquisas retrospectivas que ponham em evidência decisões ou ações passadas. Isso reduz a incerteza e torna a tomada de decisões mais segura, a partir do aprofundamento do conhecimento da cultura institucional e do processo decisório (SOUSA, 2009, p. 144).

Observa-se que o documento arquivístico possui um valor imediato, de modo que é produzido para apoiar funções e atividades da administração. Após o

cumprimento desse valor, os documentos arquivísticos são guardados em virtude do seu valor histórico, social, probatório e informativo. Esse valor adquirido de forma não intencional é denominado valor mediato, e determinante para que os documentos sejam escolhidos para preservação em caráter permanente.

Os documentos dotados de valor permanente constituem o patrimônio arquivístico. Trata-se de um conjunto de arquivos (públicos ou privados) que são acumulados no âmbito da esfera pública (CAMARGO; BELLOTTO, 2012). Os documentos preservados por estes arquivos podem possuir valor histórico e informativo, fatos que despertam o interesse social e motivam a sua preservação. Tradicionalmente os documentos foram produzidos apenas em suportes analógicos, como, por exemplo, o papel. Todavia a evolução das tecnologias da informação proporcionou o advento do documento arquivístico digital.

Os documentos digitais consistem em sequências de *bits* produzidas e acessadas com o uso de equipamentos computacionais e sistemas de *software* (BODÊ, 2016). Dessa forma, as informações produzidas no decorrer das funções e atividades de uma organização são registradas em suportes digitais, como, por exemplo, *Compact Disc* (CD), *Digital Versatile Disc* (DVD) e *Hard Disk* (HD).

Diante do avanço das tecnologias da informação, o documento arquivístico se transformou de objeto físico para objeto conceitual, de modo que passou a ser controlado por metadados que relacionam seu conteúdo, contexto e estrutura (FONSECA, 2005). Esse processo de ressignificação da Arquivística se faz necessário para que os documentos produzidos e armazenados em ambiente digital possam servir como fontes de informações confiáveis. Portanto, os conceitos tradicionais precisaram ser reformulados para contemplar as complexidades do ambiente digital e manter as especificidades do documento arquivístico. Logo, pode-se afirmar que o documento arquivístico digital consiste em uma inovação.

Destaca-se que as inovações podem ser basicamente classificadas em dois tipos essencialmente distintos: sustentada e disruptiva. As inovações sustentadas ajudam organizações a aprimorar seus produtos e serviços, de modo que podem ser negociados com maiores lucros. Dessa forma, os consumidores recebem o padrão de qualidade que foi historicamente definido pelo mercado (CHRISTENSEN; HORN; STAKER, 2013).

No entanto, com o aumento da produção de informações em formato digital, surgiram questionamentos com relação a sua preservação e garantida de acesso em longo prazo (ARELLANO, 2004). Isso demonstra que as tecnologias da informação não têm considerado as especificidades dos documentos arquivísticos, fato que resulta na dificuldade de preservá-los. Tal aspecto remete ao conceito de que os documentos digitais são produtos de uma inovação disruptiva.

> As inovações disruptivas, por sua vez, não procuram trazer produtos melhores para clientes existentes em mercados estabelecidos. Em vez disso, elas oferecem uma nova definição do que é bom — assumindo normalmente a forma de produtos mais simples, mais convenientes e mais baratos que atraem clientes novos ou menos exigentes. Com o tempo, elas se aperfeiçoam o suficiente para que possam atender às necessidades de clientes mais exigentes, transformando um setor (CHRISTENSEN; HORN; STAKER, 2013, p.2).

Dessa forma, apesar de significativos investimentos em tecnologia da informação, há uma crescente vulnerabilidade estrutural dos sistemas informatizados. Tais entraves ameaçam a preservação e o acesso contínuo no longo prazo, de modo que os documentos podem ser facilmente alterados ou excluídos, sem deixar vestígios aparentes que comprovem tais ações (CONSELHO NACIONAL DE ARQUIVOS, 2005).

Os mecanismos para manter a autenticidade não acompanharam a evolução das tecnologias. Esse fato eleva as vulnerabilidades dos documentos arquivísticos digitais, além de impactar diretamente em sua credibilidade enquanto fonte de prova (FLORES; ROCCO; SANTOS, 2016). Portanto, os sistemas informatizados requerem adaptações a fim de comportar as complexidades dos documentos digitais e as especificidades da disciplina Arquivística.

Há de se destacar que as inovações sustentáveis são melhores que as disruptivas, de modo que são vitais para setores saudáveis e sedimentados. Com isso, as organizações buscam a melhoria contínua de seus produtos e serviços (CHRISTENSEN; HORN; STAKER, 2013).

Assim, pondera-se que a transformação digital realizada no âmbito dos arquivos é disruptiva, pois não considerou a autenticidade dos documentos e nem princípios arquivísticos como: proveniência, unicidade, organicidade, naturalidade e indivisibilidade. Logo, é preciso agregar segurança à custódia documental por meio de sistemas informatizados que considerem tais especificidades.

4 CUSTÓDIA E CICLO DE VIDA DOS DOCUMENTOS ARQUIVÍSTICOS

Após serem produzidos no âmbito administrativo, os documentos arquivísticos têm um ciclo de vida no qual eles perpassam as fases: arquivo corrente, arquivo intermediário e arquivo permanente. Essa divisão é motivada pela frequência de uso, de modo que os documentos em fase corrente são frequentemente consultados.

Assim, quando sua demanda diminui são transferidos ao arquivo intermediário, e após serem avaliados, os documentos considerados de “interesse social” (MACNEIL, 2016) são recolhidos ao arquivo permanente. Os demais documentos, que não possuem interesse social e nem valor probatório são devidamente eliminados tendo em vista a eficiência administrativa.

> A razão de ser do arquivar e dos arquivos era atender aos interesses do Direito, da Administração e da História. As discussões contemporâneas ligam os objetivos dos arquivos e o papel das instituições arquivísticas a necessidades e interesses sociais definidos de forma mais ampla e giram em torno de questões relacionadas à responsabilidade, à identidade, à inclusão e à justiça social. A noção de arquivo como "arsenal para responsabilidade" e como "lugar de memória coletiva" inclui essa perspectiva mais ampla (MACNEIL, 2016, p. 8).

Para sustentar tal relevância jurídica, burocrática e social, é preciso proteger os arquivos, de modo a impedir a destruição de documentos, adulterações, inclusões indevidas, dentre outras. Para tanto, deve-se manter uma linha de custódia ininterrupta que irá assegurar que o acervo está sendo protegido nos moldes da disciplina Arquivística e em consonância com a legislação vigente.

Independente de serem documentos arquivísticos analógicos ou digitais deve-se constituir um ambiente confiável, de modo que os métodos empregados possam garantir a sua autenticidade. Ressalta-se que no caso dos documentos arquivísticos digitais, surgem entraves decorrentes de sua natureza digital, fato que reforça a ressignificação de conceitos tradicionais, como, por exemplo, autenticidade e custódia.

4.1 Autenticidade e confiabilidade

Há significativos desafios em relação aos documentos arquivísticos digitais, dentre eles, produzir documentos confiáveis, manter a sua autenticidade e garantir

acesso contínuo no longo prazo (ROCHA; SILVA, 2007). Ressalta-se que os documentos arquivísticos em suportes digitais não possuem a estabilidade equivalente àqueles registrados em suportes analógicos (ARELLANO; ANDRADE, 2006). Portanto, é preciso implementar mecanismos para demonstrar que seria impossível modificar ou excluir documentos digitais sem que tais ações fossem identificadas (DURANTI; PRESTON, [2007a]).

No entanto, a preservação digital requer ações para garantir o acesso, logo, os critérios para presumir a autenticidade variam conforme a natureza dos documentos (THIBODEAU, 2002). Portanto, permitem-se escolher quais são as propriedades significativas, que caracterizam o documento digital e devem ser preservadas. Tais propriedades devem ser mencionadas em uma política de preservação, de modo que cada classe de documento terá suas peculiaridades a serem mantidas. Por exemplo, para um documento textual é fundamental manter o seu conteúdo escrito, já os efeitos de sombra e cores são questões secundárias.

Quando se considera a problemática da preservação digital sabe-se que em algum momento será preciso executar estratégias, como migrações e conversões, o que torna inviável a ideia de manter os documentos digitais inalteráveis. O nível de alteração aqui permitido reserva-se às ações necessárias para manter a integridade e o acesso em longo prazo. Portanto, será preciso implementar mecanismos de controle para manter um histórico que registre todas as alterações realizadas, de modo que possa corroborar com a presunção de autenticidade no longo prazo.

> A autenticidade é configurada por uma série de elementos que caracterizam a confiabilidade e a fixidez de um documento. Para que um documento se torne autêntico, precisa ser custodiado por uma instituição responsável e possuir elementos que garantam sua estrutura diplomática, tais como autoria, data, e outros elementos de documentos confiáveis. São estes elementos que validam o documento e concretizam a autenticidade e a veracidade dele, tornando-o confiável (LUZ; FLORES, 2018, p. 174).

No Brasil, tem-se implementado a assinatura digital, entretanto, ela não é efetiva no longo prazo, justamente pelo fato de que os documentos necessitam ser migrados para novos formatos de arquivo para que continuem acessíveis. Ou seja, não é possível migrar as assinaturas digitais juntamente com os documentos (CONSELHO NACIONAL DE ARQUIVOS, 2012).

As assinaturas digitais não garantem autenticidade no longo prazo, somente integridade e o não repúdio. Todavia, suas limitações podem ser mitigadas por meio de um sistema informatizado capaz de atribuir um identificador único aos documentos, que será atualizado juntamente no momento da conversão.

A fim de corroborar com a autenticidade, os documentos arquivísticos digitais precisam ser produzidos em um ambiente confiável. Dessa forma, a confiabilidade consiste em sustentar os atos e os fatos que os documentos atestam, garantindo que foram produzidos por indivíduos que possuem competência para tal. Ademais, deve-se considerar a manutenção da integridade e o grau de controle exercido no processo de produção (CONSELHO NACIONAL DE ARQUIVOS, 2012; VOUTSSÁS MARQUEZ; AMOZORRUTIA, 2014).

Ressalta-se que a confiabilidade depende do ambiente em que os documentos são produzidos e custodiados. Logo, é preciso definir políticas organizacionais de gestão e preservação para implementar os sistemas informatizados *a posteriori*, capazes de comprovar que os documentos permanecem autênticos no longo prazo.

4.2 Cadeia de custódia e cadeia de preservação

De acordo com a teoria tradicional, a disciplina Arquivística atribui presunção de autenticidade aos documentos considerados confiáveis por seus produtores. Todavia, com o advento dos sistemas informatizados, a presunção de autenticidade deverá ser sustentada por evidências de que as propriedades significativas dos documentos digitais não foram modificadas ou corrompidas durante sua transmissão (DURANTI, 2005).

A custódia está relacionada à transmissão dos arquivos, entre produtores, conforme as mudanças nas estruturas administrativas. Ao fim desse ciclo, a responsabilidade pela custódia irá chegar ao arquivista, que terá de preservar os documentos. Dessa forma, os produtores e o arquivista mantém uma linha idônea de responsabilidades, composta por sucessores legítimos (SILVA, 2017).

Nessa perspectiva, a autenticidade está condicionada aos métodos empregados na produção, gestão, preservação e custódia dos documentos arquivísticos, ou seja, durante todo o ciclo de vida. Quaisquer interrupções dessa

cadeia irão colocar o acervo em risco, de modo que poderá ocorrer eliminação indevida de documentos, furtos, alterações e até mesmo inclusão de documentos falsificados.

> O conceito de custódia arquivística está intrinsecamente ligado à proteção e guarda da prova. A posse física dos registros é apenas um dos meios pelos quais, historicamente, os arquivistas têm garantido essa proteção. As novas tecnologias da informação e as condições específicas que elas produzem não alteram a substância da responsabilidade custodial dos arquivistas: eles poderiam apenas mudar um dos meios pelos quais a exercem. Os arquivistas não precisam ter a custódia física dos registros eletrônicos para exercer o controle sobre eles e proteger sua integridade: eles podem fazer isso à distância, contanto que detenham autoridade legal para essa função (DURANTI, 1994, p. 62).

Se a cadeia de custódia for interrompida, cria-se um lapso temporal, onde não houve proteção, fato que poderá criar dúvidas com relação à autenticidade dos documentos (CONSELHO NACIONAL DE ARQUIVOS, 2012). Ao ser observada, pelo prisma jurídico, a cadeia de custódia consiste no dispositivo que objetiva assegurar a integridade e a capacidade probatória, de modo que permita utilizar determinada evidência em juízo. Esse dispositivo contempla todo o caminho percorrido pelo elemento probatório, assegura a sua rastreabilidade, e consequentemente, lhe atribui credibilidade (EDINGER, 2016; MENEZES; BORRI; SOARES, 2018; PRADO, 2014).

Observa-se que os conceitos de cadeia de custódia advindos da Arquivística e do Direito são convergentes. De tal modo, a preservação de documentos digitais pode incorporar tais referenciais a fim de propor o fortalecimento do tema por meio de um diálogo interdisciplinar. Ademais, deve-se considerar a perspectiva da custódia compartilhada, entre os setores de arquivo e de informática, que remodela o conceito tradicional de custódia, pensada para documentos analógicos.

No âmbito dos arquivos, também existe uma cadeia de preservação que comporta elementos de políticas e metodologias para a gestão de documentos digitais (DURANTI; PRESTON, [2007a]). A cadeia de preservação deve começar na produção dos documentos arquivísticos digitais, de modo que os preservadores orientem os produtores (DURANTI; PRESTON, [2007b]).

Nesse sentido, os preservadores podem recomendar que os produtores utilizem determinados formatos de arquivo e padrões de metadados, de modo a facilitar a preservação digital. Assim, a cadeia de preservação se estende durante todo

o ciclo de vida dos documentos arquivísticos, visa a sua manutenção e garantia de acesso contínuo no longo prazo.

A cadeia de preservação se sustenta em uma série de procedimentos interdependentes ao gerenciamento dos documentos. Logo, a integridade dos documentos pode ser colocada em risco caso não sejam submetidos a determinado procedimento (DURANTI; PRESTON, [2007a]). Para tanto, a cadeia de preservação precisa estar em consonância com a legislação vigente, normas, metodologias e requisitos técnicos. Assim, poderá ser definida antes da implementação dos sistemas informatizados para gestão e preservação (FLORES; PRADEBON; CÉ, 2017).

Há de se ressaltar que a custódia e a preservação estão diretamente relacionadas, pois o material custodiado precisa de ações que visem a sua preservação e acesso no longo prazo. Para tanto, é preciso que tais ações sigam uma política de preservação que vislumbre a manutenção da autenticidade dos documentos (SILVA, 2019). O ciclo de vida dos documentos arquivísticos requer tratamento adequado para gerar confiança contínua, tais aspectos demonstram a relação de interdependência entre a cadeia de custódia e a cadeia de preservação (VOUTSSÁS MÁRQUEZ, 2010).

Tal interdependência entre as cadeias pode ser observada por suas ações são convergentes e complementares, de modo que a ruptura de uma cadeia inviabiliza as atividades da outra. Logo, a responsabilidade pela custódia implica no dever de preservar e promover o acesso à informação.

5 ELEMENTOS DE UMA CADEIA DE CUSTÓDIA DIGITAL ARQUIVÍSTICA

As práticas de gestão, preservação e acesso são tradicionalmente orientadas aos documentos analógicos. Quando se pensa em documentos arquivísticos em ambientes digitais, torna-se necessário ressignificar tais conceitos. Essa reformulação requer unir as abordagens da cadeia de custódia e da cadeia de preservação, criando assim, uma cadeia de custódia arquivística pensada para comportar o ciclo de vida dos documentos digitais.

5.1 Ambientes para gestão, preservação e acesso

A gestão de documentos consiste no conjunto de medidas e rotinas que visam a eficiência e a racionalização no uso primário dos documentos. Dentre as sete funções arquivísticas (produção, aquisição, classificação, avaliação, conservação, descrição e difusão), a gestão de documentos concentra-se nas quatro primeiras (CAMARGO; BELLOTTO, 2012; HERRERA, 1998). Entretanto, isso não impede que as demais funções arquivística sejam executadas já na fase corrente, aliás, do ponto de vista das cadeias de preservação e custódia, é recomendável.

Com o advento dos documentos arquivísticos digitais percebeu-se a necessidade de uma intervenção arquivística na concepção dos sistemas informatizados (RONDINELLI, 2005). O diálogo entre os profissionais do arquivo e da informática permite a implementação dos requisitos necessários para manter elementos como, por exemplo, a autenticidade e as cadeias de custódia e preservação.

Destaca-se que a gestão de documentos arquivísticos digitais depende diretamente dos sistemas informatizados, imputados da tarefa de controlar o ciclo de vida, assegurar a autenticidade e manter princípios como: organicidade, unicidade e proveniência. Tais requisitos devem ser considerados pelos sistemas que produzem e armazenam os documentos (SILVA, 2017).

Nessa perspectiva, recomenda-se o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil) a fim de implementar sistemas para gestão de documentos. O e-Arq Brasil consiste em um conjunto de requisitos para assegurar a confiabilidade do sistema informatizado e garantir o acesso aos documentos. Logo, define os requisitos essenciais para implementar um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), sem depender de plataformas tecnológicas específicas (CONSELHO NACIONAL DE ARQUIVOS, 2011).

Sendo assim, o SIGAD comporta o conjunto de procedimentos e técnicas para realizar a gestão arquivística dos documentos. Poderá ser um *software* específico ou um conjunto de *softwares* que operam em conjunto. Ressalta-se que o êxito do SIGAD dependerá da definição, prévia e adequada, das políticas de gestão arquivística (CONSELHO NACIONAL DE ARQUIVOS, 2011). A versão vigente do e-Arq Brasil é

datada do ano de 2011, acredita-se que precisa ser atualizado para melhor refletir os avanços recentes da pesquisa em documentos digitais, principalmente no que tange aos repositórios arquivísticos e a cadeia de custódia.

Fica expresso que o SIGAD será responsável pela gestão de documentos em arquivos correntes e intermediários, de modo que irá coordenar atividades como, por exemplo, classificação, avaliação e transferência/recolhimento ao arquivo permanente. Ademais, o SIGAD pode ser implementado de forma interoperável com os sistemas de negócio da organização, fato que facilita a captura/transferências de documentos arquivísticos.

A interoperabilidade pode ser entendida como a capacidade de sistemas diferentes operarem em conjunto para executar determinadas tarefas. Tal característica pode ser obtida por meio de acordos nos quais as partes se comprometem com o uso de padrões tecnológicos específicos (MARCONDES, 2016). Dessa forma, é possível interligar os sistemas para gestão, preservação e acesso, de modo que os documentos custodiados seguem padrões compatíveis, como, por exemplo, os formatos de arquivo e as estruturas de metadados.

> A necessidade de interoperabilizar a informação é básica para os tempos de comunicação em rede. A interoperabilidade garante o uso e a encontrabilidade dos metadados estruturados dos objetos informacionais. As formas de estruturar a informação arquivística, aquela referente aos acervos documentais disponíveis digitalmente, não é obrigatoriamente padronizada. Isso representa que cada serviço informacional, ou unidade de tratamento documental (um serviço de arquivo, por exemplo), pode definir a forma como vai estruturar este tipo de informação, gerando suas específicas políticas de interoperabilidade e de descrição, além do seu próprio padrão de metadados (LUZ, 2016, p. 29-30).

Deve-se ressaltar que a cooperação entre produtores e preservadores, no que tange a implementação de padrões e formatos comuns, possibilita a reutilização dos metadados. Tal padronização torna os documentos interoperáveis para outros sistemas, e permite a sustentabilidade do acervo no longo prazo (CAMPOS; SARAMAGO, 2007). Portanto, os padrões de metadados requeridos no ambiente de gestão, pelo SIGAD, devem manter consonância com os do Arquivo Permanente Digital, doravante, Repositório Arquivístico Digital Confiável (RDC-Arq).

Nessa perspectiva o RDC-Arq é responsável por armazenar e gerenciar os documentos em fase permanente. Há casos excepcionais em que poderá ser utilizado para documentos nas fases corrente e intermediária, principalmente quando se

tratarem de documentos complexos ou sigilosos. Destaca-se que o RDC-Arq deve gerenciar documentos e metadados conforme as práticas e as normas da Arquivologia, além de proteger características do documento arquivístico, como, por exemplo, a autenticidade, a proveniência e a organicidade (CONSELHO NACIONAL DE ARQUIVOS, 2015).

Um RDC-Arq deve realizar a organização hierárquica dos documentos arquivísticos digitais, tomando por base o plano de classificação e as normas para descrição multinível (CONSELHO NACIONAL DE ARQUIVOS, 2015). Além dos requisitos arquivísticos, o RDC-Arq deve manter conformidade com o modelo *Open Archival Information System* (OAIS), que se tornou a norma *International Organization for Standardization* (ISO) 14721:2012, considerada a principal referência na preservação digital.

Há uma tradução no Brasil, realizada pela Associação Brasileira de Normas Técnicas (ABNT), como Norma Brasileira Recomendada (NBR), tornando-se ABNT/NBR 15472:2007, Sistema Aberto de Arquivamento de Informação (SAAI). No entanto essa tradução carece de atualização, tendo em vista que a versão atual do OAIS foi publicada em 2012.

O modelo OAIS/SAAI propõe um conjunto de funções para preservar documentos e informações relacionadas, de modo que é responsável por questões como: admissão, armazenamento arquivístico, gerenciamento de dados, planejamento da preservação, administração do ambiente, acesso e disseminação. Ademais, o OAIS discorre sobre a migração para novos formatos de arquivo e suportes, bem como, define um modelo para representar as informações arquivadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2007; THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2012; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012a).

Dessa forma, o ambiente de preservação consiste em um RDC-Arq que mantêm conformidade com o modelo OAIS. Logo, será possível contornar as complexidades e as especificidades dos documentos arquivísticos digitais tendo em vista a sua preservação e acesso no longo prazo com garantia de autenticidade. Neste ponto, destaca-se a obsolescência tecnológica como um dos principais entraves para a efetividade da preservação digital.

A obsolescência tecnológica se manifesta em nível de *hardware*, *software* e suporte. Conforme a evolução do *software*, os formatos de arquivo que ele produz também sofrem transformações, fato que dificulta a correta interpretação do documento (FERREIRA, 2006). Portanto, durante o ciclo de vida dos documentos será necessário implementar uma série de estratégias de preservação para mitigar os efeitos da obsolescência tecnológica.

As estratégias tratam-se de intervenções com objetivo de garantir a preservação e o acesso aos documentos. Há diversas estratégias com foco direcionado para preservar determinado nível dos documentos digitais. O refrescamento concentra-se na preservação do suporte. A preservação de tecnologia, a emulação e o encapsulamento preservam a integridade da cadeia de *bits*. Já a migração concentra-se em preservar a representação. No entanto, nenhuma estratégia tem sido capaz de solucionar todos os problemas da obsolescência tecnológica, de forma isolada. Cada uma possui vantagens e desvantagens, logo, devem ser implementadas em conjunto (FERREIRA, 2006; ARELLANO, 2004; THIBODEAU, 2002).

A preservação e o acesso requerem o monitoramento dos suportes e dos formatos de arquivo, para que assim, possam ser implementadas as estratégias de preservação necessárias (ROCHA; SILVA, 2007). Contudo, tais ações devem ser proferidas no âmbito do RDC-Arq, em consonância com políticas de preservação definidas *a priori*. Dessa forma, é possível controlar e registrar a ações, por meio de uma estrutura de metadados, e assegurar a presunção de autenticidade. Ademais, com a definição dessas políticas é possível monitorar questões como:

> A evolução das plataformas tecnológicas de *hardware* e *software*; os formatos de arquivo; os padrões de metadados; as mídias de armazenamento; as normas; a legislação; e as recomendações técnicas. Além disso, é preciso que o RDC-Arq tenha um plano de sucessão caso, por algum motivo, encerre suas atividades de preservação. O plano de sucessão é a garantia de que os esforços em preservação serão continuados, na ausência dele, qualquer interrupção dos serviços do RDC-Arq será o suficiente para questionar a autenticidade dos documentos custodiados (SANTOS; FLORES, 2019, p. 129).

As políticas de preservação precisam especificar questões como: os procedimentos para escolha das estratégias; os *softwares* que serão utilizados para implementar o RDC-Arq; os formatos de arquivo adequados para preservação; e os padrões de metadados. As tecnologias devem estar subordinadas às políticas

organizacionais. Portanto, os sistemas informatizados devem ser adaptados para comportar os requisitos e princípios preconizados pela disciplina Arquivística (SANTOS; FLORES, 2015).

Observa-se que além de preservar os documentos com garantia de autenticidade, o RDC-Arq deverá promover o acesso. Para tanto precisa disponibilizá-los em formatos de arquivo amplamente utilizados, que possam ser corretamente interpretados pelos consumidores por meio de tecnologias simples, sem a necessidade de equipamentos sofisticados. Essa perspectiva de acesso corrobora com o disposto na Lei 12.527/2011, Lei de Acesso à Informação (LAI), válida aos três Poderes da União, Estados, Distrito Federal, Municípios e entidades privadas sem fins lucrativos que recebem ou destinam recursos ao poder público.

Para atender a LAI, as organizações devem disponibilizar os seguintes itens em seus *sites*: ferramentas para pesquisa; relatórios em formatos de arquivo abertos e não proprietários; acesso por meio de sistemas; especificar o método no qual a informação é estruturada; assegurar a autenticidade; manter as informações atualizadas; indicar seus canais de comunicação; e ter mecanismos que garantam a acessibilidade (BRASIL, 2011).

Destaca-se que a LAI rompe com a cultura do sigilo, preconizando a cultura do acesso, ou seja, o acesso é a regra geral e o sigilo passa a ser a exceção. Com isso, surge a necessidade de definir políticas e implementar sistemas para se adequar as novas exigências.

Sendo assim, o RDC-Arq tem as atribuições de preservar, manter a autenticidade e garantir o acesso. Para tanto, necessita desenvolver um ambiente confiável, capaz de satisfazer as complexidades advindas dos avanços das tecnologias, bem como, manter conformidade com os princípios arquivísticos (organicidade, proveniência, unicidade, naturalidade e indivisibilidade). Logo, o estágio do RDC-Arq poderá ser avaliado por meio de auditorias periódicas, que visam determinar a evolução dos seus níveis de confiabilidade.

A auditoria é um processo sistemático e independente, que utiliza um conjunto de critérios para obter evidências objetivas que irão sustentar a existência ou veracidade de determinados fatos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018). Está relacionada às atividades de controle e tem por objetivo identificar funções e atividades realizadas em determinado período. Com isso, é

possível verificar o nível de adequação dos comportamentos no ambiente organizacional (BATISTA; OLIVEIRA, 2019).

Com as auditorias é possível compreender a eficiência do sistema, verificar se está satisfazendo os interesses da comunidade designada, e caso necessário, promover modificações nos serviços prestados. Ademais, o processo de auditoria permite avaliar questões como: os recursos disponíveis, a equipe, os componentes do sistema e o gerenciamento de documentos. Assim, além de identificar os problemas organizacionais, irá auxiliar na busca por soluções (DÍAZ; MUGICA; GUEVARA, 2019).

A auditoria do RDC-Arq poderá ser realizada por meio do padrão *Audit and Certification of Trustworthy Digital Repositories* (ACTDR), o qual se tornou a ISO 16363:2012. Os critérios utilizados por esse padrão concentram-se em avaliar: a infraestrutura organizacional; a gestão de objetos digitais; e a infraestrutura de segurança.

Com a ISO 16363:2012 é possível desenvolver um processo de melhoria contínua que não deve seguir uma lógica binária de sim ou não (confiável ou não confiável). Dessa forma, a análise irá apontar as áreas do RDC-Arq que precisam ser melhoradas para elevar os níveis de confiabilidade (THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS, 2011; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012b). Assim, o RDC-Arq evolui de forma contínua, especialmente quando considera as auditorias, pois permitem solucionar diversos problemas técnicos em sua infraestrutura (REZENDE; CRUZ-RIASCOS; HOTT, 2017).

O processo de auditoria com a ISO 16363:2012 irá verificar a conformidade do RDC-Arq com o modelo de referência OAIS. Caso obtenha êxito, poderá ser submetido à certificação, para que assim, o RDC-Arq seja denominado de “confiável”. Há de se ressaltar que tanto a auditoria, quanto a certificação devem ser periódicas, a fim de comprovar que o RDC-Arq mantém-se confiável ao longo do tempo.

5.2 Custódia ininterrupta: uma abordagem holístico-sistêmica

Tradicionalmente, a cadeia de custódia consiste em uma linha ininterrupta que perpassa todo o ciclo de vida dos documentos. Esse princípio estipula que os

documentos devem estar sob a custódia de partes conhecidas e consideradas confiáveis, para mantê-los intactos (JENKINSON, 1922). Entretanto, o conceito tradicional de cadeia de custódia não é suficiente para os documentos digitais, pois foi pensado para documentos analógicos. Sendo assim, não há como presumir a autenticidade caso um Arquivo receba transferência ou recolhimento por meio do envio de CDs, DVDs, HDs, dentre outras mídias, apenas considerando a custódia física dos suportes.

A posse dos documentos analógicos por parte dos seus responsáveis legais era suficiente para manter custódia, porém manter a posse dos documentos digitais não é suficiente para presumir a sua autenticidade. Logo, a custódia confiável para documentos digitais requer a possibilidade de criar “rastros digitais”, equivalentes aos vestígios de adulteração em documentos analógicos. Esses “rastros” podem ser produzidos por meio de trilhas de auditoria e metadados que registram a data e o indivíduo que proferiu alterações sobre os documentos arquivísticos digitais custodiados.

Nessa perspectiva, as ações de implementar um SIGAD nos moldes do e-Arq, e um RDC-Arq seguindo o OAIS, tornam-se fundamentais para atender a legislação vigente. Destaca-se o artigo 25 da Lei nº 8.159/1991, que dispõe sobre as responsabilidades (penal, civil e administrativa) para aquele que desfigurar ou destruir documentos arquivísticos de valor permanente, de interesse público e social (BRASIL, 1991).

Observa-se que a Lei nº 8.159/1991 foi pensada para documentos analógicos, no entanto, a adesão aos documentos digitais tem forçado a discussão em torno da capacidade probatória desses documentos. Portanto, acredita-se que o valor agregado e a dependência por documentos e informações digitais possam a gerar novas discussões, especialmente no que tange a sua confiabilidade.

Há de destacar a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais, incluindo os digitais. A lei exige que os profissionais da informação realizem a manutenção dos dados, além de garantir o sigilo e a segurança (BRASIL, 2018).

Sendo assim, a Lei nº 8.159/1991, a LAI e a LGPD despertam a atenção para a importância da correta gestão e preservação de documentos, inclusive os digitais. Logo, destaca-se a pertinência de manter uma cadeia de custódia confiável e

ininterrupta entre o SIGAD e o RDC-Arq. Com isso, estima-se assegurar a confidencialidade e o sigilo das informações sensíveis, bem como, promover o acesso às informações de interesse público.

Quando se considera a problemática dos documentos arquivísticos digitais, é preciso pensar em procedimentos para preservá-los, garantir a autenticidade e o acesso em todas as etapas do seu ciclo de vida. Para tanto, é preciso implementar uma política de preservação digital que vislumbre a manutenção de um ambiente confiável (ROCHA; SILVA, 2007).

Ressalta-se que o preservador deverá demonstrar que não tem interesses em adulterar ou permitir que outros adulterem tais documentos. Ademais, para ser considerado um custodiador confiável, o preservador também precisa ser capaz de implementar os requisitos de preservação necessários, bem como manter uma linha de custódia ininterrupta (DURANTI; PRESTON, [2007b]).

A responsabilidade por custodiar os documentos, bem como planejar, implementar e manter o SIGAD e o RDC-Arq deve ser compartilhada entre os profissionais de arquivo e de tecnologia da informação. Esse diálogo possibilita desenvolver sistemas que atentem para as complexidades tecnológicas e as especificidades da Arquivística (CONSELHO NACIONAL DE ARQUIVOS, 2015).

Tendo em vista a necessidade de ressignificação da tradicional cadeia de custódia, para assegurar a autenticidade dos documentos, chega-se a uma ruptura paradigmática: a Cadeia de Custódia Digital Arquivística (CCDA). Trata-se de uma linha ininterrupta que contempla desde a produção dos documentos arquivísticos digitais, e sua captura pelo SIGAD; essa linha se estenderá até a eliminação segura ou guarda permanente, por meio do RDC-Arq. Todas essas etapas devem assegurar a presunção de autenticidade e promover o acesso à informação.

Reitera-se que a CCDA segue regida pelas referências tradicionais, de modo que ainda é entendida como: a sucessão encadeada de pessoas que tiveram contato com a fonte probatória (BADARÓ, 2017), de modo que há um conjunto de procedimentos para documentar a história cronológica da prova em si (BRASIL, 2019). Dessa forma, a cadeia de custódia torna-se ainda mais relevante para os documentos digitais, em virtude da facilidade de serem alterados sem deixar vestígios salientes (STOPANOVSKI, 2015). Ademais, Badaró (2017) destaca que é fundamental o registro da custódia:

> O que não pode ser pode ser confundido com a cadeia de custódia em si. O procedimento de documentação da cadeia de custódia que assegura a autenticidade e a integridade da fonte de da cadeia de custódia que assegura a autenticidade e a integridade da fonte de prova. A autenticidade significa que a fonte de prova é genuína, autêntica quanto à sua origem (BADARÓ, 2017, p. 525).

Considerando a convergência entre os conceitos tradicionais e emergentes da cadeia de custódia, a CCDA consiste em um princípio aplicável aos documentos arquivísticos em ambientes digitais, que considera as suas complexidades e especificidades. Dessa forma, garante que tais documentos estão protegidos pelo custodiador de forma ininterrupta, desde a produção/captura, perpassando assim, a tramitação, o arquivamento, a eliminação segura ou guarda permanente, até o acesso.

Esse monitoramento contínuo trata-se de uma visão holística, e significa que o documento arquivístico recebe tratamento adequado ao longo de todo o seu ciclo de vida. Dessa forma, os documentos podem ser produzidos em formatos de arquivo recomendados para preservação, ou podem ser convertidos para tais formatos ainda durante a fase de gestão. Logo, não é preciso esperar que os documentos cheguem à fase permanente para se preocupar com a sua preservação, autenticidade e acesso em longo prazo.

Contudo, é elementar que a cadeia de custódia seja devidamente documentada, do contrário, a autenticidade de quaisquer elementos de prova que forem extraídos poderá ser questionada (BADARÓ, 2017). Quando abordada na perspectiva da CCDA, faz-se necessário o registro de todas as alterações proferidas sobre os documentos. Tais questões são motivadas pelas vulnerabilidades implícitas da natureza digital e requerem uma abordagem sistêmica, pautada em padrões sedimentados na literatura técnica da preservação digital.

A preservação digital sistêmica concentra-se no gerenciamento por meio de sistemas informatizados que sigam padrões. Assim, as estratégias (migração, emulação, e outras) passam a ser executadas em um ambiente confiável que irá registrar todas as ações realizadas. A obsolescência tecnológica e a facilidade de adulteração dos documentos digitais reiteram a necessidade de sistemas como o SIGAD e o RDC-Arq, para envolver o ciclo de vida dos documentos em uma CCDA. Todavia, a efetividade de suas ações está condicionada a sua capacidade de interoperar.

Os níveis de interoperabilidade podem ser elevados ao se preferir o uso de “padrões abertos” em vez de “padrões proprietários”. Dessa forma, é possível reduzir a aplicação de estratégias, como, por exemplo, a conversão (VOUTSSÁS MÁRQUEZ, 2009). Igualmente, os sistemas informatizados devem ser desenvolvidos com a capacidade de interoperar, mantendo consonância com os padrões recomendados na literatura.

Ao considerar o caso dos processos judiciais eletrônicos, observa-se que ainda não recebem tratamento arquivístico adequado, nos moldes da preservação digital sistêmica (BÖTTCHER, 2020). Nesse sentido, o Conselho Nacional de Justiça (CNJ) em sua Resolução nº 324 (CONSELHO NACIONAL DE JUSTIÇA, 2020), reafirma a necessidade do uso de sistemas informatizados para produzir documentos arquivísticos capazes de atender os requisitos de autenticidade, então definidos pelo Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus), que tem entre seus fundamentos, o e-Arq Brasil (CONSELHO NACIONAL DE JUSTIÇA, 2009).

Logo, o Moreq-Jus define requisitos para produzir, receber, tramitar, armazenar e preservar os documentos, sejam eles digitais, analógicos ou híbridos. Tais requisitos também se aplicam aos sistemas de gestão de processos e tem por objetivo garantir a confiabilidade, a autenticidade e o acesso. Ademais, o Moreq-Jus estabelece processos e requisitos necessários ao Sistema Informatizado de Gestão de Processos e Documentos (GestãoDoc), equivalente ao SIGAD (CONSELHO NACIONAL DE JUSTIÇA, 2009).

> A Gestão Documental, decorrente de mandamento constitucional, existe para assegurar o acesso à informação e a integridade dos documentos para o exercício de direitos pelo cidadão durante o tempo necessário para tal. Também existe para garantir a preservação dos documentos históricos, que fazem parte do Patrimônio Cultural nacional (BÖTTCHER, 2020, p. 1).

É preciso considerar ainda o fator da segurança jurídica, condição que proporciona aos indivíduos a certeza de que as relações estabelecidas diante de um contexto legal serão mantidas mesmo após a alteração desse contexto (SILVA, 2009). Assim, observa-se que a correta e adequada gestão arquivísticos propicia a segurança jurídica, tendo em vista que preconiza um ambiente confiável para proteger os documentos de quaisquer adulterações que possam ferir, por exemplo, algum direito adquirido.

Tendo em vista o exposto, percebe-se que a abordagem da preservação digital sistêmico-holística é pautada no uso de sistemas que seguem padrões, e incorporam todo o ciclo de vida dos documentos em uma CCDA. Esses elementos corroboram para validar o sistema de arquivos como fonte de prova, propiciando um ambiente de segurança jurídica, capaz de salvaguardar direitos e possibilitar o exercício da cidadania plena.

6 CONSIDERAÇÕES FINAIS

Este estudo discorreu sobre os aspectos tradicionais da cadeia de custódia, transpondo-os na perspectiva dos documentos arquivísticos digitais. Para tanto se sustentou nos referenciais da Arquivística e recorreu a conceitos advindos do Direito, tendo em vista a sua aplicabilidade.

A abordagem proposta perpassou a importância de preservar a memória, especialmente a documental, destacando sua relevância histórico-social e probatória. Diante disso, surge a preocupação com uma possível transformação digital disruptiva, ocasionada pelos desenfreados avanços da tecnologia e sua consequente adesão acrítica.

O cerne deste estudo foi pautado na manutenção da autenticidade dos documentos arquivísticos digitais. Para tanto, é necessário desenvolver um ambiente confiável para armazenar e proteger tais documentos. Ao fundamentar a cadeia de custódia e a cadeia de preservação, observou-se a relação de interdependência; fato que motivou uni-las e adaptá-las ao contexto digital por meio do conceito de CCDA.

As complexidades advindas do ambiente informático aliadas às especificidades da disciplina Arquivística requerem políticas e sistemas capazes de satisfazê-las. Logo, preconiza-se a implementação do SIGAD em conformidade com o e-Arq Brasil no ambiente de gestão; e do RDC-Arq em conformidade com o OAIS no ambiente de preservação.

Sendo assim, SIGAD e RDC-Arq devem ser envolvidos em uma CCDA, de modo que, nesse ambiente, todas as ações proferidas sobre os documentos arquivísticos digitais são devidamente registradas. Para tanto, faz-se necessário definir uma política de preservação digital que oriente a escolha de: padrões de

metadados, formatos de arquivo, estratégias de preservação, propriedades significativas, e demais componentes do sistema de arquivos.

A preservação digital passa a ser orientada por meio de sistemas que realizam o monitoramento das tendências de obsolescência para antecipá-las. Os procedimentos passam a seguir padrões recomendados pela literatura científica (preservação sistêmica), como, por exemplo, e-Arq Brasil, OAIS, ISO 16363, Moreq-Jus, dentre outros. Igualmente, a preservação começa a ser pensada durante todo o ciclo de vida dos documentos (visão holística), inclusive antes da concepção dos sistemas informatizados.

Observa-se que a CCDA é elementar para a presunção de autenticidade do documento arquivístico digital, de modo que este sirva como de fonte de prova, testemunho, memória, patrimônio e cidadania plena. Para o Direito, a abordagem da cadeia de custódia se expande, de modo que passa a lançar um olhar crítico com relação aos documentos digitais. Assim, deve-se ponderar sobre os possíveis riscos de insegurança jurídica que são proporcionados pela ausência das políticas de gestão e preservação de documentos digitais. Nessa perspectiva, a CCDA é o meio para desenvolver um ambiente confiável pautado na interdisciplinaridade entre a Arquivística e o Direito com objetivo de proteger a capacidade probatória dos documentos digitais e salvaguardar a memória coletiva.

Por fim, este estudo limitou-se a introduzir a abordagem da preservação digital holístico-sistêmica, a fim de facilitar a compreensão por parte dos pesquisadores recém-iniciados na temática. Destaca-se a importância de uma abordagem interdisciplinar que vislumbre a manutenção da autenticidade, proteção do sigilo, preservação e garantia de acesso contínuo à informação no longo prazo. Ademais, preconiza-se que a CCDA contribui para que a transformação digital seja uma inovação sustentável, e não disruptiva.

REFERÊNCIAS

ARELLANO, M. Á. M.; ANDRADE, R. S. Preservação digital e os profissionais da informação. **DataGramaZero**, Rio de Janeiro, v. 7, n. 5, 2006. Disponível em: http://ridi.ibict.br/bitstream/123456789/259/1/MIGUELDgz2006.pdf. Acesso em: 16 jul. 2020.

ARELLANO, M. Á. M. Preservação de documentos digitais, **Ciência da Informação**, Brasília, v. 33, n. 2, p. 15-27, 2004. Disponível em: http://revista.ibict.br/ciinf/article/view/1043. Acesso em: 16 jul. 2020.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 19011**: diretrizes para auditoria de sistemas de gestão. Rio de Janeiro: ABNT, 2018.

BADARÓ, G. A cadeia de custódia e sua relevância para a prova penal. *In*: SIDI, R.; LOPES, A. B. (org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido Ed., 2017. p. 517-538.

BATISTA, D. A.; OLIVEIRA, E. B. Auditoria arquivística: uma proposta de requisitos. **Informação & Sociedade: Estudos**, João Pessoa, v. 29, n. 1, p. 159-180, 2019. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/44006/22577. Acesso em: 16 jul. 2020.

BELLOTTO, H. L. Arquivo e sociedade: políticas e ações voltadas para a cultura e para a educação. *In*: BELLOTTO, H. L. **Arquivo**: estudos e reflexões. Belo Horizonte: Ed. UFMG, 2014. p. 132-143.

BODÊ, E. C. Documento digital e preservação digital: algumas considerações conceituais. **RICI: R.Ibero-amer. Ci. Inf.**, Brasília, v. 9, n. 2, p. 503-516, 2016. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/2425/2163. Acesso em: 16 jul. 2020.

BÖTTCHER, C. A. Resolução CNJ 324/2020: gestão documental e da memória do poder judiciário. **Consultor Jurídico**, São Paulo, 2020. Disponível em https://www.conjur.com.br/2020-mai-02/opiniao-dia-memoria-poder-judiciario-resolucao-cnj-3162020 . Acesso em: 16 jul. 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 jul. 2020.

BRASIL. **Lei, n°. 12.527, de 18 de novembro de 2011**. 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. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em: 16 jul. 2020.

BRASIL. **Lei nº. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 16 jul. 2020.

BRASIL. **Lei n°. 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 16 jul. 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. Brasília, DF: Presidência da República, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm. Acesso em: 16 jul. 2020.

CAMARGO, A. M. A.; BELLOTTO, H. L. **Dicionário de terminologia arquivística**. 3. ed. São Paulo: Associação dos Arquivistas Brasileiros, Núcleo Regional de São Paulo, 2012.

CAMPOS, F. M. G.; SARAMAGO, M. L. Preservação digital de longo prazo em instituições patrimoniais: reutilização e adaptação de metadados. **Actas dos Congressos Nacionais de Bibliotecários, Arquivistas e Documentalistas**, [*S. l.*], v. 9, n. 1, p. 1-7, 2007. Disponível em: http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/540/330. Acesso em: 16 jul. 2020.

CHRISTENSEN, C. M.; HORN, M. B.; STAKER, H. **Ensino híbrido**: uma inovação disruptiva? Uma introdução à teoria dos híbridos. [Boston]: Clayton Christensen Institute, 2013. Disponível em: https://www.pucpr.br/wp-content/uploads/2017/10/ensino-hibrido_uma-inovacao-disruptiva.pdf. Acesso em: 16 jul. 2020.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Carta para a preservação do patrimônio arquivístico digital**. [Rio de Janeiro]: UNESCO: CONARQ, 2005. Disponível em: http://conarq.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf. Acesso em: 16 jul. 2020.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **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: 16 jul. 2020.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **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: 16 jul. 2020.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **e-ARQ Brasil**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). **Modelo de requisitos para sistemas informatizados de gestão de processos e documentos do judiciário brasileiro**. Brasília, DF: CNJ, 2009. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2011/01/manualmoreq.pdf. Acesso em: 16 jul. 2020.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). Resolução n. 324, de 30 de junho de 2020. **Diário da Justiça [do] Conselho Nacional de Justiça**, Brasília, DF, n. 215, p. 4-11, 2020. Disponível em: https://hdl.handle.net/20.500.12178/174501. Acesso em: 16 jul. 2020.

THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS. **Audit and certification of trustworthy digital repositories**. Washington: CCSDS, 2011. Disponível em: http://public.ccsds.org/publications/archive/652x0m1.pdf. Acesso em: 16 jul. 2020.

THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS. **Reference model for an open archival information system (OAIS)**. Washington: CCSDS, 2012. Disponível em: https://public.ccsds.org/pubs/650x0m2.pdf. Acesso em: 16 jul. 2020.

CORDEIRO, A. M. *et al*. 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: 16 jul. 2020.

DIAS, R. **Cultura organizacional**. 3. ed. Campinas: Alínea, 2012.

DÍAZ, G. R.; MUGICA, M. M. M.; GUEVARA, J. D. C. Requisitos para la valoración de riesgos de preservación en repositorios digitales. **Biblios: Journal of Librarianship and Information Science**, Brasília, n. 75, p. 25-34, 2019. Disponível em: https://doi.org/10.5195/biblios.2019.484. Acesso em: 16 jul. 2020.

DURANTI, L.; PRESTON, R. **Diretrizes do preservador**: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. Vancouver: InterPARES, [2007a]. Disponível em: http://www.siga.arquivonacional.gov.br/images/publicacoes/diretrizes_produtor_digital.pdf. Acesso em: 16 jul. 2020.

DURANTI, L.; PRESTON, R. **Diretrizes do preservador**: a preservação de documentos arquivísticos digitais: diretrizes para organizações. Vancouver: InterPARES, [2007b]. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf. Acesso em: 16 jul. 2020.

DURANTI, L. 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: 16 jul. 2020.

DURANTI, L. Rumo a uma teoria arquivística de preservação digital: as descobertas conceituais do projeto InterPARES. **Revista Arquivo & Administração**, Rio de Janeiro, v. 4, n. 5, p. 5-18, 2005.

EDINGER, C. Cadeia de custódia, rastreabilidade probatória. **Revista Brasileira de Ciências Criminais**, [*S. l.*], v. 120, p. 237-257, 2016. Disponível em: https://www.academia.edu/32968479. Acesso em: 16 jul. 2020.

FERREIRA, M. **Introdução à preservação digital**: conceitos, estratégias e actuais consensos. Guimarães: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf. Acesso em: 16 jul. 2020.

FLORES, D.; PRADEBON, D. S.; CÉ, G. 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. 72-80, 2017. Disponível em: https://doi.org/10.36311/1981-1640.2017.v11n4.11.p73. Acesso em: 16 jul. 2020.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. Cadeia de custódia para documentos arquivísticos digitais. **Acervo**, Rio de Janeiro, v. 29, n. 2, p. 117-132, 2016. Disponível em: http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717/732. Acesso em: 16 jul. 2020.

FONSECA, M. O. K. **Arquivologia e ciência da informação**. Rio de Janeiro: FGV, 2005.

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

GONÇALVES, E. P. **Conversas sobre iniciação científica**. 5. ed. Campinas: Alínea, 2011.

HEDSTROM, M. Arquivos e memória coletiva: mais do que uma metáfora, menos do que uma analogia. *In*: EASTWOOD, T.; MACNEIL, H. (org.). **Correntes atuais do pensamento arquivístico**. Belo Horizonte: Ed. UFMG, 2016. p. 237-259.

HERRERA, A. H. El debate sobre la gestión documental. **Métodos de información**, Valencia, v. 5, n. 22-23, p. 30-36, 1998. Disponível em: https://core.ac.uk/download/pdf/11877283.pdf. Acesso em: 16 jul. 2020.

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

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

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

LARAIA, R. B. **Cultura**: um conceito antropológico. 14. ed. Rio de Janeiro: Zahar, 2001.

LÉVY, P. **As tecnologias da inteligência**: o futuro do pensamento na era da informática. 2. ed. São Paulo: Editora 34, 2010.

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

LUZ, C. S. A interoperabilidade na preservação da informação arquivística: os metadados e a descrição. **Informação Arquivística**, Rio de Janeiro, v. 5, n. 1, p. 27-48, 2016. Disponível em: http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/139. Acesso em: 16 jul. 2020.

LUZ, C. S.; FLORES, D. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos. *In*: SEMINÁRIO SERVIÇOS DE INFORMAÇÃO EM MUSEUS, 4., 2016, São Paulo. **Anais** [...]. São Paulo: Pinacoteca de São Paulo, 2017. p. 171-181. Disponível em: https://www.researchgate.net/publication/325225229. Acesso em: 16 jul. 2020.

MACNEIL, H. Correntes em transformação. *In*: EASTWOOD, T.; MACNEIL, H. (org.). **Correntes atuais do pensamento arquivístico**. Belo Horizonte: Ed. UFMG, 2016. p. 7-16.

MARCONDES, C. H. Interoperabilidade entre acervos digitais de arquivos, bibliotecas e museus: potencialidades das tecnologias de dados abertos interligados. **Perspectivas em Ciência da Informação**, v. 21, n. 2, p. 61-83, 2016. Disponível em: http://dx.doi.org/10.1590/1981-5344/2735. Acesso em: 16 jul. 2020.

MENEZES, I. A.; BORRI, L. A.; SOARES, R. J. A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 4, n. 1, p. 277-300, 2018. Disponível em: https://doi.org/10.22197/rbdpp.v4i1.128. Acesso em: 16 jul. 2020.

PRADO, G. **Prova penal e sistema de controles epistêmicos**: a quebra da cadeia de custódia das provas obtidas por meios ocultos. São Paulo: Marcial Pons, 2014.

REZENDE, L. V. R.; CRUZ-RIASCOS, S. A.; HOTT, D. F. M. Em busca de repositórios digitais confiáveis no Brasil: análise da infraestrutura organizacional conforme a norma ISO 16363/2012. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, Rio de Janeiro, v. 11, p. 1-12, 2017. Disponível em: http://dx.doi.org/10.29397/reciis.v11i0.1390. Acesso em: 16 jul. 2020.

ROBINSON, A. **Escrita**: uma breve introdução. Porto Alegre: L&PM, 2016.

ROCHA, C. L.; SILVA, M. 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: 16 jul. 2020.

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

SANTOS, H. M.; FLORES, D. Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 20, n. 2, p. 198-218, 2015. Disponível em: http://dx.doi.org/10.1590/1981-5344/2341. Acesso em: 16 jul. 2020.

SANTOS, H. M.; FLORES, D. Responsabilidades de um repositório arquivístico digital confiável na perspectiva do open archival information system. **Páginas a&b: Arquivos e Bibliotecas**, Porto, v. 11, n. 3, p. 116-132, 2019. Disponível em: https://doi.org/10.21747/21836671/pag11a9. Acesso em: 16 jul. 2020.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: UFSC, 2005. Disponível em: https://www.researchgate.net/publication/312125489_Metodologia_da_Pesquisa_e_Elaboracao_de_Dissertacao. Acesso em: 16 jul. 2020.

SILVA, J. A. **Comentário contextual à constituição**. 6. ed. São Paulo: Malheiros, 2009.

SILVA, M. Custódia, cadeia de preservação e custodiante confiável: conceitos para a preservação de documentos digitais autênticos. **Conhecimento em Ação**, Rio de Janeiro, v. 4, n. 2, p. 46-64, 2019. Disponível em: https://revistas.ufrj.br/index.php/rca/article/view/30291/17721. Acesso em: 16 jul. 2020.

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

SOUSA, R. T. B. A classificação como função matricial do que-fazer arquivístico. *In:* SANTOS, V. B. (org.). **Arquivística**: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. 3. ed. Brasília: SENAC, 2009. p. 79-172.

STOPANOVSKI, M. E-mails exigem cuidados específicos para que sirvam como prova. **Consultor Jurídico**, São Paulo, 2015. Disponível em: https://www.conjur.com.br/2015-set-02/suporte-litigios-servir-prova-acoes-mail-passar-pericia. Acesso em 16 jul. 2020.

THIBODEAU, K. Overview of technological approaches to digital preservation and challenges in coming years. *In*: **THE state of digital preservation**: an international perspective. Washington: CLIR, 2002, p. 4-31. Disponível em: https://www.clir.org/pubs/reports/pub107/pub107.pdf#page=10. Acesso em: 16 jul. 2020.

VOLPATO, G. L. *et al.* **Dicionário crítico para redação científica**. Botucatu: Best Writing, 2013.

VOUTSSÁS MÁRQUEZ, J. Factores tecnológicos, legales y documentales de la preservación documental digital. **Investigación Bibliotecológica**, Cidade do México, v. 23, n. 49, p. 67-124, 2009. Disponível em: http://dx.doi.org/10.22201/iibi.0187358xp.2009.49.21391. Acesso em: 16 jul. 2020.

VOUTSSÁS MÁRQUEZ, J. La cadena de preservación en archivos digitales. *In*: BARNARD, A. A. (org.). **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. 143-167.

VOUTSSÁS MARQUEZ, J.; AMOZORRUTIA, A. B. **Glosario de preservación archivística digital**: versión 4.0. México: UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información, 2014. Disponível em: http://dx.doi.org/10.22201/iibi.9786070257445e.2014.