ISSN 3085-5624

Eixo Temático 1 – Produção, Mediação e Gestão da Informação

A RUPTURA DA CADEIA DE CUSTÓDIA DIGITAL ARQUIVÍSTICA EM INSTITUIÇÕES DA INICIATIVA PRIVADA: DIAGNÓSTICO E PROPOSIÇÕES BASEADO NO E-ARQ BRASIL

THE RUPTURE OF THE DIGITAL ARCHIVAL CHAIN OF CUSTODY IN PRIVATE SECTOR INSTITUTIONS: DIAGNOSIS AND PROPOSALS BASED ON E-ARQ BRAZIL

Williane Torres dos Santos Monteiro - Universidade Federal de Alagoas (UFAL), *willianemonteiro986@gmail.com*, https://orcid.org/0009-0005-8193-962X

Daniel Flores - Universidade Federal de Alagoas (UFAL), *daniel.flores@ichca.ufal.br*, https://orcid.org/0000-0001-8888-2834

Modalidade: Trabalho Completo

Resumo: O estudo visa analisar as consequências da ruptura da cadeia de custódia digital arquivística em instituições privadas, destacando os fatores que levam à negligência na preservação segura de documentos digitais e à ausência de profissionais qualificados na área. A pesquisa, de abordagem qualitativa e caráter descritivo-exploratório, baseia-se em um estudo de caso que combina revisão bibliográfica com observação direta em três instituições. Os resultados apontam para a necessidade urgente de ambientes de gestão arquivística confiável, conforme a norma e-ARQ Brasil, com o suporte de profissionais da informação.

Palavras-chave: cadeia de custódia digital arquivística; gestão arquivística; empresas privadas; ambiente confiável.

Abstract: *The study seeks to analyze the consequences of the disruption of the digital archival chain of custody in private institutions, highlighting the factors that lead to negligence in the secure preservation of digital documents and the absence of qualified professionals in the field. The research, employing a qualitative approach and descriptive-exploratory character, is based on a case study combining bibliographic review with direct observation in three institutions. The results point to the urgent need for reliable records management environments, in accordance with the e-ARQ Brasil standard, supported by information professionals.*

Keywords: *digital archival custody chain; records management; private companies; trusted environment.*

1 INTRODUÇÃO

Um documento digital é toda informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional. Por essa razão, é fundamental que o ambiente destinado à sua produção, armazenamento e preservação seja tecnicamente estruturado e confiável, de modo a assegurar uma custódia arquivística segura, autêntica e conforme os princípios da gestão documental.

Nesse contexto, para uma administração eficiente dos documentos arquivísticos digitais, destaca-se a importância da adoção de um sistema informatizado de gestão arquivística de documentos (SIGAD). Esse tipo de sistema assegura a manutenção da organicidade, confiabilidade, autenticidade e acessibilidade contínuas – preservando, assim, o seu valor como evidência das atividades realizadas pelo órgão ou entidade produtora.

Sob essa perspectiva, é relevante destacar o papel estratégico do profissional da informação no âmbito das empresas privadas. Seu conhecimento técnico contribui diretamente para a organização, gestão e preservação de arquivos, promovendo a eficiência administrativa e a conformidade com as normas arquivísticas. Além disso, no que diz respeito aos ambientes destinados à gestão e preservação dos documentos digitais, é imprescindível o uso de sistemas arquivísticos confiáveis, administrado por profissionais capacitados, a fim de assegurar a continuidade da cadeia de custódia digital e do ciclo de vida documental.

Assim, a presente pesquisa abordará a forma como instituições da iniciativa privada realizam o armazenamento e a gestão de seus documentos arquivísticos digitais. Isso porque, ao iniciar a produção de documentos digitais sem dispor de um ambiente de gestão confiável, a empresa compromete a autenticidade e a integridade desses documentos, ocasionando uma ruptura na cadeia de custódia arquivística – situação que afeta negativamente todo o ciclo de vida do documento digital.

Nesse sentido, considerando que o arquivo é o setor responsável por gerenciar e resguardar as informações corporativas, esse estudo parte das seguintes questões: por que as empresas privadas não preservam seus documentos digitais de forma adequada? E por que não contratam especialistas para gerenciar seus arquivos?

Diante disso, os objetivos desta pesquisa são: investigar as razões pelas quais as empresas privadas deixam de adotar práticas corretas de preservação digital e deixam de contar com profissionais especializados na gestão de seus arquivos, bem como propor alternativas que contribuam para a implementação de uma preservação documental eficaz, segura e alinhada às normas arquivísticas vigentes.

2 CADEIA DE CUSTÓDIA

O processo de transição da documentação analógica para a digital, isto é, a digitalização, é definido, conforme o Conselho Nacional de Arquivos (CONARQ, 2016, p. 20),

como a "[...] conversão de um documento para o formato digital, por meio de dispositivo apropriado", processo essencial em uma sociedade interconectada. Porém, como ressaltam Schäfer e Flores (2013), "[...] há uma 'confiança' nas informações contidas em um documento arquivístico original que pode não ser possível em um representante digital".

Entretanto, para que uma instituição realize procedimentos de digitalização com validade legal, é necessário dispor de, no mínimo, um plano de classificação (PCD) e uma tabela de temporalidade de documentos (TTD), bem como regras claras de acesso à informação e mecanismos de tratamento de dados com restrição de acesso (Brasil, 2020). Também se exige a utilização de um sistema informatizado que atenda aos requisitos arquivísticos e implementação de um repositório digital confiável, capaz de assegurar a integridade, a autenticidade e a preservação dos documentos digitais desde sua captura até o final de seu ciclo de vida. Tais exigências reforçam a importância da gestão documental como base para garantir a confiabilidade jurídica e administrativa dos documentos digitais e sua preservação a longo prazo.

Tendo isso em vista, para garantir a presunção da autenticidade dos documentos digitais, é necessário analisar sua forma, conteúdo e o ambiente de produção, uso e preservação. No que se refere ao ambiente, é imprescindível a definição de direitos de acesso, espaços de trabalho, conjunto de metadados e políticas de preservação (CONARQ, 2012). Além disso, a entidade custodiadora deve possuir reputação íntegra, demonstrar capacidade técnica e conhecimento específico em gestão documental, de modo a inspirar a confiança dos usuários (CONARQ, 2012).

Nesse contexto, a cadeia de custódia digital arquivística (CCDA) equivale a um princípio aplicável aos documentos digitais, considerando suas especificidades e complexidades, para garantir que esses documentos de arquivo não sofram uma ruptura em sua cadeia de custódia arquivística em um ambiente digital. Ela os mantém sempre confinados em ambientes auditáveis, com requisitos arquivísticos homologados e sem interrupções – desde sua produção, transmissão, arquivamento até sua destinação final (Gava; Flores, 2020, 2021).

A CCDA desempenha um papel estratégico na organização e na proteção do percurso dos documentos arquivísticos digitais ao longo de suas três fases – corrente, intermediária e permanente (Gomes; Souza, 2024). Cada uma dessas etapas requer ambientes tecnológicos distintos e controlados: enquanto as fases iniciais concentram-se na gestão e no uso ativo

dos documentos, a fase permanente demanda um ambiente orientado à preservação a longo prazo e difusão segura.

Nessa conjuntura, torna-se imprescindível que as instituições da iniciativa privada adotem programas de gestão arquivística documental, preferencialmente integrados a SIGADs, aliados à implementação dos repositórios arquivísticos digitais confiáveis (RDC-Arq). Essa combinação possibilita o controle eficiente dos ciclos vitais dos documentos, contribuindo para a preservação adequada e segura de toda a documentação produzida.

Considerando esse cenário, para que essa realidade seja implementada nas instituições privadas, é imprescindível que elas iniciem a adoção do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos (e-ARQ Brasil), o qual é:

> [...] uma especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como seu acesso, pelo tempo que for necessário (CONARQ, 2022, p. 10).

Nesse sentido, o e-ARQ Brasil apresenta os fundamentos da gestão de documentos arquivísticos, introduzindo conceitos essenciais como documento arquivístico, documento arquivístico digital e gestão documental (Garcia; Sayão; Silva, 2023). Além disso, as propriedades desses documentos – organicidade, autenticidade, integridade, unicidade e acessibilidade – são elementos fundamentais para a compreensão das especificidades de sistemas voltados à produção, organização, controle e preservação de objetos digitais.

Garcia, Sayão e Silva (2023) destacam a importância da formulação de políticas institucionais, da definição de requisitos funcionais e da utilização de instrumentos arquivísticos que assegurem a custódia, a confiabilidade e a preservação desses documentos ao longo do tempo para garantir sua validade como registros autênticos das ações institucionais e instrumentos de prova administrativa, jurídica e histórica.

Com relação ao ambiente de gestão de documentos, seu planejamento e implantação são essenciais para o desenvolvimento ou a aquisição de um sistema aderente aos requisitos do e-ARQ Brasil. Nesse viés, a gestão de documentos envolve procedimentos e operações técnicas de produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária até sua destinação final (Brasil, 1991).

Desse modo, o SIGAD possui a função de gerenciar, de forma segura e confiável, a crescente produção documental nas organizações, independente do seu suporte (CONARQ,

2022). Esse gerenciamento abrange um conjunto articulado de operações, como a captura, armazenamento, controle de acesso, aplicação de PCDs e TTDs, tramitação, acompanhamento do ciclo de vida documental e a definição de critérios para avaliação, destinação e preservação.

Ele contribui para garantir a integridade, autenticidade e acessibilidade dos documentos arquivísticos a médio e longo prazo, assegurando sua disponibilização para fins administrativos, legais, fiscais e históricos até seu destino final, seja eliminação ou recolhimento para guarda permanente. Portanto, sua implementação deve estar alinhada aos princípios da gestão documental e diretrizes arquivísticas nacionais (CONARQ, 2022, 2023).

Assim, é importante debater também a respeito da preservação digital, isto é, o "Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário" (CONARQ, 2020, p. 39). O seu desenvolvimento precisa envolver toda a organização e demanda investimento em recursos financeiros, humanos, tecnológicos e alteração da cultura organizacional.

A preservação digital exige planejamento sistemático, por meio de políticas e planos de preservação, amparado por estudos técnicos e diagnósticos institucionais (Souza; Aganette, 2020). As políticas estabelecem diretrizes institucionais, viabilizam a alocação de recursos e asseguram a sustentabilidade das ações preservacionistas. Já os planos são instrumentos operacionais que orientam a implementação de estratégias e procedimentos voltados à manutenção da autenticidade, integridade, confiabilidade e acessibilidade dos documentos.

Portanto, a preservação digital sistêmica (PDS**)** pressupõe a manutenção da CCDA de forma ininterrupta em ambientes digitais confiáveis (Gava; Flores, 2021, 2022). Na formação da PDS, observa-se a manutenção de características duradouras dos documentos, tal como a autenticidade e a própria organicidade (Melo; Luz, 2022), além de características trazidas aos documentos nato-digitais, como forma fixa, conteúdo estável, documento estático, documento interativo e variabilidade limitada (Santos; Flores, 2017).

3 MODELO OAIS

O *Open Archival Information System* (OAIS), formalizado pelo padrão da *International Organization for Standardization* (ISO 14721:2025), é um modelo conceitual fundamental para a preservação digital de longo prazo. Ele estabelece uma estrutura completa para sistemas de arquivamento, garantindo que as informações digitais permaneçam acessíveis e compreensíveis ao longo do tempo, independentemente das mudanças tecnológicas (ISO, 2025a).

No modelo, o "longo prazo" é um elemento central, esse termo está associado a um período indefinido em que tecnologias, formatos de dados e métodos de acesso podem se tornar obsoletos (ISO, 2025a). O objetivo principal é assegurar a autenticidade, integridade e utilidade dos dados para as futuras gerações. Para isso, o OAIS define claramente os papéis, responsabilidades e processos necessários, desde a ingestão dos conteúdos até sua disponibilização aos usuários.

Portanto, ele é utilizado no contexto de estratégias voltadas para a padronização dos processos que conduzem à conferência da preservação da informação digital, suportada por meios de acesso e difusão como os repositórios institucionais. Ele fornece uma ampla visão das etapas necessárias ao tratamento dos recursos para acesso, considerando os atores envolvidos neste processo, que consistem basicamente em quatro entidades: produtor (*producer*), consumidor (*consumer*), administração e arquivo (ISO, 2025a).

Já as entidades funcionais são essenciais para organizar as responsabilidades e os fluxos de trabalho dentro de um arquivo digital. Elas garantem que a informação seja recebida, armazenada, gerenciada e disponibilizada de forma confiável e consistente ao longo do tempo. Nesse sentido, as principais são: ingestão, administração, área de armazenamento, gerenciamento de dados, acesso e planejamento de preservação (Flores; Pradebon; Cé, 2017).

O modelo OAIS foi estruturado para gerenciar o fluxo de informações necessário à preservação de documentos digitais (Santos; Flores, 2020b). Para isso, ele utiliza três tipos de pacotes de informação para facilitar o transporte e a custódia dos documentos: o pacote de informação para submissão (SIP), a entrada de dados; pacote de informação para arquivamento (AIP), a preservação de longo prazo; e pacote de informação para disseminação (DIP), a entrega aos usuários.

Os pacotes possuem funções distintas complementares na preservação de documentos digitais (Santos; Flores, 2020b). O SIP reúne informações administrativas e contextuais que sustentam a autenticidade do documento desde sua entrada no sistema. O AIP, por sua vez, preserva o SIP e adiciona metadados que garantem a integridade e a rastreabilidade do conteúdo ao longo do tempo. Já o DIP corresponde à versão disponibilizada ao público, em formatos acessíveis, mas mantendo as propriedades arquivísticas essenciais.

A entidade funcional de ingestão é responsável por preparar os conteúdos para armazenamento e gerenciamento no arquivo OAIS (Flores; Pradebon; Cé, 2017). Esse processo ocorre através dos SIPs, enviados pelo produtor ao OAIS. A forma e o conteúdo desses pacotes são negociados entre o produtor e o administrador do arquivo. Essa etapa garante a recepção e organização adequada dos dados, seguindo as regras e padrões estabelecidos.

No ambiente OAIS, os SIPs são transformados em um ou mais AIPs, essenciais para a preservação. Cada AIP é composto por um conjunto completo de *preservation description information* (PDI), que detalha as informações de conteúdo associadas, e pode, ainda, incorporar outros AIPs (ISO, 2025a).

As informações sobre os pacotes AIP estão de acordo com normas internas do OAIS, podendo variar, uma vez que são geridas neste ambiente. Após uma solicitação, o OAIS retorna a totalidade ou uma parte do AIP como resposta ao consumidor. Esse material será enviado na forma de um DIP. O DIP também poderá incluir coleções de AIPs, as quais podem ou não conter uma PDI completa (ISO, 2025a).

As atividades do OAIS podem ser consideradas arquivísticas, pois corroboram com a conceituação dada pela norma internacional para descrição de funções (Conselho Internacional de Arquivos, 2008, p. 13) que as conceituam como: "Qualquer objetivo de alto nível, [...] como atribuição de uma entidade coletiva pela legislação, política ou mandato". Nesse sentido, as entidades funcionais apresentam serviços de alto nível a serem executados por um repositório.

Externo ao ambiente OAIS, há duas entidades a serem consideradas: o produtor e o consumidor. Elas exercem funções elementares referentes à origem e finalidade dos processos de preservação digital. O produtor envia um fluxo de dados contendo o pacote SIP ao repositório. Posteriormente, ocorre sua transformação em AIP para o arquivamento em

longo prazo. E, por fim, o consumidor poderá fazer consultas/solicitações (*query responses/orders*) ao OAIS e obter o pacote DIP com os respectivos resultados (Santos; Flores, 2020b).

É nesse alinhamento com a estrutura do OAIS que o RDC-Arq configura-se como a solução brasileira para a preservação digital de longo prazo, incorporando seus princípios de gestão e as melhores práticas internacionais para assegurar a confiabilidade arquivística dos documentos digitais. A conformidade do RDC-Arq com tais requisitos é avaliada por meio de auditorias baseadas em padrões, como a ISO 16363:2025 (ISO, 2025b), que especifica requisitos para auditoria e certificação de repositórios digitais confiáveis.

Nesse sentido, documentos com valor permanente exigem a preservação no RDC-Arq de forma a assegurar a segurança e manutenção de sua autenticidade e organicidade (CONARQ, 2023). Enquanto para os em fases corrente e intermediária pode ser recomendado quando forem sensíveis, complexos ou de longa temporalidade.

Na medida em que os formatos de arquivo se tornam obsoletos, o RDC-Arq executa conversões e migrações para novos formatos conforme a política de preservação definida pela instituição, a fim de assegurar o acesso contínuo aos documentos (CONARQ, 2023). A preservação por intermédio do RDC-Arq admite diversos formatos de arquivo, sejam textuais, sonoros, multimídia, iconográficos, entre outros.

Somando a isso, é fundamental que o RDC-Arq assuma uma missão institucional clara e comprometida com a preservação digital e o acesso contínuo à informação arquivística em longo prazo (Santos; Flores, 2020a). Para garantir esse compromisso, diretrizes bem definidas, como os planos de sucessão e a política de recolhimento para custódia, devem ser formuladas (Santos; Flores, 2020a). Esses instrumentos são essenciais para garantir não apenas a continuidade e estabilidade da preservação digital, mas também a manutenção da integridade, da autenticidade e do valor probatório dos documentos arquivísticos.

4 RUPTURA DA CADEIA DE CUSTÓDIA

Jenkinson (1922, p. 11, tradução nossa) afirma que: "[...] para ser considerado arquivo, é necessário que o material seja autêntico e o meio de demonstrar a autenticidade é a possibilidade de provar uma linha imaculada de custodiados responsáveis". A preocupação desse autor refere-se à existência de falsificações ou mesmo documentos que

foram separados de sua origem e que, em muitos casos, ocorreram por interrupção na custódia (Silva, 2019).

A autenticidade é configurada por uma série de elementos que caracterizam a confiabilidade e a flexibilidade de um documento. Para que um documento torne-se autêntico, ele precisa ser custodiado por uma instituição responsável e possuir elementos para garantir sua estrutura diplomática, tais como autoria e data (CONARQ, 2012). Esses elementos validam o documento e concretizam sua autenticidade e veracidade, tornando-o confiável. São caracteres intrínsecos e extrínsecos de cada documento que pressupõem a análise de seu suporte segundo os referenciais da Diplomática (Flores; Rocco; Santos, 2016).

Já a autenticação – que resulta no documento autenticado, na digitalização autenticada ou na assinatura digital –, é uma declaração de autenticidade de um documento, em um determinado momento, resultante do acréscimo de um elemento ou afirmação por parte de uma pessoa investida de autoridade para tal (Flores; Rocco; Santos, 2016). Ao reconhecerem a diferença entre esses dois conceitos, as organizações estão mais preparadas para adotar estratégias preventivas, de modo a diminuir os riscos e garantir a integridade e autenticidade de seus documentos digitais a longo prazo.

Além disso, a guarda inadequada de documentos arquivísticos pode gerar implicações jurídicas sérias para a instituição responsável. Quando há perda de autenticidade, integridade ou acesso indevido, isso pode configurar negligência administrativa, implicando em sanções civis, administrativas ou até penais, conforme a legislação vigente (Brasil, 1991). A instituição deve garantir a proteção dos documentos arquivísticos contra perdas, danos, alterações não autorizadas e extravios, assegurando sua função probatória, histórica e administrativa.

Nesse contexto, a busca por soluções que garantam, de fato, a eficiência do gerenciamento eletrônico de documentos (GED) nas organizações não é algo trivial. As organizações produzem um volume documental considerável e, com o avanço tecnológico e eventuais alterações nas diretrizes internas focadas nas melhorias de processos ou implantações de novos projetos, os documentos e sua gestão sofrem diversas atualizações.

A pessoa ou entidade que for transferir para essa instituição precisa apresentar cabalmente a autenticidade dos documentos digitais. Para tanto, faz-se necessário verificar se houve alteração, intencional ou não, pois a instituição arquivística assumiria um risco ao recolher materiais não verificados e avaliados em sua própria condição de documento

autêntico, e essa é uma tarefa do produtor (Silva, 2019). Dessa forma, é fundamental reconhecer o papel dos sistemas informatizados na preservação digital, pois permitem o acompanhamento e monitoramento contínuo do ciclo de vida e custódia ininterrupta (Santos, 2019).

5 METODOLOGIA

Esta pesquisa consiste em um estudo de caso de natureza qualitativa, centrado no aprofundamento da compreensão de um ou poucos objetos de investigação (Gil, 2002; Gerhardt; Silveira, 2009). Além disso, possui caráter descritivo-exploratório, pois visa "[...] descrever completamente determinado fenômeno" (Marconi; Lakatos, 2003, p. 188).

A abordagem adotada é a pesquisa de campo, realizada em três instituições privadas de Maceió, para analisar as práticas adotadas referentes à gestão, armazenamento e preservação de documentos arquivísticos digitais. A pesquisa concentrou-se na observação do ambiente institucional e análise de normativas, procedimentos internos, estruturas tecnológicas e sistemas utilizados na gestão documental.

Para o levantamento e análise dos dados, foram utilizados instrumentos como a observação sistemática e a pesquisa documental, o que possibilitou uma visão crítica das condições estruturais, normativas e tecnológicas relacionadas à custódia e preservação digital. O diagnóstico obtido foi interpretado à luz do e-ARQ Brasil, da cadeia de custódia digital e dos princípios do modelo OAIS, permitindo a identificação de fragilidades e a proposição de melhorias.

6 DIAGNÓSTICO

Durante a realização da pesquisa, identificou-se que nenhuma das três instituições avaliadas contratou profissional especializado para o controle e a manutenção de seus arquivos. Em todos os casos, a gestão optou por designar profissionais da área de Tecnologia da Informação ou de áreas correlatas para essa função. Embora essa escolha seja compreensível, considerando que esses profissionais possuem habilidades valiosas no ambiente digital, ela evidencia a ausência de uma abordagem arquivística adequada na gestão dos documentos digitais dessas empresas.

Nesse cenário, ao analisar os ambientes digitais utilizados pelas empresas para o armazenamento de seus documentos, constatou-se a ausência de sistemas de gestão

arquivística confiáveis. Essa deficiência compromete diretamente a manutenção da CCDA, fragilizando o controle contínuo sobre a autenticidade, integridade e confiabilidade da informação registrada. Verificou-se, ainda, a utilização de sistemas de GED como repositórios arquivísticos, os quais apresentam fragilidades técnicas e procedimentais que colocam em risco tanto a segurança da informação quanto a segurança jurídica das organizações.

Como exemplo, destaca-se a adoção do Google Drive pelas três instituições analisadas como principal ambiente de gestão e preservação de documentos arquivísticos digitais. A escolha, segundo os usuários, justifica-se pela praticidade e funcionalidade da ferramenta, que permite o acesso rápido, o *download* e a modificação dos documentos. No entanto, essa prática compromete os princípios da cadeia de custódia arquivística digital, pois o sistema utilizado não oferece mecanismos adequados para a autenticidade desses documentos.

Vale destacar que, em decorrência desse cenário, observou-se uma desordem nos documentos armazenados no Google Drive, em grande parte, causada pela ausência de um PCD adequado. Essa lacuna comprometia a organização da informação e, em consequência, tornava mais onerosa a busca e recuperação de documentos pelos funcionários.

Dessa forma, ao confiar seus documentos digitais a um sistema que não adota os princípios arquivísticos nem respeita as etapas do ciclo de vida documental, o gestor expõe a instituição a riscos de insegurança jurídica, em razão do comprometimento da autenticidade.

As empresas analisadas compartilham um objetivo em comum: digitalizar seus documentos analógicos para preservá-los permanentemente. Entretanto, a preocupação estava voltada ao volume de documentos digitalizados, deixando em segundo plano a qualidade, fidelidade e conformidade técnica exigida pelo processo. Por esse motivo, era comum que a tarefa fosse atribuída a estagiários, priorizando-se apenas a execução rápida da atividade, sem o devido rigor técnico.

7 PROPOSTA

Com base no diagnóstico realizado, torna-se imprescindível que as empresas privadas adotem sistemas arquivísticos de gestão confiável, a fim de organizar e preservar seus documentos digitais conforme as normas arquivísticas brasileiras vigentes. Paralelamente, é

dever da gestão dessas instituições reavaliar o perfil dos profissionais responsáveis pela administração desses sistemas, uma vez que ambientes arquivísticos e informacionais exigem atuação técnica especializada de profissionais da informação (arquivistas, bibliotecários e gestores da informação), capazes de assegurar a autenticidade, integridade e acesso contínuo aos documentos digitais.

Nesse contexto, recomenda-se a implementação de um SIGAD (CONARQ, 2022) para que a organização dos documentos passe a contemplar o ciclo de vida documental, respeitando as fases corrente e intermediária até a destinação final. Essa medida garante a continuidade da cadeia de custódia arquivística, preservando a integridade, a autenticidade e o valor probatório dos documentos ao longo do tempo.

Em complemento, propõe-se a adoção do modelo de referência OAIS (ISO, 2025a) como arcabouço conceitual para a preservação digital de longo prazo e a implementação de RDC-Arq (CONARQ, 2023).

Para sustentar a confiança no repositório, recomenda-se ainda que seus sistemas sejam projetados de acordo com padrões e convenções amplamente aceitos, e passíveis de auditoria (ISO, 2025b). Assim, a confiabilidade deve ser demonstrada aberta e explicitamente, mediante políticas, práticas e indicadores de desempenho auditáveis e mensuráveis, contemplando as responsabilidades de longo prazo perante depositantes e usuários.

Por fim, as empresas devem complementar suas ações organizacionais com instrumentos arquivísticos fundamentais – PCD, TTD (CONARQ, 2022), normas de descrição arquivística, vocabulários controlados, guias e catálogos –, além de políticas formais voltadas à preservação digital, segurança da informação, acesso e transparência ativa. Tais medidas são essenciais para assegurar a conformidade com as melhores práticas nacionais e internacionais, bem como garantir a efetividade da gestão arquivística digital.

8 CONSIDERAÇÕES FINAIS

Durante a realização desta pesquisa, constatou-se que o comodismo aliado à busca por soluções mais acessíveis e imediatas leva às empresas analisadas a negligenciarem práticas adequadas de preservação e gestão de seus documentos arquivísticos digitais. Essa postura compromete a autenticidade, integridade, confiabilidade e acessibilidade dessas informações ao longo do tempo.

Diante desse cenário, destaca-se a relevância do referencial teórico apresentado nesse estudo, o qual fornece fundamentos técnicos e conceituais para orientar possíveis transformações nos arquivos dessas instituições. A adoção efetiva das práticas arquivísticas, aliada à contratação de profissionais qualificados – como arquivistas e gestores da informação –, é fundamental para a implementação de políticas eficientes de gestão documental.

Ao longo do trabalho, foram discutidos conceitos como a cadeia de custódia arquivística digital, que garante a guarda contínua, segura e autenticada de documentos digitais durante todo o seu ciclo de vida. A manutenção dessa cadeia – sem rupturas – é condição indispensável para assegurar o valor probatório dos documentos, reforçando a importância de se estruturar um SIGAD corporativo eficiente e integrado às práticas arquivísticas.

Adicionalmente, foi evidenciada a importância da aplicação do modelo de referência OAIS, especialmente por meio de seus pacotes de informação, articuladores da relação entre os produtores, administradores e consumidores da informação digital. O OAIS oferece uma estrutura padronizada e, portanto, contribui para a preservação a longo prazo e a garantia da autenticidade dos documentos digitais.

Importa ainda destacar que a continuidade da CCDA se sustenta na interoperabilidade entre três ambientes complementares: o ambiente de gestão documental (SIGAD), o de preservação digital confiável (RDC-Arq) e a plataforma de acesso, descrição e difusão. A integração entre esses sistemas assegura uma abordagem sistêmica da gestão documental, essencial para a longevidade da informação arquivística digital.

Nesse contexto, torna-se urgente que as três empresas analisadas adotem um SIGAD, conforme preconizado pelo modelo de requisitos e-ARQ Brasil, junto com o RDC-Arq. Por fim, é imprescindível que essas instituições reconheçam a complexidade e a vulnerabilidade dos documentos digitais e compreendam que a adoção de práticas arquivísticas confiáveis não é apenas uma exigência normativa, mas uma necessidade estratégica para garantir segurança jurídica, eficiência administrativa e transparência institucional.

REFERÊNCIAS

BRASIL. **Decreto nº 10.278, de 18 de março de 2020**: regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682,

de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados [...]. Brasília: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10278.htm. Acesso em: 07 jun. 2025.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991**: dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília: Presidência da República, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8159.htm. Acesso em: 07 jun. 2025.

CONSELHO INTERNACIONAL DE ARQUIVOS. **ISDF**: norma internacional para descrição de funções. Rio de Janeiro: Arquivo Nacional, 2008. Disponível em: https://www.gov.br/conarq/pt-br/centrais-deconteudo/publicacoes/ISDF.pdf. Acesso em: 02 jun. 2025.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis – RDC-Arq**. 2. ver. Rio de Janeiro: Arquivo Nacional, 2023. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/publicacoes-conarq. Acesso em: 21 abr. 2025.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais**. Rio de Janeiro: CONARQ, 2012. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/publicacoes-conarq. Acesso em: 21 abr. 2025.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. **e-ARQ Brasil**: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. 2. ver. Rio de Janeiro: Arquivo Nacional, 2022. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/publicacoes-conarq. Acesso em: 21 abr. 2025.

CONSELHO NACIONAL DE ARQUIVOS - CONARQ. **Glossário documentos arquivísticos digitais**. 8. ver. Rio de Janeiro: CONARQ, 2020. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glossario-da-ctde. Acesso em: 21 abr. 2025.

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. DOI: https://doi.org/10.36311/1981-1640.2017.v11n4.11.p73. Disponível em: https://revistas.marilia.unesp.br/index.php/bjis/article/view/7511. Acesso em: 21 jun. 2025.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. Autenticidade e cadeia de custódia. **Acervo**, Rio de Janeiro, v. 29, n. 2, p. 77-100, jul./dez. 2016. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/717. Acesso em: 28 jul. 2025.

GARCIA, A. C. S.; SAYÃO, L. F.; SILVA, M. O sistema eletrônico de informações (SEI): um exame comparativo das avaliações do Arquivo Nacional e do Ministério da Economia com

base no e-ARQ Brasil. **Revista Brasileira de Preservação Digital**, Campinas, v. 4, p. 1-23, 2013. DOI: https://doi.org/10.20396/rebpred.v4i00.17426. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/17426. Acesso em: 01 ago. 2025.

GAVA, T. B. S.; FLORES, D. Auditoria e certificação ao longo da cadeia de custódia digital arquivística. **Informação & Informação**, Londrina, v. 26, n. 4, p. 424-449, 2021. DOI: https://doi.org/10.5433/1981-8920.2021v26n4p424. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/44504. Acesso em: 28 jul. 2025.

GAVA, T. B. S.; FLORES, D. Problematizando a pós-custódia com a contemporaneidade da cadeia de custódia digital arquivística compartilhada e distribuída na preservação digital sistêmica. **InCID**: revista de ciência da informação e documentação, Ribeirão Preto, v. 13, n. 2, p. 222-243, set. 2022. DOI: https://doi.org/10.11606/issn.2178-2075.v13i2p222-243. Disponível em: https://revistas.usp.br/incid/article/view/191654. Acesso em: 28 jul. 2025.

GAVA, T. B. S.; FLORES, D. Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. **Informação & Informação**, Londrina, v. 25, n. 2, p. 74-99, 2020. DOI: https://doi.org/10.5433/1981-8920.2020v25n2p74. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/38411. Acesso em: 28 jul. 2025.

GERHARDT, T. E.; SILVEIRA, D. T. (org.). **Métodos de pesquisa**. Porto Alegre: UFRGS, 2009. Disponível em: https://lume.ufrgs.br/handle/10183/52806. Acesso em: 28 jul. 2025.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOMES, W. S.; SOUZA, E. D. A trilha para a preservação digital sistêmica na arquivologia: abordagem teórico-conceitual de um modelo de gestão compartilhada e distribuída. *In*: ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO, 24., 2024, Vitória. **Anais** [...]. Vitória: Ancib, 2024. Disponível em: https://enancib.ancib.org/index.php/enancib/xxivenancib/paper/view/2725. Acesso em: 10 jun. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721:2025**: space data and information transfer systems - Open Archival Information System (OAIS) – reference model. 3. ed. Genebra: ISO, 2025a.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363:2025**: space data and information transfer systems - audit and certification of trustworthy digital repositories. 2. ed. Genebra: ISO, 2025b.

JENKINSON, H. **A manual of archive administration including the problems of war archives and archive making**. Oxford: Oxford University, 1922. Disponível em: https://archive.org/details/manualofarchivea00jenkuoft/manualofarchivea00jenkuoft/page/218/mode/2up. Acesso em: 10 jun. 2025.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MELO, I. F.; LUZ, C. S. A aderência de sistemas informatizados de gestão arquivística ao e-ARQ Brasil: verificação de requisitos mínimos e obrigatórios. **Acervo**, Rio de Janeiro, v. 35, n. 1, p. 1-15, jan./abr. 2022. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/1778. Acesso em: 22 jun. 2025.

SANTOS, H. M. Auditoria de repositórios arquivísticos digitais confiáveis. **Informação em Pauta**, Fortaleza, v. 4, n. 2, p. 156-172, jul./dez. 2019. DOI: https://doi.org/10.36517/ip.v4i2.41787. Disponível em: https://periodicos.ufc.br/informacaoempauta/article/view/41787. Acesso em: 12 jul. 2025.

SANTOS, H. M.; FLORES, D. 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, 2020a. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/1305. Acesso em: 12 jul. 2025.

SANTOS, H. M.; FLORES, D. Preservação sistêmica para repositórios arquivísticos. **Revista Eletrônica de Comunicação, Informação e Inovação em Saúde**, Rio de Janeiro, v. 14, n. 3, p. 764-781, jul./set. 2020b. DOI: https://doi.org/10.29397/reciis.v14i3.2089. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2089. Acesso em: 12 jul. 2025.

SANTOS, H. M.; FLORES, D. Preservação de documentos digitais: reflexões sobre as estratégias de refrescamento. **Revista Brasileira de Biblioteconomia e Documentação**, São Paulo, v. 13, n. 2, p. 31-41, 2017. Disponível em: https://rbbd.febab.org.br/rbbd/article/view/449. Acesso em: 12 jul. 2025.

SCHÄFER, M. B.; FLORES, D. A digitalização de documentos arquivísticos no contexto brasileiro. **Tendências da Pesquisa Brasileira em Ciência da Informação**, João Pessoa, v. 6, n. 2, jul./dez. 2013. Disponível em: https://revistas.ancib.org/index.php/tpbci/article/view/290. Acesso em: 30 jul. 2025.

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. DOI: https://doi.org/10.47681/rca.v4i2.30291. Disponível em: https://revistas.ufrj.br/index.php/rca/article/view/30291. Acesso em: 10 jun. 2025.

SOUZA, L. G. S.; AGANETTE, E. C. A preservação digital em longo prazo amparada por planos de ações: uma revisão sistemática de literatura. **Revista Digital de Biblioteconomia e Ciência da Informação**, Campinas, v. 18, p. 1-25, 2020. DOI: https://doi.org/10.20396/rdbci.v18i0.8661185. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8661185. Acesso em: 22 jul. 2025.