Artigo

Preservation as a Service for Trust (PaaST): Requisitos para serviços de preservação digital em ambientes de Nuvem

Preservation as a Service for Trust (PaaST): Requirements for digital preservation services in Cloud environments

Alex Pereira de Holanda | Doutorando em Ciência da Informação (UFF). Mestre em Memória Social (Unirio). Graduado em Arquivologia (Unirio) com especializações em Gestão da Informação e Inteligência Competitiva (Unesa) e Preservação do Patrimônio Cultural (Fiocruz). Pesquisador e líder de grupo de pesquisa no IBICT. Arquivista do Arquivo Nacional. E-mail: alexholanda@ibict.br / alex_holanda@id.uff.br. ORCID: 0000-0002-1213-8360

Margareth Silva | Doutora em História Social pela Universidade de São Paulo (2015). Mestre em História Social pela Universidade Federal do Rio de Janeiro (1995). Graduada em História pela Universidade Federal Fluminense (1983). Professor Adjunto da Universidade Federal Fluminense e professora credenciada no Programa de Pós-Graduação em Memória e Acervos da Fundação Casa de Rui Barbosa. ORCID https://orcid.org/0000-0002-4343-8390

Clarissa M S Schmidt | Doutora em Ciência da Informação (2012) pelo Programa de Pós-graduação em Ciência da Informação da Escola de Comunicações e Artes da Universidade de São Paulo (ECA-USP). Mestre em História Social (2005). Bacharel em Ciências Sociais (2001), Pontifícia Universidade Católica de São Paulo (PUC-SP). Professora no Programa de Pós-graduação em Ciência da Informação da Universidade Federal Fluminense - PPGCI/UFF, Integra o quadro diretivo da Associação de Arquivistas de São Paulo (ARQ-SP). E-mail: clarissaschmidt@id.uff.br. ORCID https://orcid.org/0000-0003-1555-4594

Resumo

O artigo discute a crescente adoção de tecnologias de nuvem no Brasil e a necessidade urgente de abordagens confiáveis para a preservação de documentos arquivísticos digitais autênticos nesse contexto dinâmico. O PaaST, uma iniciativa do ***InterPARES*** Trust, é apresentado como uma solução que propõe um conjunto de requisitos funcionais e de dados para garantir a preservação confiável desses documentos na nuvem, assegurando sua autenticidade, confiabilidade e admissibilidade legal, independentemente das mudanças tecnológicas ou das fronteiras jurisdicionais. A metodologia utilizada combina a análise de documentos normativos e a revisão de literatura, abordando a complexidade da preservação digital em ambientes distribuídos e os desafios na manutenção da autenticidade em cadeias digitais de custódia. O artigo contribui para o avanço das práticas de preservação digital ao oferecer reflexões relevantes para arquivistas e tomadores de decisão, destacando a importância de desenvolver padrões e protocolos para a preservação de documentos digitais em ambientes de nuvem. O modelo PaaST, ao herdar e adaptar princípios do OAIS, propõe uma estrutura flexível e aplicável a diferentes cenários tecnológicos, enfatizando a necessidade de colaboração interdisciplinar para garantir a confiabilidade dos sistemas utilizados. No entanto, a aplicação do PaaST no contexto brasileiro exige uma análise mais aprofundada, especialmente quanto à custódia e à relação entre as organizações produtoras e as instituições arquivísticas.

Palavras-chave: Autenticidade; Documentos arquivísticos digitais; Nuvem; PaaST (Preservation as a Service for Trust); Preservação digital.

Abstract

The article discusses the growing adoption of Cloud [Padronizar a utilização do termo – ou inicial maiúscula sempre, como no título, ou inicial minúscula sempre] technologies in Brazil and the urgent need for trusted approaches to the preservation of digital records in this dynamic context. PaaST, an initiative of the InterPARES Trust, is presented as an innovative solution that proposes a set of functional and data requirements to ensure the trusted preservation of digital records in the Cloud, safeguarding their authenticity, trustworthiness and legal admissibility, regardless of technological changes or jurisdictional boundaries. The methodology used combines the analysis of normative documents and a literature review, addressing the complexity of digital preservation in distributed environments and the challenges of maintaining authenticity in digital chains of custody. The article contributes to the advancement of digital preservation practices by offering relevant insights for archivists, librarians, and decision-makers, highlighting the importance of developing robust standards and protocols for the preservation of digital records in Cloud environments. The PaaST model, by inheriting and adapting principles from OAIS, proposes a flexible structure applicable to different technological scenarios, emphasizing the need for interdisciplinary collaboration to ensure the trustworthiness of the systems used. However, the application of PaaST in the Brazilian context requires further analysis, especially regarding custody and the relation between producing organizations and archival institutions.

KEYWORDS: *Authenticity; Digital archival records; Cloud; PaaST (Preservation as a Service for Trust); Digital preservation.*

1. Introdução

A adoção crescente de soluções de nuvem no Brasil marca uma revolução na forma como instituições públicas e privadas gerenciam e preservam seus documentos digitais. Este cenário, evidenciado por um estudo da O'Reilly Media[1] que prevê que 94% das organizações migrarão para tecnologias de nuvem nos próximos cinco anos (2017 a 2022), é reforçado por pesquisas que apontam que no Brasil cerca de 42% das empresas usam a nuvem para processamento, com estimativas de crescimento de mais de 10% para os próximos 2 anos[2], destacando a necessidade urgente de abordagens confiáveis para a preservação de documentos arquivísticos digitais autênticos[3]. A complexidade desta tarefa é amplificada pela dinâmica e pela elasticidade da nuvem, que, embora ofereça vantagens econômicas significativas através da economia de escala, também introduz desafios sem precedentes em termos de segurança, autenticidade, custódia e legalidade dos documentos armazenados.

Diante deste contexto, o modelo "Preservation as a Service for Trust" (PaaST) emerge como uma resposta inovadora, propondo um conjunto de requisitos funcionais e de dados para a preservação de documentos arquivísticos digitais de forma confiável na nuvem. O PaaST, uma iniciativa do ***InterPARES*** Trust[4], visa garantir que os documentos digitais sejam preservados de forma a manter sua autenticidade, confiabilidade e admissibilidade legal, independentemente das mudanças tecnológicas ou das fronteiras jurisdicionais que possam afetar sua gestão.

[1] Alois Mary, Peter Putz, Dirk Wallerstorfer, Anna Gerber. 2017. Cloud-Native Evolution. O'Reilly Media, Sebastopol, CA. ISBN: 978-1-491-97396-7

[2] 34ª Pesquisa Anual do FGVcia: Uso da TI nas Empresas. https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/pesti-fgvcia-2023_0.pdf

[3] A autenticidade dos documentos arquivísticos é assegurada por sua criação, manutenção e custódia de acordo com procedimentos regulares e verificáveis. Um documento é considerado autêntico quando é produzido com a intenção de servir como meio de ação e é mantido como um testemunho fiel dos fatos ou atos por seu criador e seus legítimos sucessores. A autenticidade fundamenta-se em dois aspectos essenciais: a identidade, que se refere aos atributos que caracterizam e distinguem o documento de outros, incluindo os nomes das pessoas envolvidas em sua criação (autor, destinatário, escritor, originador, criador), as datas relevantes (criação, recepção, depósito, transmissão), a matéria ou ação a que o documento se refere, suas relações contextuais com outros documentos (como código de classificação) e a indicação de anexos; e a integridade, que diz respeito à qualidade de ser completo e inalterado em todos os aspectos essenciais. (MACNEIL, Heather et al. 2002).

[4] Quarta fase do ***InterPARES*** Project foca credibilidade de documentos produzidos, armazenados e preservados em ambientes distribuídos.

Este trabalho busca apresentar o PaaST, onde a transformação digital acelerada e a adoção de serviços baseados na nuvem apresentam tanto oportunidades quanto desafios para a preservação de documentos digitais. Por meio de uma abordagem metodológica que combina análise de documentos normativos e revisão de literatura, este artigo delimita o tema da preservação de documentos arquivísticos digitais na nuvem, estabelece objetivos claros e apresenta uma justificativa robusta para a escolha do tema, destacando sua relevância em um cenário de crescente dependência de tecnologias digitais.

A organização do trabalho reflete uma estrutura lógica e coesa que apresenta os fundamentos teóricos do PaaST. Ao final, buscamos contribuir para o avanço das práticas de preservação digital no país, fornecendo reflexões sobre o tema para auxiliar arquivistas, bibliotecários, profissionais da informação e tomadores de decisão em instituições que dependem da preservação confiável de documentos digitais.

2. Metodologia

Este estudo adota uma abordagem metodológica que combina a análise de documentos normativos e uma revisão de literatura. A metodologia utilizada é fundamentada na exploração dos textos acadêmicos e normativos mais relevantes para o campo da preservação digital, com foco particular no Projeto ***InterPARES*** e no modelo Preservation as a Service for Trust (PaaST). A análise se concentra em como os requisitos e diretrizes estabelecidos pelo PaaST podem ser aplicados para assegurar a preservação confiável de documentos arquivísticos digitais em ambientes de nuvem, garantindo sua autenticidade, integridade e admissibilidade legal, independentemente das mudanças tecnológicas ou das fronteiras jurisdicionais.

A revisão de literatura foi realizada com base em textos acadêmicos e normativos na área de preservação digital, arquivologia e ciência da informação. Os principais textos que fundamentaram a revisão incluem:

1. **Normas e documentos e do *InterPARES* Trust:** Especialmente o modelo OAIS e o Preservation as a Service for Trust (PaaST), que foi central para a análise e discutido em termos de sua aplicabilidade.

2. **Estudos sobre Autenticidade e Custódia:** Textos que abordam os conceitos de autenticidade, identidade e integridade dos documentos arquivísticos, além das implicações da custódia em ambientes distribuídos.

Esta revisão e a subsequente análise normativa permitiram uma compreensão dos desafios e das melhores práticas na preservação de documentos arquivísticos digitais, especialmente em contextos de nuvem. Assim, a metodologia adotada buscou fornecer uma base para as recomendações apresentadas no artigo.

3. O Documento Arquivístico Digital e os desafios de sua preservação

Os documentos arquivísticos digitais representam uma categoria específica de documentos, definidos como qualquer registro criado ou recebido no decorrer de atividades práticas, servindo como instrumento ou subproduto dessas atividades. A autenticidade desses documentos é vital e estabelecida por meio de sua identidade[5] e integridade[6].

[5] A totalidade das características de um documento ou registro que o identifica unicamente e o distingue de qualquer outro documento ou registro, juntamente com a integridade, compõe um componente da autenticidade. [Archives- Authenticity Task Force Report, Page: 47]. Atributo que singulariza um documento arquivístico, com elementos como os nomes dos envolvidos na sua criação (autor, destinatário, redator, originador e criador), suas datas (criação, recebimento e arquivamento), o tema ou ação em que participa, a expressão de suas relações contextuais com outros documentos (código de classificação).

[6] A integridade, refere-se à qualidade de ser um documento arquivístico completo e inalterado.

A autenticidade dos documentos arquivísticos digitais surge como uma questão crítica nos anos 1990, conforme evidenciado por trabalhos na área (cf. Duranti e Eastwood 1995; Duff 1996; Duranti e MacNeil 1997; Bearman e Trant 1998). No ano de 1993, o Comitê de Documentos Arquivísticos Eletrônicos do Conselho Internacional de Arquivos (ICA), empreendeu a elaboração de uma série de iniciativas cuja finalidade residia em fomentar a realização de estudos e pesquisas, incentivar o intercâmbio de experiências e conceber normativas e diretrizes que orientassem a criação e o tratamento arquivístico de documentos arquivísticos eletrônicos. Esta empreitada culminou na produção de três estudos: "Programas de Documentos Arquivísticos Eletrônicos: Relatório da Pesquisa 1994/95", "Gestão de Documentos Arquivísticos Eletrônicos: Uma Revisão da Literatura", e "Guia para a Gestão de Documentos Arquivísticos Eletrônicos sob uma Perspectiva Arquivística" (Comitê de Documentos Arquivísticos Eletrônicos, 2005, Prefácio, p. 5).

De acordo com o ***InterPARES*** Project[7], a autenticidade só pode ser presumida em maior ou menor grau a partir da avaliação de determinados atributos e elementos do documento arquivístico, deste modo, quanto maior a quantidade de atributos e elementos encontrados maior será o grau de presunção de autenticidade do documento.

A autenticidade é um conceito fundamental na teoria arquivística, vinculado aos processos de criação, manutenção, preservação e custódia de documentos. A autenticidade dos arquivos se manifesta quando esses documentos são gerados com a finalidade de servir como meio de ação, preservados como testemunho fiel de eventos pelo criador e seus sucessores legítimos. (EASTWOOD, 1994, p.127) (Duranti, 2022).

Esse conceito de autenticidade abrange o contexto completo em que os documentos foram produzidos, acessados, armazenados e gerenciados e preservados, desde o momento de sua produção até o fim de sua vida útil e eventual descarte, ou seja, durante todo o seu ciclo vital. O desafio de preservar a autenticidade dos documentos arquivísticos digitais é amplificado pela natureza dinâmica e elástica da computação em nuvem.

A autenticidade contínua dos documentos arquivísticos digitais depende necessariamente da forma como estes documentos são preservados em uma cadeia ininterrupta de custodiadores confiáveis. Tais custodiadores devem manter os documentos arquivísticos devidamente identificados e resguardados de corrupção intencional, garantindo a integridade do conjunto, suas inter-relações, estabilidade e fixidade.

Na Arquivologia, "custódia" denota a incumbência associada ao cuidado, controle, guarda e acesso de documentos arquivísticos. Esta responsabilidade abarca tanto o controle físico quanto o legal dos documentos, visando garantir sua preservação, segurança e acessibilidade. Essa responsabilidade é comumente delegada a uma instituição ou organização arquivística designada como custodiadora, por meio de instrumentos legais e administrativos. No contexto dos documentos digitais, assume uma importância ainda maior, dado que é por meio de uma custódia confiável que um documento arquivístico digital pode ser preservado a em longo prazo para garantir sua autenticidade.

A custódia ininterrupta confiável revela-se importante para salvaguardar a autenticidade dos documentos arquivísticos. Qualquer interrupção no controle sobre o documento implica riscos de exclusão, alteração ou substituição, e qualquer descontinuidade na custódia pode comprometer a capacidade de demonstrar que um documento não foi modificado. No ambiente digital, onde os documentos arquivísticos não estão fisicamente fixados em mídias duráveis e sua forma pode ser dissociada do conteúdo, o conceito tradicional

[7] ***InterPARES***. ***InterPARESProject***. Diretrizes do Produtor: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. 2002-2007, p.37. Disponível em: http://www.***InterPARES***.org/display_file.cfm?doc=creator_guidelines_booklet--portuguese.pdf

de cadeia de custódia ininterrupta[8] necessita de uma expansão. Assim surge a noção de "cadeia de preservação", que engloba informações sobre práticas do produtor, transferência entre sistemas, reprodução de documentos e tramitação ao longo do tempo.

> Os pressupostos por trás da cadeia de custódia ininterrupta são inadequados para os documentos digitais, mesmo que todos os custodiadores sucessivos exerçam o nível de diligência que teriam no caso de documentos analógicos, porque a inscrição de documentos digitais está longe de ser fisicamente fixa. (...) a forma física de um documento digital muda toda vez que é movido entre um processador e o armazenamento, entre um processador e um dispositivo de entrada/saída e entre diferentes processadores. O processamento, tanto por firmware quanto por software, pode alterar elementos intrínsecos e extrínsecos de forma, comprometendo a identidade e a integridade de um documento. Os riscos são agravados sempre que o software é modificado, o que ocorre com frequência. Além disso, mesmo especialistas conscientes são improváveis de estar totalmente cientes de todas as implicações das alterações no software e hardware. (Duranti, Rogers e Thibodeau, 2022, p. 193-194)

Por esse motivo, a Preservation Task Force do ***InterPARES***-1 Project propôs a criação de uma nova "cadeia" complementar à cadeia de custódia. Enquanto a cadeia de custódia se concentra em rastreabilidade de posse e responsabilidade (de ordem jurídica e administrativa), a cadeia de preservação preocupa-se nos registros de atuação e interferência sofridos pelo documento arquivístico digital ao longo de seu ciclo de vida, algo como uma rastreabilidade operacional. A proposta do ***InterPARES*** é que os documentos arquivísticos digitais devem passar por processos específicos de armazenamento, processamento e preservação em um fluxo predefinido conforme o modelo pré-estabelecido, em todo o seu ciclo de vida.

Duranti e Rogers (2012) abordam a credibilidade dos documentos arquivísticos a partir de dois arcabouços teóricos distintos: o primeiro é o da arquivologia e o segundo é o da forense digital[9], evidenciando as convergências e divergências entre perspectivas, conceitos e definições de cada uma dessas áreas. Em seu artigo, as pesquisadoras apresentam os elementos que definem a integridade do documento arquivístico, segundo a forense digital, baseados em dois princípios, o da não interferência e o da interferência identificável. Tais princípios balizam a análise e validade dos materiais coletados como evidências em julgamentos. A autenticação de evidências digitais em juízo demanda uma declaração autoritativa, comumente fornecida por uma testemunha familiarizada com o registro ou, na ausência desta, por um perito em forense digital. Este último demonstra a precisão dos resultados produzidos pelo sistema ou processo computacional sob uso e operação adequados durante a geração da evidência.

A credibilidade de evidências digitais circunstanciais é reforçada por metadados[10] detalhados, incluindo cronologia de transmissões e identificação dos dispositivos de origem e recebimento. A cadeia digital de

[8] A proposta de cadeia de custódia ininterrupta de Jenkinson como mecanismo de garantia de autenticidade estava relacionada à mudança de custódia desses documentos quando transferidos do produtor para o preservador. De acordo com Duranti, Rogers e Thibodeau (2022) mesmo que os documentos sejam autênticos, suas inter-relações podem ser modificadas pela forma como o material é mantido ao longo do tempo ou por aqueles que o guardaram. Esta ideia corresponde ao à da cadeia de provas no Direito: as provas podem ser autênticas quando colhidas, mas têm de ser mantidas pelas pessoas competentes.

[9] Forense digital é um ramo da ciência forense relacionada à prática de coletar, analisar e relatar dados de dispositivos eletrônicos de forma a ser utilizada em investigações e em contextos legais. Especialistas em forense digital examinam sistemas de computador, dispositivos móveis e redes para identificar e recuperar evidências digitais relacionadas a crimes cibernéticos, fraudes, disputas legais e outras investigações. Esse campo combina elementos de direito e ciência da computação para solucionar crimes e disputas onde informações digitais são componentes fundamentais à investigação.

[10] Metadados são informações que descrevem outros dados, fornecendo contexto e significado. Eles são importantes para a credibilidade das evidências digitais, pois ajudam a estabelecer a autenticidade, a integridade e o contexto dos dados ou documentos. Por exemplo, metadados podem incluir detalhes sobre a criação de um documento, como o autor, a data e a hora da criação, acessos, e qualquer alteração subsequente. A importância dos metadados para a credibilidade é destacada no contexto da computação em nuvem, onde os registros são armazenados e gerenciados remotamente.

custódia, isto é, as informações preservadas sobre o registro e suas mudanças, mostrando que dados específicos estavam em um determinado estado em uma data e hora específicas, documentando as alterações do documento arquivístico, fundamenta a inferência da presunção da autenticidade, corroborada por avaliações periciais sobre a integridade do sistema de registros e seus procedimentos de controle. Assim, evidências circunstanciais que demonstram a funcionalidade inalterada do sistema, livre de manipulações, fortalecem a autenticidade do documento (Duranti, 2012, p 526-527).

Em uma apresentação sobre o ***InterPARES*** Trust realizada no ICA-ALA ***Conference***, na Cidade do México em 2017[11], Duranti apresenta os meios para efetuar a autenticação arquivística: a cadeia de legítimos custodiadores, a declaração de um especialista baseada na confiabilidade do sistema e processos que mantém, preservam e possibilitam o uso do documento e, por fim, a cadeia digital de custódia, demonstrando uma apropriação deste conceito e sua aplicação da forense digital como meio de autenticação pela arquivologia.

Em 2020, na mesa redonda sobre autenticidade de documentos digitais ocorrida no Simpósio Internacional de Arquivos, promovido pela Associação de Arquivistas de São Paulo, Luciana Duranti e Rosely Curi Rondinelli argumentaram o seguinte acerca da importância da cadeia digital de custódia:

> Em relação aos documentos digitais, a cadeia ininterrupta de custódia não é suficiente, ou seja, já não basta demonstrar que os documentos passaram linearmente do produtor para o preservador. É preciso demonstrar também o que aconteceu com eles ao longo de sua existência (se houve perdas, alterações), afinal, agora, a probabilidade desses eventos acontecerem é muito maior. Essa é a cadeia digital de custódia, ou seja, uma cadeia de informações (metadados) sobre os documentos digitais. Trata-se então de um conceito que se aplica aos documentos digitais independentemente da existência ou não de Sigads e de Rdc-Arqs. Sigads e Rdc-Arqs apoiam essa custódia, mas não são a custódia. (Duranti e Rondinelli, 2020).

Para além da explicação sobre a importância da cadeia digital de custódia, Duranti e Rosely apontam algo que é fundamental, isto é, que algumas traduções da terminologia para o português traduzem ***digital chain of custody*** como cadeia de custódia digital e não como cadeia digital de custódia, o que é um equívoco já que, de fato, o que é digital é a cadeia (sequência de processo que ocorre no meio digital) e não a custódia, tendo em vista que ela é relacionada à responsabilidade jurídica e administrativa sobre os arquivos. Pode parecer simples, mas essa inversão das palavras altera completamente o entendimento do conceito e, consequentemente, sua aplicação no ambiente arquivístico.

Todo este cenário se complica quando o ambiente de produção, manutenção, preservação e acesso dos documentos é distribuído em um sistema global de provedores, em países distintos e, portanto, em diferentes jurisdições, que podem levar ao deslocamento do local de armazenamento do documento sem o conhecimento de seu proprietário, o que pode representar um risco à sua autenticidade, como afirma Duranti (2018, pag. 133-136), pois qualquer quebra no conhecimento de como a informação digital foi preservada pode tornar impossível afirmar que o que permaneceu é o que deveria ser preservado.

Segundo Duranti e Rogers (2019), a dependência crescente dos serviços de internet e a redução da confiança pública em organizações de todos os setores, que utilizam esses serviços, estão provocando uma crise de confiança. Indivíduos delegaram a gestão de seus documentos para terceiros, cujas preocupações com a precisão, confiabilidade e autenticidade podem divergir das expectativas originais do

[11] O título da apresentação era "***An Infrastructure for Truth: Estrusting Digital Facts to Archival Theory***" e está disponível em https://www.alaarchivos.org/wp-content/uploads/2017/12/Magistral-Luciana-Duranti.pdf

proprietário de documentos. Este cenário destaca a necessidade de reavaliar e fortalecer os mecanismos de confiança nas relações digitais e na administração de documentos online.

A confiança tradicionalmente depositada nos documentos não digitais, fundamentada em séculos de práticas legais e acumulação de conhecimento, enfrenta desafios sem precedentes no ambiente digital. A dinâmica das relações de confiança na internet, ou ambiente de terceiros, é dificultada pela vulnerabilidade do material digital, assim como pela gestão e armazenamento de documentos e dados digitais. As rápidas mudanças tecnológicas exacerbam estas questões, levantando dúvidas sobre autoria, propriedade e jurisdição, e colocando em xeque os pilares da confiança anteriormente estabelecidos.

A transição da confiança de documentos não digitais para os digitais e a subsequente dependência em provedores de serviços em nuvem introduzem uma complexidade inédita na manutenção da autenticidade dos documentos. Esta transição é agravada pela necessidade de adaptar práticas e estruturas de confiança estabelecidas a um ambiente onde a propriedade e o controle dos dados são externalizados. O desafio reside em assegurar que os mecanismos de preservação e cadeias de custódia e cadeia de preservação, sejam robustos e transparentes o suficiente para sustentar a autenticidade dos documentos digitais, em meio às dinâmicas voláteis da tecnologia e da jurisdição digital. Este elo intermediário evidencia a importância crítica de desenvolver padrões e protocolos, que possam ser aplicados de forma consistente, garantindo a credibilidade dos documentos digitais armazenados em ambientes de terceiros, onde a gestão de riscos e a responsabilidade pela autenticidade se tornam ainda mais pertinentes.

Sob uma perspectiva probatória, a utilização de Provedores de Serviços em Nuvem para armazenar documentos de significativo valor legal levanta questões sobre a credibilidade desses documentos após sua transferência do controle da entidade produtora. Esse cenário suscita preocupações quanto à existência de documentação adequada que permita estabelecer uma cadeia de custódia detalhada, necessária para validar a autenticidade dos documentos recuperados da nuvem. A documentação deve ser suficientemente abrangente para traçar o percurso dos documentos dentro da infraestrutura dos provedores de serviço, incluindo quem acessou os documentos e quando, desde o momento de sua transferência de seu produtor. A responsabilidade sobre qualquer dano que ocorra sobre o documento e sua integridade se dilui em meio a contratos de serviço de nuvem. Essa fluidez põe em risco a autenticidade dos documentos arquivísticos já que estão “fora” do controle de seus produtores.

Deste modo, o registro detalhado da cadeia de custódia se torna fundamental, já que garante minimamente a rastreabilidade de todas as ocorrências sobre os documentos, de acessos, intervenções sobre o seu conteúdo e até mesmo eventos de preservação. Esses registros devem estar previstos nos acordos e contratos entre os proprietários dos documentos e os provedores de serviço de nuvem.

O “***Preservation as a Service for Trust***” (PaaST), uma iniciativa do ***InterPARES Project Trust***[12], estabelece critérios detalhados para a preservação de informações digitais em múltiplos contextos, incluindo a nuvem. Esses critérios são projetados para serem aplicáveis independentemente das tecnologias empregadas ou das entidades que as utilizam, abordando a heterogeneidade dos objetos de informação, a diversidade de diretivas legais e normativas, as variações nas condições de propriedade e acesso, os arranjos institucionais, e um leque de circunstâncias operacionais. Foram desenvolvidos como uma forma de garantir os elementos mínimos necessários para se garantir a autenticidade dos documentos em ambientes distribuídos, ou seja, incorpora elementos da cadeia de custódia ininterrupta neste contexto.

[12] O ***InterPARES*** Trust é a quarta fase do ***InterPARES*** Project, iniciado após as fases anteriores do ***InterPARES***. Aborda os desafios impostos pelos avanços tecnológicos e pela crescente tendência de armazenamento de dados em nuvem, que complicam a gestão de documentos arquivísticos e a manutenção da confiança pública na informação. O projeto reconhece que a preservação digital não é apenas uma questão técnica, mas também envolve considerações legais, éticas e de governança. Portanto, busca desenvolver diretrizes e melhores práticas que possam ser aplicadas globalmente para garantir que os documentos digitais sejam preservados de maneira a manter sua confiabilidade ao longo do tempo, independentemente de onde ou como são armazenados.

A implementação do modelo PaaST proporciona uma solução integrada para a preservação digital em ambientes de nuvem, permitindo que as organizações adaptem suas práticas de preservação às especificidades tecnológicas e legais de diferentes contextos. A estrutura flexível do PaaST facilita a manutenção da autenticidade dos documentos arquivísticos, mesmo em cenários de responsabilidades distribuídas, assegurando que as práticas de preservação se mantenham eficazes e alinhadas com as exigências normativas e operacionais ao longo do tempo.

4. A preservação como um serviço para a confiança

O "***Preservation as a Service for Trust***" (***PaaST***), fundamentando-se nas descobertas do ***InterPARES*** Project, enfoca a preservação digital confiável tanto em ambientes de nuvem quanto em outros contextos. Articula e implementa critérios essenciais para a preservação eficaz de informações digitais, utilizando esses critérios para avaliar e documentar tanto as medidas adotadas para a preservação quanto o estado dos objetos digitais preservados. Os requisitos do PaaST são projetados para sustentar a autenticidade dos documentos, permitindo o registro e a avaliação das ações de forma mais eficaz. Contudo, são suficientemente flexíveis para se adaptarem a diferentes cenários de preservação, inclusive quando os objetos de informação não são mantidos explicitamente como documentos arquivísticos. Essa flexibilidade é ilustrada na abordagem adotada para a preservação de conjuntos de dados, dependendo de seu propósito final, seja para evidência documental ou para futuras pesquisas científicas, enfatizando a necessidade de critérios de qualidade dos dados adaptáveis.

Enquanto o ***Open Archival Information System*** (OAIS)[13] estabelece um ***framework*** conceitual para a preservação, abrangendo tanto documentos analógicos quanto digitais sem prescrever tecnologias específicas, o PaaST direciona-se especificamente para a implementação de soluções digitais, delineando critérios aplicáveis diretamente em ambientes computacionais. Destaca-se que, ao contrário do OAIS, o PaaST foca exclusivamente em dados digitais, propondo um escopo de aplicação mais restrito e centrado na tecnologia. Diferencia-se do OAIS pela sua aplicabilidade prática e abordagem empírica (Figura 1), visando facilitar a implementação dos critérios de preservação digital em sistemas computacionais existentes. Tal especificidade permite que o PaaST aborde de maneira efetiva os desafios da preservação em ambientes digitais, especialmente em contextos de nuvem, sem vincular-se a tecnologias particulares. Porém, herda do OAIS a neutralidade tecnológica, permitindo flexibilidade na escolha de métodos para enfrentar questões como a obsolescência tecnológica.

Figura 1 - Comparação entre OAIS e PaaST

	OAIS	**PaaST**
Âmbito	Qualquer tipo de objeto de informação	Somente objetos de informação digitais, com foco em documentos arquivísticos digitais
Intenção	Um modelo de referência	Destina-se a orientar e facilitar a implementação

[13] O modelo de referência OAIS (Open Archival Information System), lançado em 2002 pelo Consultative Committee for Space Data Systems (CCSDS), foi concebido para oferecer um framework conceitual destinado à preservação de longo prazo de dados, inicialmente voltado para os dados gerados por missões espaciais. Em 2003, o modelo foi adotado como a norma ISO 14721. O OAIS define uma estrutura que abrange funções, conceitos, responsabilidades e objetivos, sendo amplamente aplicável em diversos contextos de preservação de informações digitais. Ele organiza e sistematiza estratégias de preservação, facilitando o gerenciamento eficiente das atividades envolvidas. O modelo identifica seis entidades funcionais principais, propõe um esquema ontológico para os pacotes de informação utilizados pelo repositório, e descreve as inter-relações dentro dessa estrutura, além dos diversos processos e serviços que devem ser operados para assegurar a preservação eficaz.

Funcionalidade	Funções abrangentes para e relacionadas à preservação	Somente funções específicas de preservação
Abordagem de solução	Vislumbra um sistema coerente de preservação	Pressupõe que a preservação é alcançada através de um conjunto de serviços que podem ser projetados e implementados de forma independente
Implementação	Neutra	Independente de plataforma, mas projetada para automação ideal

Fonte: Duranti et Al ,2016, p.13.

O PaaST propõe uma nova terminologia e conceitos de informação, adaptando padrões existentes, como os do OAIS, para criar uma estrutura de metadados e gestão de preservação orientada para o digital. Essa abordagem introduz a noção de "***PermanentFeatures***", atributos ou operações de objetos digitais, que devem permanecer inalterados para assegurar a preservação eficaz. Tais características são fundamentais para manter a autenticidade dos documentos digitais ao longo do tempo.

Sua estrutura é projetada para ser flexível, permitindo a adaptação às diversas necessidades e cenários de preservação. Isso inclui a capacidade de especificar detalhadamente o que é necessário para a preservação de diferentes tipos de objetos de informação, considerando as variadas políticas de preservação e características dos objetos. Esta abordagem permite que políticas e decisões de gerenciamento específicas sejam implementadas de forma executável, garantindo que a preservação digital seja realizada de acordo com os critérios estabelecidos.

É estabelecido um quadro abrangente para a preservação digital, identificando quatro papéis essenciais no processo: (i) o Titular Inicial, que detém os objetos a serem preservados; (ii) o Diretor de Preservação, responsável pela gestão da preservação; (iii) o Provedor de Serviços de Preservação, que oferece os meios tecnológicos para a preservação; e o (iv) Cliente de Acesso, interessado em acessar as informações preservadas. Esses papéis facilitam a distribuição e execução de tarefas de preservação, empregando diversas tecnologias e métodos, dentro de um ambiente denominado Ambiente de Preservação. Este ambiente não pressupõe um sistema integrado, mas uma orquestração flexível de capacidades tecnológicas e ferramentas, permitindo tanto soluções de preservação internas quanto externas, contratadas através de acordos específicos.

A expressão dos requisitos do PaaST, formulada como declarações de capacidade, confere aos Diretores de Preservação a liberdade para determinar quais funções serão adotadas em cada Ambiente de Preservação. Tal flexibilidade é fundamental para ajustar a estratégia de preservação às particularidades de cada conjunto de informações digitais, respeitando os objetivos específicos e as políticas de cada organização. Esse modelo descentralizado reconhece a complexidade dos ambientes digitais atuais e promove uma abordagem mais personalizada e eficiente para a preservação de dados e documentos.

Os requisitos não são restritos a uma única solução de sistema de preservação digital. Ao invés disso, visando adaptar-se a uma diversidade de contextos, esses requisitos são organizados em grupos de funcionalidades correlatas, denominadas serviços. Esses serviços podem ser implementados utilizando-se as metodologias e ferramentas mais apropriadas para seus propósitos específicos, possibilitando que diferentes serviços sejam geridos por provedores variados. Tal estrutura permite a flexibilidade na escolha de realizar algumas funções internamente, enquanto outras podem ser delegadas a terceiros através de contratos, adequando-se assim às necessidades e estratégias de preservação das organizações.

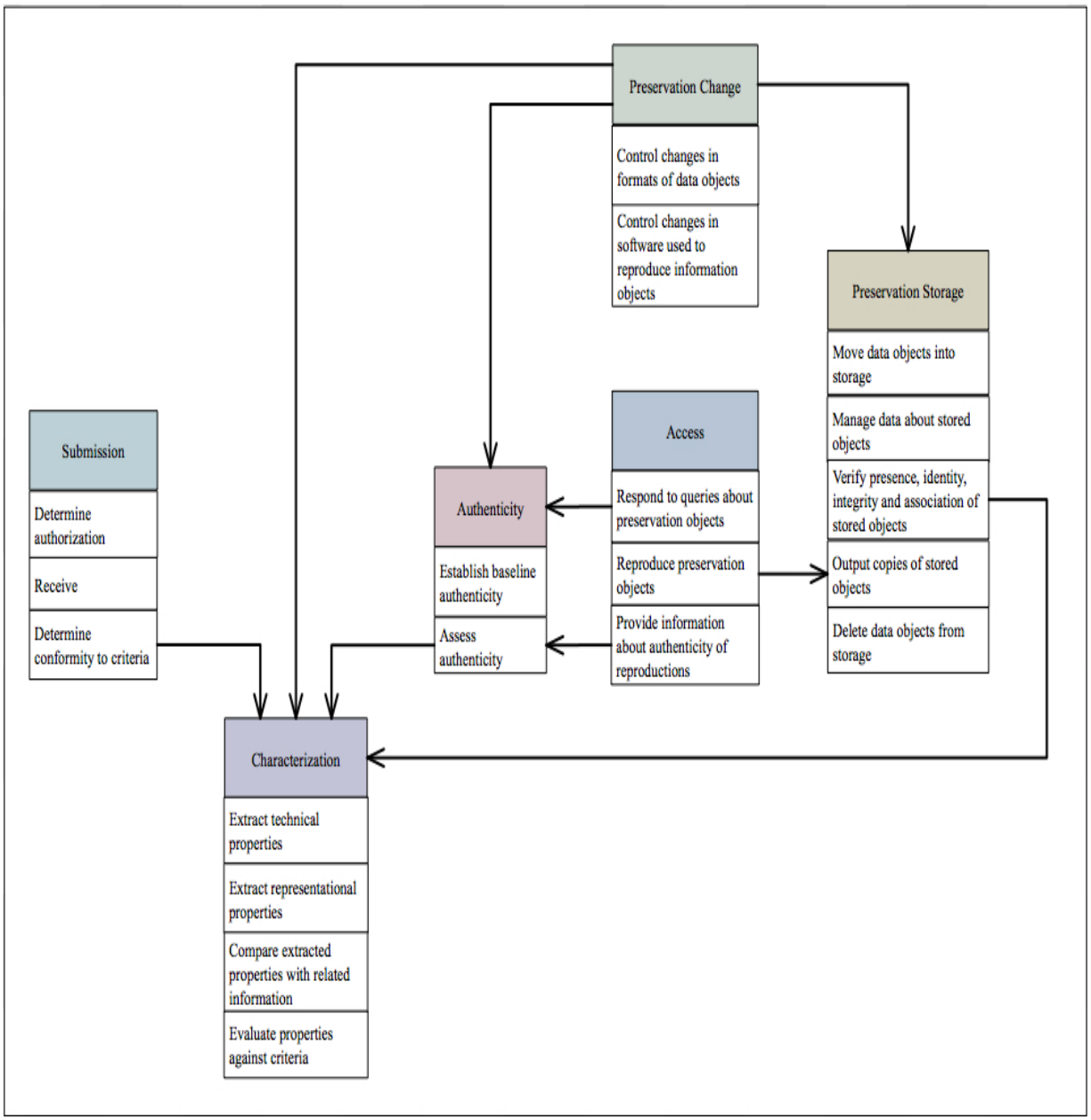
As informações mantidas e geradas em um Ambiente de Preservação, segundo o PaaST, são estruturadas em uma taxonomia de classes, onde cada classe agrupa objetos com características comuns. Essa taxonomia oferece uma estrutura flexível para a preservação digital, permitindo adaptações conforme as especificidades de cada ambiente de preservação. Para atender às necessidades particulares e políticas específicas de preservação e acesso, a taxonomia do PaaST pode ser expandida com subclasses mais detalhadas. Além disso, o PaaST proporciona diretrizes para a definição de classes e a articulação de regras e condições de preservação, promovendo uma abordagem personalizada e abrangente para a gestão de informações digitais preservadas.

Os requisitos do "***Preservation as a Service for Trust***" (PaaST) estão estruturados em categorias denominadas "serviços", que se dividem em grandes grupos: Serviços de Ação de Preservação e Recursos de Gerenciamento de Preservação. Essa organização permite a implementação flexível de práticas de preservação digital, adaptando-se a uma variedade de contextos por meio da definição de capacidades específicas. A abordagem modular do PaaST facilita a escolha de métodos e ferramentas, adequados para cada capacidade, permitindo a execução por diferentes provedores, seja internamente ou através de contratos externos.

Por sua vez, o Modelo de Domínio PaaST enriquece essa estrutura ao introduzir uma taxonomia detalhada e especializada de classes e atividades. Esse modelo conceitual visa não apenas complementar os requisitos com uma descrição mais rica das entidades envolvidas na preservação digital, mas também fornecer uma base para a extensão e especificação dos requisitos em ambientes de preservação concretos. Utilizando a Linguagem de Modelagem Unificada (UML) para a representação, o PaaST propõe um sistema de organização que pode ser adaptado e expandido conforme necessário, garantindo que os objetivos de preservação sejam alcançados de maneira eficaz em diferentes contextos.

Os serviços específicos incluem: Submissão, para inserção de objetos de preservação no ambiente; Caracterização, para avaliação das propriedades técnicas, arquivísticas e representativas dos objetos; Autenticidade, abordando a identidade e integridade dos objetos e aplicando métodos de autenticação; Armazenamento de Preservação, gerenciando o armazenamento para manter a identidade dos objetos e evitar corrupção; Mudança de Preservação, para adaptar a tecnologia, como migração de formato ou atualização de software, visando manter a usabilidade; e Acesso, que facilita a entrega de cópias dos objetos preservados. Estes serviços são projetados para operar de forma interconectada, garantindo a eficácia da preservação digital.

Figura 2 – PaaST Services



Fonte: Duranti Et Al, 2016, p. 31.

O modelo não abrange serviços que não sejam especificamente destinados à preservação digital, nem serviços gerais que poderiam ser oferecidos por um provedor de serviços, independentemente da designação dos objetos de preservação para preservação a longo prazo. Tais serviços gerais incluem telecomunicações, gestão de dados, registros de sistema, segurança, funcionalidades de busca genérica, subsistemas de armazenamento e capacidades de transferência de arquivos. Embora os serviços de preservação muitas vezes recorram a esses serviços gerais, a suposição de sua disponibilidade implica que não precisam ser detalhados nos requisitos do PaaST. Exemplifica-se com o sistema de gestão de acervos, comumente utilizado por arquivos e bibliotecas para gerir os inventários de materiais sob sua responsabilidade.

Além dos Serviços de Preservação essenciais, o modelo PaaST incorpora três categorias de recursos de apoio projetados para reforçar e complementar a eficácia desses serviços. A primeira categoria, **Gestão**, abrange recursos dedicados ao controle e ao tratamento de problemas, essenciais para a administração eficiente das diretrizes de preservação e para a identificação, classificação, atribuição e acompanhamento

de problemas emergentes. A segunda, **Processamento de Informações**, engloba recursos como gestão da informação, relatórios, definição de classe e definição de composição, que facilitam a criação, manutenção e manipulação de informações críticas para a preservação. A terceira, **Processamento de Objetos**, inclui inspeção, verificação e avaliação de autenticidade, garantindo a integridade e a autenticidade dos objetos de preservação ao longo do tempo. Cada recurso desempenha um papel vital no ecossistema de preservação do PaaST, oferecendo um conjunto abrangente de ferramentas para enfrentar os desafios da preservação digital.

Toda a lógica de papeis, serviços e recursos, são transcritos em requisitos que estabelecem uma base para confiar na preservação de informações digitais fornecidas por provedores de serviços de nuvem. A essência desta fundação reside em um conjunto de dados que habilitam tanto os responsáveis pela custódia dos objetos de informação preservados quanto os interessados em produzir conhecimento desses objetos a avaliar sua autenticidade. Especificamente, isto implica na capacidade de discernir as características dos objetos de preservação que se mantiveram constantes ao longo do tempo, de analisar o impacto das mudanças tecnológicas tanto na codificação digital dos objetos de preservação quanto no software empregado para seu processamento, e de determinar a ocorrência de qualquer forma de corrupção. Estes dados são coletados, produzidos, administrados e utilizados na prestação de serviços de preservação que concretizam os requisitos funcionais estabelecidos pelo PaaST, assegurando uma gestão eficaz que sustente a integridade e a autenticidade dos objetos de informação ao longo de seu ciclo de vida.

No contexto da preservação em ambientes de nuvem, os requisitos estabelecidos demonstram sua aplicabilidade universal às diversas metodologias de preservação digital, abarcando uma ampla gama de objetos de informação. Os serviços delineados pelo PaaST definem um conjunto de ações estratégicas a serem implementadas por determinadas funções, quer se situem interna ou externamente à entidade organizacional, com o propósito de assegurar e evidenciar a autenticidade dos objetos de preservação através do tempo. Este processo implica na adoção de uma abordagem sistemática e documentada para a gestão da informação, enfatizando a necessidade de mecanismos robustos de verificação e documentação que sustentem a integridade e a proveniência dos dados no ambiente digital.

5. Considerações Finais

O *Preservation as a Service for Trust* (PaaST), introduz uma série de serviços de preservação destinados a manter a autenticidade dos registros ao longo do tempo e do espaço, detalhando as ações e atributos necessários para documentar a transferência e armazenamento de documentos em nuvem. Assim, ao implementar os serviços PaaST, os sistemas capturarão metadados essenciais para estabelecer a identidade dos registros e demonstrar sua integridade dentro de uma cadeia de custódia documentada.

Sua proposta incorpora toda a lógica da cadeia ininterrupta de custódia e da cadeia de preservação em entidades distintas, cujas atividades são regidas por contratos e acordos de serviços. No caso da preservação como serviço, a definição dos papeis, serviços e recursos em uma lógica compatível ao modelo OAIS deve ser documentada, indicando os papeis e atividades em um processo contínuo de produção, submissão, preservação e acesso de modo a permitir que a qualquer momento a presunção de autenticidade possa ser aferida.

O modelo PaaST também destaca a importância de estabelecer metadados precisos e detalhados que servem não apenas para identificar os registros, mas também para registrar sua trajetória e manipulações ao longo do tempo. Essa abordagem garante que os registros possam ser verificados e validados em qualquer ponto de sua existência, fornecendo uma base sólida para a autenticidade. A adoção de contratos e acordos

de serviços, alinhados com os princípios do modelo OAIS, promove uma gestão transparente e responsável dos documentos digitais, reforçando a confiança dos usuários nos sistemas de arquivamento.

Sua implementação requer uma compreensão profunda das tecnologias e normas envolvidas, bem como das práticas da Arquivologia. A colaboração entre arquivistas, tecnólogos e juristas é essencial para desenvolver e manter sistemas de preservação que sejam não apenas tecnicamente viáveis, mas também legalmente sólidos e eticamente responsáveis. Esse esforço conjunto garante que o PaaST possa se adaptar às mudanças tecnológicas e às novas demandas legais e sociais, preservando a relevância e a eficácia dos sistemas de arquivamento digital a longo prazo.

Ao estabelecer processos transparentes e auditáveis para a preservação e o acesso aos documentos digitais, o modelo promove uma maior abertura e responsabilização das instituições que detêm os objetos digitais de importância pública. Isso é particularmente relevante em uma era onde a informação é um recurso valioso e a transparência institucional uma expectativa crescente da sociedade.

Em conclusão, o ***Preservation as a Service for Trust*** representa um paradigma emergente na preservação de documentos digitais, oferecendo um caminho promissor para enfrentar os desafios de autenticidade, integridade e acesso. Sua implementação bem-sucedida depende de um compromisso contínuo com a inovação, a colaboração interdisciplinar e a adaptação às dinâmicas tecnológicas e sociais. Ao fazer isso, o PaaST tem o potencial de reforçar a confiança nos documentos digitais como pilares da memória, ferramentas para o exercício da cidadania, fontes de descoberta e divulgação cientificas, da governança e da cultura. No entanto, sua aplicação no contexto brasileiro demanda análises mais aprofundadas, principalmente a respeito da custódia e da relação entre as organizações produtoras e as instituições arquivísticas, considerando os aspectos de avaliação, transferência e recolhimento.

Referências

BEARMAN, D.; TRANT, J. Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process. **D-Lib Magazine**, v. 4, n. 6, jun. 1998. Disponível em: https://chnm.gmu.edu/digitalhistory/links/pdf/introduction/0.19c.pdf. Acesso em: 12 dez. 2023.

DUFF, W. Ensuring the Preservation of Reliable Evidence: A Research Project Funded by the NHPRC. **Archivaria**, Canadá, v. 42, p. 28-45, out. 1996. Disponível em: https://archivaria.ca/index.php/archivaria/article/view/12152 . Acesso em: 12 dez. 2023.

DURANTI, L.; FRANKS, P. C. (Eds.). **Encyclopedia of Archival Science**. Lanham, Maryland; Estados Unidos. MD: Rowman & Littlefield, junho 2015. 464 p. ISBN 978-0-8108-8810-4 (hardback), ISBN 978-0-8108-8811-1 (eBook).

DURANTI, L.; MACNEIL, H. The Protection of the Integrity of Electronic Records: An Overview of the UBC-MAS Research Project. **Archivaria**, Canadá, v. 42, p. 46-67, out. 1996. Disponível em: https://archivaria.ca/index.php/archivaria/article/view/12153. Acesso em: 10 nov. 2023.

DURANTI, L. et al. Preservation as a Service for Trust. In: Security in the Private Cloud. 1st ed. CRC Press, 2016. Disponível em: https://www.researchgate.net/publication/301490739_Preservation_as_a_Service_for_Trust_PaaST. Acesso em: 22 ago. 2023.

DURANTI, L.; PRESTON, R. (Eds.). International Research on Permanent Authentic Records in Electronic Systems (*InterPARES*) 2: Experiential, Interactive and Dynamic Records. Disponível em: http://www.InterPARES.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf. Acesso em: 16 dez. 2023.

DURANTI, L.; ROGERS, C. Trust in Digital Records: An increasingly Cloudy Legal Area. **Computer Law & Security Review**, v. 28, n. 5, p. 522-531, 2012.

DURANTI, L.; RONDINELLI, R. C. Diálogo sobre Autenticidade de Documentos Digitais. In: SIMPÓSIO INTERNACIONAL DE ARQUIVOS, 2020, São Paulo, online. **Mesa Redonda:** Associação de Arquivistas de São Paulo. Disponível em: https://www.even3.com.br/conteudos/mesa-redonda--dialogo-sobre-autenticidade-de-de-documentos-digitais-569090/. Acesso em: 28 fev. 2024.

DURANTI, L.; THIBODEAU, K. The Concept of Record in Interactive, Experiential, and Dynamic Environments: The View of *InterPARES*. **Archival Science**, v. 6, n. 1, p. 13–68, 2006. DOI 10.1007/s10502-006-9021-7. Disponível em: https://www.researchgate.net/publication/225115957_The_Concept_of_Record_in_Interactive_Experiential_and_Dynamic_Environments_the_View_of_InterPARES

DURANTI, L. et al. Preservation as a Service for Trust (PaaST). In: DURANTI, L.; PRESTON, R. Security in the Private Cloud. **Boca Raton**, Flórida, CRC Press, 2016. p. 95-122. DOI: 10.1201/9781315372211-5. Disponível em: https://www.researchgate.net/publication/301490739_Preservation_as_a_Service_for_Trust_PaaST. Acesso em: 22 ago. 2023.

EASTWOOD, T. What is Archival Theory and Why is it Important. **Archivaria**, Canadá, n. 37, p. 122-130, 1994.

FUNDAÇÃO GETÚLIO VARGAS. 34ª pesquisa anual sobre o uso de TI nas empresas. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/pesti-fgvcia-2023_0.pdf. Acesso em: 28 fev. 2024.

INTERNATIONAL COUNCIL ON ARCHIVES. **Electronic Records**: A Workbook for Archivists. ICA Study 16, Paris, França; abril 2005. Disponível em: https://arxivers.com/wp-content/uploads/2018/07/ICASPA_0504_Manual_edocs_en-ICA-SPA.pdf. Acesso em: 17 out. 2023.

MACNEIL, H. et al. Authenticity Task Force Report. *InterPARES* Project. University of British Columbia, 2002. Disponível em: http://www.InterPARES.org/book/InterPARES_book_d_part1.pdf. Acesso em: 22 ago. 2024.