UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE ARQUIVOLOGIA

Glênio Vincenzo Baumhardt Varaschini

Computação na nuvem: autenticidade e acessibilidade ao longo do tempo

Santa Maria, RS
2022

Glênio Vincenzo Baumhardt Varaschini

Computação na nuvem: autenticidade e acessibilidade ao longo do tempo

Trabalho de Conclusão de Curso apresentado ao Curso de Arquivologia, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Arquivologia**.

Orientador: Prof. Ms. Sérgio Renato Lampert

Santa Maria, RS
2022

Glênio Vincenzo Baumhardt Varaschini

Computação na nuvem: autenticidade e acessibilidade ao longo do tempo

Trabalho de Conclusão de Curso apresentado ao Curso de Arquivologia, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Arquivologia**.

Aprovado em 1º de fevereiro de 2022:

_____
Sérgio Renato Lampert, Me. (UFSM)
(Presidente/Orientador)

_____
Andre Zanki Cordenonsi, Dr. (UFSM)

_____
Glaucia Vieira Ramos Konrad, Dra. (UFSM)

Santa Maria, RS
2022

RESUMO

Computação na nuvem: autenticidade e acessibilidade ao longo do tempo

AUTOR: Glênio Vincenzo Baumhardt Varaschini
ORIENTADOR: Sérgio Renato Lampert

A partir da evolução da internet, surge-se a problemática da garantia de autenticidade dos documentos digitais na nuvem. Com isso, este trabalho vem com o objetivo de elucidar algumas questões sobre deste tema, buscando analisar os serviços disponibilizados para a computação na nuvem e sua respectiva segurança em relação à autenticidade e confiabilidade dos documentos arquivísticos digitais na nuvem. A partir disso foram definidos os objetivos deste trabalho e seu respectivo referencial teórico que se baseou em quatro principais pilares: Computação na nuvem; Documento arquivístico digital; Projeto InterPARES e Preservação Digital. Diante desses pilares foram analisados diversos textos acerca do assunto, obtidos a partir da metodologia aplicada neste trabalho que é considerada aplicada, exploratória e bibliográfica. Todavia, os resultados obtidos neste estudo foram satisfatórios, uma vez que foram identificados os tipos de nuvem pública, privada, híbrida e comunitária e seus respectivos serviços SaaS, PaaS, IaaS, DaaS, CaaS, EaaS, DBaaS, FaaS e PaaST, assim como as características do documento arquivístico digital e as iniciativas identificadas para a garantia da autenticidade dos documentos na nuvem, que foram os metadados, considerados um mecanismo para auxílio da preservação com autenticidade. Além disso, o modelo de referência OAIS que serve também para auxiliar na preservação digital à longo prazo e o modelo PaaST que é apresentado como resultado do projeto InterPARES como elemento para a garantia de confiança dos documentos na nuvem, complementando o modelo OAIS.

Palavras-chave: Computação na nuvem. Documento Arquivístico Digital. Preservação Digital. Autenticidade. Acessibilidade.

ABSTRACT

Cloud computing: authenticity and accessibility over time

AUTHOR: Glênio Vincenzo Baumhardt Varaschini
ADVISOR: Sérgio Renato Lampert

From the evolution of the internet, the problem of guaranteeing the authenticity of digital documents in the cloud arises. With that, this work comes with the objective of elucidating some questions about this topic, seeking to analyze the services available for cloud computing and their respective security in relation to the authenticity and reliability of digital archival documents in the cloud. Based on this, the objectives of this work and its respective theoretical framework were defined, based on four main pillars: Cloud computing; Digital archival document; InterPARES Project and Digital Preservation. In view of these pillars, several texts on the subject were analyzed, obtained from the methodology applied in this work, which is considered applied, exploratory and bibliographical. However, the results obtained in this study were satisfactory, since the types of public, private, hybrid and community cloud and their respective services SaaS, PaaS, IaaS, DaaS, CaaS, EaaS, DBaaS, FaaS and PaaS were identified, as well as the characteristics of the digital archival document and the initiatives identified to guarantee the authenticity of documents in the cloud, which were the metadata, considered a mechanism to help in the preservation with authenticity. In addition, the OAIS reference model that also serves to assist in long-term digital preservation and the PaaST model that is presented as a result of the InterPARES project as an element to guarantee the trust of documents in the cloud, complementing the OAIS model.

Keywords: Cloud Computing. Digital Record. Digital Preservation. Authenticity.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AIP	Pacote de informação de Arquivamento
AWS	Amazon Web Services
CaaS	Comunicação como serviço
CONARQ	Conselho Nacional de Arquivos
CTDE	Câmara Técnica de Documentos Eletrônicos
DaaS	Desenvolvimento como serviço
DBaaS	Banco de dados como serviço
DIP	Pacote de Informação de Disseminação
DLF	Digital Library Federation
FaaS	Função como serviço
EaaS	Tudo como serviço
IaaS	Infraestrutura como Serviço
InterPARES	Pesquisa Internacional sobre Documentos Permanentes Autênticos em Sistemas Eletrônicos
METS	Metadata Encoding & Transmission Standard
NISO	Organização Nacional dos Estados Unidos para Padrões de Informação
OAIS	Open Archival Information System
OCLC	Non Profit Library Organization
PaaS	Plataforma como Serviço
PaaST	Preservação como serviço de confiança
PREMIS	Preservation Metadata: Implementation Strategies
RLG	Research Library Group
SAAI	Sistema Aberto para Arquivamento de Informação
SaaS	Software como Serviço
SIP	Pacote de Informação de Submissão
TIC	Tecnologias da Informação e Comunicação
XML	eXtensible Markup Language

SUMÁRIO

1 INTRODUÇÃO

Com a evolução da tecnologia e o aumento dos dados criados e disponibilizados na internet, surgem diversas questões referentes à segurança, custos e usabilidade destes dados. Desta forma, a computação na nuvem chegou como uma solução para aqueles que precisam de um maior espaço de armazenamento ou redução de custos em determinados casos. A partir do aumento de volume dos dados, surgiu a problemática da segurança e confiabilidade dos mesmos na internet, onde há a possibilidade de alteração dos arquivos sem uma gestão adequada.

A partir disso, buscou-se compreender como funcionam os serviços de utilização dos dados na nuvem, pois estes serviços estão se fazendo cada vez mais necessários devido à potencial redução de custos e de espaço físico para armazenamento de dados. Também há a necessidade de entender a computação na nuvem frente ao desafio da segurança dos dados na internet devido ao grande número de *hackers* no ambiente digital. Partindo dessa perspectiva, esta pesquisa vem com o objetivo de elucidar questões relativas à computação na nuvem, apresentando os principais serviços disponíveis e as medidas necessárias para manter os dados e documentos digitais íntegros e autênticos na internet.

Diante deste cenário, e com o grande aumento do volume de dados que circulam na internet, se torna quase impossível administrar tanta informação. Com isso, os produtores de documentos acabam deixando-os acumular devido ao grande espaço de armazenamento que se tem nos serviços disponibilizados na nuvem. Neste escopo, a pesquisa tem como tema às questões relacionadas ao uso de documentos arquivísticos digitais ante a computação na nuvem. A partir desta temática e ao considerar que com o passar do tempo o volume de dados cresce cada vez, surge o questionamento que permeia este estudo: como garantir a autenticidade e confiabilidade dos mesmos ao longo do tempo?

1.1 OBJETIVOS

1.1.1 Objetivo geral

Examinar a garantia da autenticidade dos documentos arquivísticos digitais na nuvem, a partir dos serviços disponibilizados para computação na nuvem e sua

respectiva segurança perante os documentos arquivísticos digitais na internet.

1.1.2 Objetivos específicos

Os objetivos específicos deste estudo visam:

- Distinguir os diferentes serviços disponíveis para computação na nuvem;
- Compreender o documento arquivístico digital e suas características;
- Identificar iniciativas que apresentem os elementos necessários para garantir a autenticidade e a confiabilidade dos documentos arquivísticos digitais na nuvem.

1.2 JUSTIFICATIVA

Através do tempo, cada vez mais avançamos na era digital e com isso o volume de dados cresce de forma exponencial. A partir deste crescimento, os problemas referentes aos dados e documentos arquivísticos digitais também avançaram, aflorando dúvidas em relação à sua autenticidade e confiabilidade, considerando o fato de que, por vezes, é a empresa custodiadora que transmite transparência em relação ao armazenamento de dados do produtor. Devido ao exponencial crescimento dos dados ao longo do tempo, tem-se, na visão de Duranti (2015, tradução nossa), que com o aumento da produção de dados se torna ingovernável administrar tanto volume espalhado através de múltiplas plataformas online onde a maioria dos produtores simplesmente escolhem deixar acumular. Solucionar este problema se torna cada vez mais difícil à medida que o tempo passa dada às frequentes mudanças do âmbito digital e a falta de legislação.

Diante desta falta de legislação, conforme Duranti (2014, tradução nossa), a mesma ocorre devido à globalização da internet, que dificulta a supervisão sobre a rede. A autora ainda esclarece que muitos países criaram legislações próprias para tentar barrar crimes cibernéticos e aumentar a confiabilidade dos usuários, o problema então se deu devido à falta de barreiras na internet, pois em questão de pouco tempo os dados já atravessaram fronteiras sem nenhuma fiscalização.

A partir deste grande volume de dados, Duranti (2014, p. 2, tradução nossa) apresenta o conceito de “Big data” que aparece cada vez mais conforme o volume de

dados na internet cresce. O mesmo é usado para contribuir com o setor público ou privado ocasionando vantagens para quem possui acesso à estas informações ou até mesmo auxiliando nos setores do governo e também grandes investigações. O problema aparece quando se envolvem os dados do cidadão comum que muitas vezes se expõe na internet sem tomar o devido conhecimento deste fato. Sites e empresas cada vez mais fazem o uso deste tipo de informação para fazer anúncios direcionados para certos nichos.

Atualmente, muitas empresas também buscam reduzir o espaço físico necessário para armazenamento dos dados ou até mesmo reduzir os custos para manter os dados armazenados com usabilidade ao longo do tempo.

As empresas que oferecem os serviços na nuvem, estão cada vez mais ampliando os produtos e soluções para atender à crescente demanda observada nos últimos anos. A principal delas, a Amazon - AWS já apresenta diversos serviços voltados para a pessoa física, onde se pode armazenar dados na nuvem através da contratação de seus serviços.

Em face das restrições advindas da pandemia de Covid-19, no ano de 2020, houve uma explosão na utilização destes serviços dada a necessidade do *home office*. Muitas empresas adotaram esta medida por segurança de seus funcionários e acabaram percebendo que não há necessidade em trabalhar de forma presencial, reduzindo assim, seus custos para manter um local de trabalho adequado.

Diante do aumento dos serviços disponibilizados na internet e a adesão das empresas neste ramo, a questão da autenticidade e integridade dos dados e documentos digitais não pode ser deixada para trás, haja vista o uso que se pode fazer com estas informações, para tanto este trabalho busca elucidar algumas medidas para melhorar estes aspectos com o auxílio do projeto InterPARES Trust que buscou apresentar novos conhecimentos acerca da confiabilidade e autenticidade dos documentos digitais.

Além disso, cabe salientar ainda que os materiais utilizados nesta pesquisa foram tanto em português quanto em inglês, visto que ainda há uma certa carência de publicações deste assunto no Brasil, fato este que foi relevante para a escolha do tema pelo autor, visto que a partir deste trabalho busca-se uma maior visibilidade para o tema na área da Arquivologia.

2 REFERENCIAL TEÓRICO

Neste capítulo, foram apresentados conceitos que dão sustentação à pesquisa, tais como: Computação na nuvem; Documento arquivístico digital; Projeto InterPARES e Preservação digital.

2.1 COMPUTAÇÃO NA NUVEM

Possuindo diversas definições de diferentes autores, a computação na nuvem vem cada vez ganhando mais espaço no cenário mundial devido a globalização da internet. Segundo (BORGES et al.., 2011, p. 3) “a computação em nuvem pode ser definida, de forma simplificada, como um paradigma de infraestrutura.” Este paradigma então possibilitaria o uso dos serviços hoje disponíveis para a nuvem, como por exemplo o SaaS – Software como serviço; PaaS – Plataforma como serviço e entre outros que apresentam vantagens específicas que foram abordadas no decorrer deste trabalho.

Segundo os autores Vaquero et al. (2009, p. 51) Após a análise de diversas definições propostas, chegaram à conclusão de que as “nuvens” são “uma grande piscina de recursos virtualizados de fácil uso e acesso.” Facilmente adaptáveis a qualquer situação, esses recursos apresentaram uma vasta economia para quem fizer seu uso, visto que não são necessários altos investimentos em servidores ou computadores.

Oferecendo serviços que não demandariam alto poder de processamento, os recursos propostos, em sua maioria, necessitam apenas de acesso à internet. Retirando assim diversos custos que se fazem necessários para a criação um servidor para armazenamento de dados, por exemplo.

Atualmente ainda há muito uso nos computadores de forma “on premise”, ou seja, de maneira que é necessário a instalação dos programas e aplicativos diretamente no aparelho, necessitando assim de mais espaço e também restringindo o acesso somente ao computador em que as aplicações estão instaladas, por outro lado o “on premise” permite a execução de tarefas sem o acesso à internet (ALECRIM, 2008).

Com a implementação da computação nas nuvens os aplicativos à depender de seu uso podem ou não, serem instalados na máquina, além disso, este tipo de

serviço possibilita a não necessidade de manutenção, atualização, segurança, backup e outras medidas que ocasionariam mais gastos para o contratante do serviço. Essas tarefas ficariam então, sob a responsabilidade do fornecedor, restando-se ao usuário somente desfrutar do serviço contratado.

2.2 O DOCUMENTO ARQUIVÍSTICO DIGITAL

Para melhor compreender o documento arquivístico digital, primeiramente faz-se necessário apresentar o conceito de documento, que segundo o Dicionário Brasileiro de Terminologia Arquivística (ARQUIVO NACIONAL, 2005, p. 73) é a "unidade de registro de informações qualquer que seja o suporte ou formato". Por outro lado, o glossário de terminologia do Projeto InterPARES 3 (INTERPARES PROJECT 3, 2012) definiu documento como "uma unidade indivisível de informação constituída por uma mensagem fixada num suporte (registrada) com uma sintaxe estável. Um documento tem forma fixa e conteúdo estável".

Compreendido o conceito de documento, buscou-se entender a definição de documento arquivístico. Assim, segundo o Glossário da Câmara Técnica de documentos eletrônicos – CTDE (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 24) este é tido como o "documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência". Por outro lado, tem-se a definição por parte do Conselho Internacional de Arquivos, que compreendeu documento arquivístico como "documento produzido ou recebido e mantido por uma agência, organização ou indivíduo em cumprimento de obrigações legais e transações de negócios" (INTERNATIONAL COUNCIL OF ARCHIVES, 2010 apud RONDINELLI, 2013, p. 204).

A partir dessa contextualização, procurou-se assimilar o conceito de documento digital. Para o Glossário da CTDE (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 25), documento digital é a "informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional". Diante disso, temos a definição proposta pelo Arquivo Nacional, a qual definiu documento digital como o "documento codificado em dígitos binários, acessível por meio de sistema computacional" (ARQUIVO NACIONAL, 2005, p. 75).

Mesmo não sendo objeto da pesquisa, é relevante apresentar o conceito de documento eletrônico, a fim de demonstrar a diferença para o documento digital. Assim sendo, documento eletrônico é a “informação registrada, codificada em forma analógica ou em dígitos binários, acessível e interpretável por meio de um equipamento eletrônico” (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 25).

A partir destes princípios, notou-se que, a principal diferença entre estes dois tipos de documento se faz por seu suporte, uma vez que o documento eletrônico não precisa ser necessariamente reproduzido em um sistema computacional, como por exemplo, uma fita que torna necessário o uso de um aparelho específico para sua reprodução. Ao contrário do documento digital que tem sua codificação em bits e possibilita sua leitura somente através de sistemas computacionais.

Elencadas as definições de documento, documento arquivístico e documento digital/eletrônico, passou-se à definição de documento arquivístico digital. Segundo Rondinelli (2013, p. 235), o conceito de documento arquivístico digital surgiu a partir de uma junção de conceitos:

> Unidade indivisível de informação constituída por uma mensagem fixada num suporte (registrada), com uma sintaxe estável, produzida e/ou recebida por uma pessoa física ou jurídica, no decorrer de suas atividades, codificada em dígitos binários e interpretável por um sistema computacional em suporte magnético, óptico ou outro.

Neste escopo, o Conselho Nacional de Arquivos (2020) definiu o Documento Arquivístico digital como o “documento digital reconhecido e tratado como um documento arquivístico.”

A partir dos conhecimentos elencados nesta subseção, faz-se necessário apresentar o Projeto InterPARES, cujo resultado das pesquisas que utilizaram conhecimentos prévios da Diplomática e da Arquivologia como base originou boa parte dos conceitos apresentados neste capítulo.

2.3 PROJETO INTERPARES

Surgindo a partir da necessidade de preservação digital voltada para documentos arquivísticos, o projeto InterPARES criado em 1999, surgiu a partir da criação do projeto “*The preservation of integrity of electronic records*”, desenvolvido entre 1994 e 1997 na UBC – University of British Columbia. Este projeto tinha o objetivo de identificar e definir os requisitos necessários para produção, uso e

preservação à longo prazo de documentos eletrônicos confiáveis e autênticos, utilizando de conhecimentos teóricos provenientes da diplomática e da arquivística. (ROCHA, 2009).

Com o término do projeto, Luciana Duranti, então propôs um projeto colaborativo internacional reunindo as áreas de Arquivologia, Direito, Engenharia, Ciência da informação, História e Ciência da computação. Assim, o projeto InterPARES teve seu início oficial em 1999, onde na sua primeira fase, trouxe como objeto principal os documentos arquivísticos digitais “tradicionais”, ou seja, aqueles mantidos em bases de dados e sistemas de gestão de documentos.

Já na segunda fase do projeto, realizada entre 2002 e 2006, apresentou-se como eixo os documentos arquivísticos originados em ambientes complexos, por sistemas interativos, dinâmicos e experienciais. Tratando não só de autenticidade, mas também de confiabilidade e acurácia, se envolveu todo o ciclo de vida dos documentos, desde sua produção até sua destinação final (ROCHA, 2009).

Na terceira fase do projeto, iniciada em 2007, o objetivo foi testar aquilo que foi originado a partir das duas outras fases do projeto. Com diversos estudos de caso sendo produzidos com base na análise diplomática, o objetivo desta fase foi desenvolver planos de ação para casos específicos de conjuntos documentais (ROCHA, 2009).

Diante destas linhas, apresenta-se a quarta fase do projeto, denominada InterPARES Trust que iniciou em 2012 e estendeu-se até 2019. Esta fase tratou-se de uma pesquisa interdisciplinar e multinacional que visava explorar as questões relativas aos documentos e registros digitais, assim como os dados confiáveis na internet.

Segundo Indolfo e Lopes (2015, p.11-12), o iTrust como é conhecido, tem o objetivo de “apoiar o desenvolvimento de redes integradas e consistentes no estabelecimento de políticas, regras, leis, procedimentos e padrões para documentos arquivísticos digitais e dados confiados à internet.” Neste escopo então se faz o principal foco do projeto que visa analisar especialmente aqueles documentos armazenados na nuvem e em mídias sociais.

Nesta linhagem então, a pesquisa buscou investigar os benefícios e riscos de conservar os documentos arquivísticos armazenados na nuvem. A partir disso, os pesquisadores então basearam-se em conhecimentos prévios disponibilizados pela diplomática, assim como dos estudos jurídicos sobre documentos arquivísticos. Ainda, buscou-se também a aplicação e utilização dos resultados obtidos nas outras fases

do Projeto.

Ao considerar os objetivos e resultados do Projeto, busca-se a seguir abordar a temática da preservação digital enquanto elemento a ser considerado no contexto do documento arquivístico digital.

2.4 PRESERVAÇÃO DIGITAL

Neste escopo do projeto InterPARES, a preservação digital se apresentou como um dos principais objetivos que pautaram a pesquisa idealizada neste projeto que visava preservar os documentos arquivísticos digitais. A partir disso, apresentou-se a definição de preservação, que para o glossário do Projeto InterPARES 3 (INTERPARES PROJECT 3, 2012), traduzido pela equipe brasileira, é o “conjunto de princípios, políticas e estratégias que orienta as atividades projetadas para assegurar a estabilidade física e tecnológica e a proteção do conteúdo intelectual dos materiais (dados, documentos ou documentos arquivísticos)”.

Com a finalidade de complementar o conceito acima, tem-se que preservação é a “prevenção da deterioração e danos em documentos, por meio de adequado controle ambiental e/ou tratamento físico e/ou químico” (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 25). A partir das colocações elencadas, percebeu-se a semelhança entre os dois conceitos que visam garantir a preservação por meio de um conjunto de princípios e técnicas arquivísticas.

Diante disso, apresentou-se então a definição de preservação digital que segundo o glossário brasileiro do Projeto InterPARES se definiu por “processo específico de manutenção de materiais digitais ao longo do tempo e através de diferentes gerações de tecnologia, independentemente do local de armazenamento” (INTERPARES PROJECT 3, 2012). Por outro lado, a CTDE (2020, p. 39) definiu a preservação digital como o “conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário”.

Contudo, o e-ARQ Brasil (CONSELHO NACIONAL DE ARQUIVOS, 2011, p. 220) define a preservação digital como “conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo acesso e interpretação dos documentos digitais pelo tempo que for necessário”.

Já Ferreira (2006, p. 20) define a preservação digital como “conjunto de actividades ou processos responsáveis por garantir o acesso continuado a longo-prazo à informação e restante património cultural existente em formatos digitais.” E ainda complementa argumentado que a mesma “consiste na capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação” (FERREIRA, 2006, p. 20).

A partir dessas definições, pôde-se perceber que o objetivo da preservação digital é garantir a acessibilidade dos materiais digitais pelo maior período de tempo possível perpassando diferentes gerações tecnológicas as quais vivenciamos ao passar dos anos.

Depois de apontar os componentes teóricos que subsidiam a pesquisa, a seguir é apresentada a metodologia adotada.

3 METODOLOGIA

Neste capítulo apresenta-se a metodologia utilizada para realização desta pesquisa que tem como objetivo geral examinar a garantia da autenticidade dos documentos arquivísticos digitais na nuvem, a partir dos serviços disponibilizados para computação na nuvem e sua respectiva segurança perante os documentos arquivísticos digitais na internet. Diante deste objetivo, esta pesquisa se desenvolveu através de revisão bibliográfica a partir de materiais referentes a temática da pesquisa.

Dessa maneira, a pesquisa realizada é considerada aplicada, uma vez que segundo Silva et al. (2001, p. 20) a mesma objetiva “gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos”. Em relação à sua classificação, este estudo é qualitativo, onde SILVA et al. (2001, p. 20) considera que “há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números”.

Além disso, este estudo busca trazer uma pesquisa de caráter exploratório realizada a partir de outros materiais já publicados, seja em livros ou artigos, buscando a ampliação dos conhecimentos acerca da problemática deste trabalho. Onde segundo GIL (2002, p. 41) a pesquisa de caráter exploratório tem como objetivo “proporcionar maior familiaridade com o problema com vistas a torná-lo mais explícito ou a constituir hipóteses.

Além disso, esta pesquisa se apresenta como bibliográfica, uma vez que foi realizada a partir dos livros e artigos de periódicos que já haviam sido publicados previamente (GIL, 2002).

No tocante as etapas da pesquisa, primeiramente foi definida a temática, problemática e os objetivos gerais e específicos deste estudo. A seguir, diante da definição do tema, foram realizadas pesquisas nas bases Scielo[1] e BrapCi[2] pelo termo “computação na nuvem”. Na primeira base obteve-se 20 resultados e destes filtrou-se apenas 2 trabalhos, já na segunda a busca pelo termo resultou em 9 trabalhos, que a partir da filtragem se obteve um artigo. A filtragem aqui se deu através de uma rápida leitura nos materiais obtidos nas bases de pesquisa.

[1] Disponível em: <https://www.scielo.org/>.
[2] Disponível em: <https://www.brapci.inf.br/>.

Além das bases mencionadas, foi realizada também uma consulta no Google Scholar[3]. Em um primeiro momento, ao buscar pelo termo “computação na nuvem”, obteve-se 24.600 resultados. Ao adicionar o termo “arquivologia”, a consulta apresentou 417 resultados. Destes 417 materiais, buscou-se ler alguns parágrafos dos textos para identificar aqueles que seriam mais pertinentes ao trabalho, resultando assim, em um total de cinco trabalhos para agregar à pesquisa.

Com base nas publicações encontradas e no livro[4] “O documento arquivístico ante a realidade digital: uma revisão conceitual necessária” e nos materiais disponíveis nos sites do Projeto InterPARES e InterPARES Trust foi desenvolvido o referencial teórico sobre computação na nuvem, documento arquivístico digital, Projeto InterPARES e preservação digital. Este referencial serviu como base para o desenvolvimento de todo o estudo, visto que estes quatro elementos se fazem essenciais para a pesquisa objetivada.

Neste escopo, a partir dos objetivos elencados para obtenção dos resultados, foram analisados alguns referenciais teóricos que indicavam os tipos de modelos e serviços na nuvem. Salienta-se que essa etapa foi desenvolvida no segundo semestre de 2021.

Por outro lado, para desenvolvimento dos resultados acerca do documento arquivístico digital, foram usados alguns referenciais encontrados nas bases já citadas anteriormente e no livro “O documento arquivístico ante a realidade digital” de Roselly Rondinelli, que serviu como uma grande base para este estudo.

Ainda em relação as etapas voltadas para o atingimento dos resultados, para identificação das iniciativas para a garantia de autenticidade dos documentos na nuvem foram utilizadas as mesmas fontes bibliográficas das outras etapas. Salienta-se que houve uma delimitação do conteúdo, principalmente, em relação ao modelo PaaST, resultado do projeto InterPARES, em virtude de haver material apenas em língua inglesa, os quais foram traduzidos pelo autor desta pesquisa.

Conforme apresentado nesta seção, a seguir são apresentadas as etapas da pesquisa, no Quadros 1 e 2, abaixo:

---

[3] Disponível em: <https://scholar.google.com.br/>.
[4] RONDINELLI, 2013.

Quadro 1 – Etapas do Trabalho de Conclusão de Curso A

Etapas da pesquisa	**Mês/ano**
Definição do tema e problemática de pesquisa	Abril/2021
Elaboração do Referencial Teórico	Maio/2021
Fichamento Bibliográfico	Junho/2021
Escrita da Introdução e objetivos da pesquisa	Julho/2021
Escrita do Referencial, Metodologia, Recursos e Cronograma	Agosto/2021

Fonte: Autor (2021).

No Quadro 1 acima, foram apresentados o cronograma das etapas da pesquisa realizada na disciplina de Trabalho de Conclusão de Curso A. Já no Quadro 2 abaixo, são apresentadas as etapas realizadas na disciplina de Trabalho de Conclusão de Curso B.

Quadro 2 – Etapas do Trabalho de Conclusão de Curso B

Etapas da pesquisa	**Mês/ano**
Identificação dos serviços e modelos de nuvem	Outubro e Novembro/2021
Compreensão do documento arquivístico digital	Dezembro/2021
Identificação das iniciativas voltadas para autenticidade de documentos na nuvem	Dezembro/2021 e Janeiro/2022
Finalização e conclusão da pesquisa	Janeiro/2022

Fonte: Autor (2022).

Em relação à coleta e análise dos dados, estes foram coletados a partir de fichamento bibliográfico e foram avaliados com base no marco teórico, buscando solucionar a problemática da pesquisa e atingir os objetivos desta conforme os elementos teóricos e metodológicos estabelecidos no âmbito do estudo. Concluída a etapa de análise dos dados, a sistematização dos resultados e elaboração do trabalho textual foi desenvolvida e é apresentada em forma de trabalho de conclusão de curso.

4 RESULTADOS

Neste capítulo são apresentados os resultados obtidos na pesquisa bibliográfica proposta neste trabalho. A partir disso, nesta subseção que se refere aos serviços na nuvem, são apresentados os tipos de nuvem e os serviços disponibilizados. Nas subseções seguintes são apresentados os resultados a respeito do documento arquivístico digital e suas características, assim como sobre autenticidade e acessibilidade dos documentos digitais na nuvem.

4.1 SERVIÇOS NA NUVEM

Nesta seção serão abordados os tipos de nuvens existentes atualmente e suas diferenças, além de se apresentar também os serviços disponíveis no uso da nuvem. Atualmente, são quatro modelos de nuvens principais: a) Nuvem Pública; b) Nuvem Privada; c) Nuvem Híbrida; d) Nuvem comunitária. Apresentados os quatro principais tipos de nuvem, será então abordado os serviços disponibilizados na nuvem, onde atualmente, existem três principais serviços relevantes: a) SaaS; b) IaaS; c) PaaS. Além disso, mais alguns outros serviços também serão apresentados ao decorrer deste subcapítulo.

Diante destes esclarecimentos, a seguir serão apresentados os tipos de nuvem existentes na atualidade e também os serviços que estão disponíveis para contratação no mercado.

A partir dos conhecimentos elencados no referencial teórico desta pesquisa, chega-se aos diferentes serviços de computação na nuvem. Dessa forma, os modelos de serviço apresentam características específicas para determinadas situações, que começam a se definir a partir da escolha do tipo de nuvem que será usada.

Neste quesito, há quatro tipos de modelos de implementação na nuvem com características distintas conforme definido por Veras (2013, p. 56-57). A primeira delas, a nuvem pública (*Public Cloud*), é definida pelo autor como “modelo pague-por-uso. São oferecidas por organizações públicas ou por grandes grupos industriais que possuem grande capacidade de processamento e armazenamento”. Além disso, o autor ainda salienta que na época da publicação (2013), cerca de 38% das organizações estavam avaliando a adoção das nuvens públicas.

Por outro lado, Pontes (2014) define a nuvem pública como sendo:

> É um modelo de computação em nuvem que distribui para o usuário que deseja processar, armazenar e/ou compartilhar seus dados em um sistema que forneça recursos da TI. Toda infraestrutura é oferecida como um serviço de informação, onde outros usuários poderão ou não ter acesso (PONTES, 2014, p. 81).

A partir das colocações dos autores, pode-se perceber que a nuvem pública é uma boa opção para aqueles que desejam ter custos reduzidos ao utilizar dos serviços da nuvem.

O segundo modelo, chamado de Nuvem privada (*Private Cloud*) é definido como uma infraestrutura de nuvem utilizada exclusivamente por instituições, podendo ser gerenciada através de um sistema local ou remoto e controlado pela própria empresa ou por terceiros. Além disso, junto com as políticas de acesso, a responsabilidade desta nuvem é da instituição que a mantém, podendo assim gerar mais risco ao contratante (PONTES, 2014).

Todavia, Veras (2013, p. 56) complementa que, “os serviços são oferecidos para serem utilizados pela própria organização, não estando publicamente disponíveis para uso geral. Em alguns casos pode ser gerenciada por terceiros.” Diante das colocações apontadas pelos autores, a nuvem privada se apresenta com maior segurança em relação à nuvem pública, porém seu custo também será mais elevado devido a este fato.

A partir das colocações acima citadas, apresenta-se a nuvem comunitária, que se define por ser, na visão de Veras (2013):

> Compartilhada por diversas organizações e suporta uma comunidade que possui interesses comuns. A nuvem comunitária pode ser administrada pelas organizações que fazem parte da comunidade ou por terceiros e pode existir tanto fora como dentro das organizações (VERAS, 2013, p. 57).

Além disso, Pontes (2014) ainda complementa que a nuvem comunitária é “uma comunidade exclusiva que compartilha seus interesses como: a missão, requisitos de segurança, políticas, entre outros. Essa infraestrutura pode ser gerida pelas próprias instituições ou por terceiros que ofereçam o serviço de gerenciamento.” Nesta premissa, percebe-se o fato de que a nuvem comunitária é uma boa alternativa para aqueles que desejam reduzir seus custos, mas ainda assim manter a integridade da infraestrutura, visto que, só participaria aqueles que compartilham das mesmas missões.

Por último, mas não menos importante, surge a nuvem hibrida que se define por “uma composição de duas ou mais nuvens (privadas, públicas ou comunitárias)

que continuam a ser entidades únicas, porém, conectadas através de tecnologias proprietárias ou padronizadas que propiciam a portabilidade de dados e aplicações" (VERAS, 2013, p. 57).

Em outras palavras, a nuvem hibrida propiciaria o compartilhamento de dados a partir de uma nuvem privada para uma nuvem pública ou comunitária, a depender das configurações de seu proprietário possibilitando assim a execução de aplicações na nuvem pública e o armazenamento de dados na nuvem privada (PONTES, 2014).

A partir do exposto a respeito dos tipos de nuvem existentes, faz-se necessário apresentar o conceito de virtualização, já que o mesmo é empregado na computação em nuvem. Todavia, Taurion (2009) explica como a virtualização está relacionada com a computação na nuvem:

> Uma tecnologia fundamental ao conceito de nuvem é a virtualização, que é basicamente o uso de software para simular hardware. Quando alugamos os serviços de uma nuvem, na prática não estamos alugando diretamente computadores reais, mas computadores virtuais que existem simulados pelo software, que opera em cima dos computadores reais da infraestrutura do provedor da nuvem (TAURION, 2009, p. 99).

Diante do exposto, pode-se perceber que os serviços em nuvem são, em sua maioria, de uma virtualização, ou seja, ao alugar um servidor que não seja local, já estará se fazendo uso da nuvem e da virtualização que simulará o *hardware*. Esta estrutura disponibilizada pela virtualização, possibilita o uso de grandes estruturas flexíveis para armazenamento e processamento de dados com alta segurança sem necessariamente ter grandes custos para tal.

A partir dessa virtualização, começa-se então a apresentação dos serviços na nuvem mencionados no referencial deste estudo. Nesta premissa, faz-se necessário citar Pedrosa e Nogueira (2011), que definem os serviços de computação na nuvem em três classes que levam em consideração o nível de abstração dos recursos providos e também o modelo de serviço do provedor.

Complementando, os autores ainda salientam que:

> O nível de abstração pode ser visto como a camada de arquitetura onde os serviços das camadas superiores podem ser compostos pelos serviços das camadas inferiores. As três classes de serviço são nomeadas da seguinte forma: Infra-estrutura como Serviço (IaaS), camada inferior; Plataforma como Serviço (PaaS), camada intermediária; e Software como Serviço (SaaS), camada superior (PEDROSA; NOGUEIRA, 2011, p. 2)

O serviço da camada mais alta da arquitetura computacional em nuvem,

conforme destacam Pedrosa e Nogueira (2011) é o SaaS – *Software as a Service* (*Software* como serviço). Definido por Veras (2013, p. 223) o SaaS é “uma modalidade de serviços de nuvem onde os aplicativos de interesse para uma grande quantidade de usuários passam a ser hospedados na nuvem como uma alternativa ao processamento e armazenamento local”.

Trata-se de um *software* que é vendido como serviço para as empresas, sendo que a empresa que o contrata paga uma mensalidade para possibilitar sua utilização. Esta mensalidade dará o direito ao contratante de utilizar o *software* e não precisar se atentar as responsabilidades advindas da utilização desse serviço, como monitoramentos, *backups*, atualizações e a própria segurança. Isto tudo estaria incluso então na mensalidade, que se torna um benefício tanto para o fornecedor quanto para o cliente, uma vez que o preço será de acordo com a quantidade de clientes e a estrutura que será necessária (SANTOS, 2014).

Complementando o entendimento acima, tem-se como exemplo para o SaaS os aplicativos da família Google Cloud, como o Gmail, Google Docs, Google Drive, entre outros (PONTES, 2014). Estes serviços oferecidos pelo Google mostram-se com grande potencial de utilização, uma vez que possibilitam o uso remoto e compartilhado de diversas aplicações úteis no cotidiano.

O outro serviço na nuvem, sendo este da camada intermediária, é o PaaS – *Platform as a Service* (Plataforma como serviço). Neste tipo de serviço, o fornecedor proverá uma plataforma para desenvolvimento de softwares e hospedagem de aplicativos, oferecendo um amplo conjunto de recursos que possibilitarão o desenvolvimento, teste, implementação, execução e atualização de diferentes tipos de sistemas (ALECRIM, 2008).

A partir dessa contextualização, Veras (2013, p.199) define o PaaS como um conjunto “de ferramentas de desenvolvimento de *software* oferecidas por provedores de serviços, onde os desenvolvedores criam as aplicações e as desenvolvem utilizando a Internet como meio de acesso.” Cabe salientar ainda, que este tipo de serviço conversa diretamente com o SaaS, uma vez que o PaaS serviria como um suporte para o SaaS, devido às suas possibilidades de realização de testes de *software* na nuvem, sem precisar de grandes recursos para tal (PONTES, 2014).

Veras (2013, p. 201) apresenta como exemplo da utilização do PaaS o Microsoft Windows Azure, definido como “uma plataforma que pode ser usada para a execução de aplicações Windows e o armazenamento de dados na nuvem”. Neste

caso, os clientes que o utilizarem executarão e armazenarão suas aplicações e dados nos servidores da Microsoft que ficam localizados, segundo Veras (2013), na Ásia, Europa e Estados Unidos e passam pelo gerenciador de tráfego que escolherá a melhor região para o contratante do serviço.

A partir das definições elencadas pelos autores, pode-se perceber que o PaaS se mostra uma ótima alternativa para os desenvolvedores, uma vez que os mesmos poderão realizar testes em suas aplicações sem a necessidade de utilizar grandes espaços de armazenamento para tal, mas por outro lado, ficarão reféns de uma grande empresa que estará com a responsabilidade do sistema contratado.

Depois de apresentar os níveis de abstração das camadas superior e intermediária, tem-se o serviço na nuvem da camada inferior, denominado IaaS – *Infrastructure as a Service* (Infraestrutura como serviço). Similar ao PaaS, o IaaS tem como objetivo o fornecimento de uma infraestrutura com grandes recursos, viabilizando a implementação dos serviços na nuvem (ALECRIM, 2008). Neste caso o fornecedor proveria servidores, espaços para armazenamento e capacidade de rede, gerando assim um datacenter, retirando a responsabilidade do cliente de disponibilidade do servidor, energia elétrica, entre outros fatores que ficariam a cargo do provedor da infraestrutura (SANTOS, 2014).

A fim de complementar este entendimento, Pedrosa e Nogueira (2011) compreendem que o IaaS contempla:

> Serviços de infra-estrutura sob demanda, isto é, oferece recursos “de hardware” virtualizados como computação, armazenamento e comunicação. Este tipo de serviço provê servidores capazes de executar softwares customizados e operar em diferentes sistemas operacionais (PEDROSA; NOGUEIRA, 2011, p. 2).

Neste sentido, Veras (2013) complementa que:

> Neste cenário, os usuários da organização não têm o controle da infraestrutura física, mas, através de mecanismos de virtualização, possuem controle sobre as máquinas virtuais, armazenamento, aplicativos instalados e possivelmente um controle limitado dos recursos de rede (VERAS, 2013, p. 170).

A partir destas definições apontadas pelos autores, é possível perceber que a adoção deste serviço propiciará uma melhora no sistema como um todo e também no controle pelo detentor do sistema, pelo fato de o serviço oferecido ser uma completa infraestrutura de serviços na nuvem. Com isso, o IaaS possibilita uma grande

variedade de recursos para viabilizar a implementação de serviços na Cloud com segurança.

Como exemplo para o IaaS, tem-se o AWS - Amazon Web Services, que segundo Veras (2013) apresenta serviços que “permitem o acesso a recursos de computação, armazenamento e banco de dados e outros serviços de infraestrutura *on demand*.” Cabe salientar que segundo o próprio autor, estes serviços vêm sendo desenvolvidos desde 2006 e são os únicos a oferecerem esta tipologia de serviço com foco na infraestrutura como serviço.

Além dos serviços acima citados, com o atual crescimento da internet mais serviços vão surgindo e faz-se necessário apresentar alguns deles, que segundo Pontes (2014) são:

- DaaS – Desenvolvimento como um serviço: É um serviço que fornece ferramentas de desenvolvimentos de aplicativos de forma simples e compartilhada. Um exemplo deste serviço é o Cloud 915 ou Outsystem16;
- CaaS – Comunicação como um Serviço: São serviços de comunicação unificada para ambientes corporativos oferecidos pelos provedores e fabricantes. Exemplos: VOIP, Chat, SMS-Mail e outros;
- EaaS – Tudo como um Serviço: É a utilização de todas as tipologias de serviço para desenvolvimento da T.I.C.

Santos (2014) ainda complementa com mais dois tipos de serviço na nuvem:

- DBaaS – Banco de dados como serviço: Apresenta um banco de dados, onde o responsável por prover o serviço, oferece licenciamento, atualizações, segurança, replicação, performance e disponibilidade. Como exemplo para esse serviço, tem-se o Amazon Aurora e também o Google Firebase;
- FaaS – Função como serviço: Este serviço permite a execução de pequenos pedaços de código na nuvem sob demanda, aumentando assim sua escalabilidade. Como exemplo prático, pode-se apresentar um app de reservas para um restaurante, onde em determinados horários haverá picos de usabilidade e neste caso, esse serviço resolveria.

Além disso, conforme abordado anteriormente na justificativa deste estudo, é importante ressaltar que apesar dos benefícios, a computação na nuvem apresenta algumas fragilidades, como o acúmulo do volume de dados. Sobre este tema, Duranti (2015) explica que se torna cada vez mais difícil controlar os dados devido à falta de legislação e as frequentes mudanças do âmbito digital. A partir desta ideia e diante de um grande volume de dados, surge a questão da preservação digital pelo fato de possuir um grande papel a respeito da segurança e integridade destes dados.

Diante do exposto, a respeito dos serviços disponíveis para utilização na nuvem e com o grande crescimento do volume de dados na internet, surge o questionamento sob à ótica da arquivística de como garantir a autenticidade e acessibilidade dos documentos ao longo do tempo. Além dos conhecimentos arquivísticos necessários para este fim, o profissional da informação também deverá ter habilidades no campo da informática para possibilitar o prosseguimento do processo de preservação.

Partindo desta premissa, surge a necessidade de padronização da preservação e com isso chega o modelo de referência para preservação OAIS[5] (Open Archival Information System). Este modelo, foi então desenvolvido para orientar a preservação e a manutenção do acesso à informação digital no longo prazo (THOMAZ e SOARES, 2004).

A partir dos conhecimentos elencados acima, o projeto InterPARES, criado para investigar os requerimentos para a preservação digital, considera que a norma OAIS é um modelo abstrato que falta detalhes para sua implementação. Considerando isso, o modelo PaaST – *Preservation as a Service for Trust*, (Preservação como serviço de Confiança), descreve um modelo e especificações que podem ser implementadas em *software*.

Apresenta-se como um projeto que aborda diretamente os desafios da preservação digital na nuvem (DURANTI et al., 2016, tradução nossa). Os requisitos do PaaST foram criados especificamente para permitir que os responsáveis pela preservação de informações digitais confiem essas informações a provedores de serviços em nuvem (DURANTI et al., 2016, tradução nossa).

Este modelo, então desenvolvido pelo Projeto InterPARES Trust, acaba definindo os requisitos funcionais e de dados que podem ser incorporados nos contratos para preservação com provedores de serviço em nuvem. Por outro lado, os

[5] Norma ISO internacional 14721 lançada em 2003 e publicada no Brasil como Norma ABNT NBR 15472 SAAI Sistema Aberto para Arquivamento de Informação em 2007.

benefícios potenciais acabam não se limitando somente à nuvem, mas sim para a mais ampla variedade de situações (ITrustAI, 2016, tradução nossa).

Esta variedade de situações inclui heterogeneidade nos tipos de objetos da informação a serem preservados, variedade na aplicação de diretrizes, como leis, regulações, políticas, acordos contratuais. Além disso, este modelo inclui variedades de propriedade, acesso, uso e exploração e também variação nos arranjos institucionais e seus relacionamentos entre as partes envolvidas (ITrustAI, 2016, tradução nossa).

A partir dos conhecimentos elencados nesta subseção da pesquisa, para melhor compreender os serviços existentes, apresenta-se um quadro comparativo entre os diferentes serviços apontados (Quadro 3):

Quadro 3 – Modelos de serviço em nuvem

Modelos de serviço	**Sigla**	**O que é?**
Software	SaaS	Hospeda aplicativos para o usuário como um serviço.
Plataforma	PaaS	Oferece uma plataforma para desenvolvimento de aplicativos, banco de dados e serviços na *Web*.
Infraestrutura	IaaS	Recursos para o usuário final aumentar seu poder de *Hardware*.
Desenvolvimento	DaaS	Ferramentas para desenvolvimento de aplicativos de forma simples e compartilhada.
Comunicação	CaaS	Comunicação unificada para ambientes corporativos.
Tudo (*Everything*)	EaaS	Utilização de todos os serviços para o desenvolvimento das empresas de Tecnologia da Informação e Comunicação.
Banco de dados	DBaaS	Banco de dados como serviço para aumentar a capacidade de armazenamento.
Função	FaaS	Permitir a execução de códigos sob demanda para escalabilidade
Preservação	PaaST	Preservação como serviço de confiança com modelo e especificações para implementação em *software.*

Fonte: Autor (2021).

Após explanar sobre os modelos de nuvem e os serviços atualmente disponíveis, passa-se então aos resultados obtidos na pesquisa sobre o documento arquivísticos digital.

4.2 O DOCUMENTO ARQUIVÍSTICO DIGITAL E SUAS CARACTERÍSTICAS

Com base na diplomática, Rondinelli (2013) destacou que o documento arquivístico digital tem as mesmas características que seu correlato em papel: a) Forma fixa; b) Conteúdo estável; c) Relação orgânica; d) Contexto identificável; e) Ação; f) Envolvimento de até 5 pessoas. A seguir, serão apresentados conceitos e definições acerca de cada característica.

Diante deste contexto, apresentou-se a ontologia do documento arquivístico digital proposta pelo Projeto InterPARES 2, e o dividiu em três principais componentes, que são: a) Componentes Intelectuais; b) Atributos; c) Componentes Digitais. Dentro destes componentes, segundo o projeto, há mais sete atributos ao qual o documento deve-se ter, que são os atos, pessoas, seu vínculo com o arquivo, contexto, conteúdo, meio de registro e sua forma.

As pessoas ao qual o projeto InterPARES se referiu, precisariam estar envolvidas desde a criação do documento e requerem autor, redator e destinatário para tal. Já o contexto do projeto definiu que há uma hierarquia contextual que vai do geral ao específico e se divide em cinco principais contextos, jurídico-administrativo, de proveniência, de procedimento, documental e tecnológico. Além destes contextos o projeto ainda definiu a forma documental em duas partes, a primeira seria a forma intelectual caracterizando os elementos intrínsecos do documento, como seu título, data, assunto, entre outros. A outra seria a forma física do documento, que caracterizaria os elementos extrínsecos, onde o documento sempre teria suporte, texto, linguagem e também poderia ter símbolos específicos e anotações (DURANTI, 2015, p. 198).

Sobre as pessoas participantes do documento arquivístico digital, Rondinelli (2013) explica que ao menos três (autor, redator e destinatário), das cinco pessoas[6] necessitariam estar presentes no documento arquivístico. Em relação a forma fixa e

[6] Autor, redator, destinatário, originador e produtor.

conteúdo estável, a autora salienta que os documentos precisariam manter a mesma apresentação de quando foram “salvos” pela primeira vez.

A partir disso, se faz necessário apresentar as definições de forma fixa e conteúdo estável. Segundo o Projeto InterPARES 3 a forma física seria a “característica de um documento arquivístico que assegura que sua aparência ou apresentação documental permanece a mesma cada vez que o documento é manifestado, ou pode ser alterada segundo regras fixas.” (PROJECT INTERPARES 3, 2007). Diante disso, o Projeto InterPARES 3 (2007, p. 6) definiu que em um documento com conteúdo estável “os dados e a mensagem no documento arquivístico são originais e imutáveis, o que significa que as informações não podem ser sobrescritas, alteradas, apagadas ou receber adições”. Ou seja, o documento necessitaria estar da mesma forma de quando foi elaborado, recebido ou salvo pela primeira vez.

No que se refere à relação orgânica, Duranti e Thibodeau (2008) a definiram como:

> Uma característica eminentemente arquivística e que se encontra implícita no conceito de documento arquivístico, na medida em que, de acordo com esse conceito, os documentos se constituem em registros de atividades e, consequentemente, mantém um vínculo inextricável entre si. No caso do documento arquivístico digital, essa vinculação se dá entre documentos dentro e fora do sistema, isto é, nos chamados ambientes híbridos os quais se caracterizam por abranger documentos digitais e não digitais ao mesmo tempo (DURANTI; THIBODEAU, 2008 apud RONDINELLI, 2013, p. 236).

Já em relação ao contexto identificável, Rondinelli (2013, p. 236) o definiu como “uma hierarquia de estruturas fora do documento arquivístico na qual se dá sua produção e gestão”. Para a CTDE (2010, p. 19), o contexto consiste no “ambiente em que ocorre a ação registrada no documento”, o que alteraria o foco da análise do documento em si para estrutura que o cerca, conforme enfatiza Rondinelli (2013). Neste sentido, a autora abordou que os contextos se tratariam de uma hierarquia de estruturas, as quais dividem-se em cinco:

> - Contexto jurídico-administrativo: Leis e normas externas à instituição produtora de documentos as quais controlam a condução das atividades dessa mesma instituição;
> - Contexto de proveniência: Organogramas, regimentos e regulamentos internos que identificam a instituição produtora de documentos;
> - Contexto de procedimentos: Normas internas que regulam a criação, tramitação, uso e arquivamento dos documentos da instituição;

> - Contexto documental: Código de classificação, guias, índices e outros instrumentos que situam o documento dentro do conjunto a que pertence, ou seja, ao fundo;
> - Contexto tecnológico: Ambiente tecnológico (hardware, software e padrões) que envolve o documento. (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 20).

Por outro lado, como último item das características do documento arquivístico digital, a "ação se refere ao fato do documento arquivístico participar de uma ação ou simplesmente apoiá-la, significando em uma produção obrigatória ou facultativa". (RONDINELLI, 2013, p. 236)

Além das características apresentadas, Duranti e Thibodeau (2008) apontaram a forma documental como outro elemento a ser observado no documento arquivístico. Para os autores, a forma documental consistiria em "regras de apresentação de acordo com as quais o conteúdo de um documento arquivístico, seu contexto administrativo e documental, e sua autoridade são comunicados" (DURANTI; THIBODEAU, 2008 apud RONDINELLI, 2013, p. 236).

Com base nessas características, Rondinelli (2013) identificou que a forma documental se dividiria em elementos intrínsecos e extrínsecos. Em relação aos elementos intrínsecos do documento, que se referem à composição interna do documento arquivístico, Duranti e Thibodeau (2008) identificaram nove elementos, os quais são apresentados no Quadro 4 abaixo:

Quadro 4 – Elementos intrínsecos da forma documental

(continua)

Elemento	**Definição**
Autor	Pessoa física ou jurídica que tem autoridade e competência para emitir o documento arquivístico ou em cujo nome ou sob cujo comando o documento foi emitido.
Redator	Pessoa que tem autoridade e competência para articular o conteúdo do documento arquivístico.
Destinatário	Pessoa para quem o documento arquivístico é direcionado ou para quem se destina.
Originador	Pessoa designada no endereço eletrônico no qual o documento arquivístico foi gerado.
Produtor	Pessoa a cujo fundo ou arquivo o documento pertence.
Data cronológica	Data e hora de um documento arquivístico, incluída no documento por seu autor, ou pelo sistema eletrônico em nome do autor, no decorrer de sua elaboração.

(conclusão)

Elemento	**Definição**
Data Tópica	Lugar da elaboração de um documento arquivístico, incluído no documento por seu autor.
Indicação e descrição da ação ou assunto	Identificação do assunto e o teor propriamente dito do documento.
Atestação	Validação escrita de um documento arquivístico por parte daqueles que participam da sua emissão (autor, redator, autenticador), bem como por testemunhas da ação ou da assinatura do documento.

Fonte: DURANTI; THIBODEAU, 2008 apud RONDINELLI, 2013, p. 237-238.

Por outro lado, os elementos extrínsecos da forma de um documento, referem-se à "sua aparência externa, que podem ser características de apresentação geral e específica; assinatura eletrônica e sinais especiais como logos e marcas d'agua" (DURANTI; THIBODEAU, 2008; DURANTI, 2005 apud RONDINELLI, 2013, p. 238).

Com relação ao suporte do documento arquivístico digital, o mesmo é definido pela Câmara Técnica de Documentos Eletrônicos como a "base física sobre a qual a informação é registrada" (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 45). Neste contexto do documento arquivístico digital, Rondinelli (2013) afirmou que o suporte deixa de ser um dos elementos extrínsecos do documento arquivístico digital e passa fazer parte do contexto tecnológico (*hardware*).

Além destas características, Rondinelli (2013, p. 241) apresentou o que se chama de componentes digitais, "constituídos por cadeias de bits que se convertem à leitura aos olhos humanos através do uso de *softwares* dada a codificação em dígitos binários por parte do sistema". Esses componentes são divididos em três tipos: a) Dados de forma (aparência do documento); b) Dados de conteúdo (teor do documento); c) Dados de composição (se faz pela forma e conteúdo).

Estes componentes determinariam, então, a aparência e o conteúdo do documento digital, e em alguns casos também a composição do mesmo. Rondinelli (2013) apresentou alguns exemplos de componentes digitais nos documentos arquivísticos, o primeiro seria uma carta em word, onde sua cadeia de bits contém dados de forma e conteúdo que se apresentam na tela do computador, aqui não se

faz necessário os dados de composição visto que o documento manifestado na tela corresponde exatamente à cadeia de bits armazenada na máquina.

Nesta linha, a autora apresentou o segundo exemplo, que se trataria de um banco de dados de pagamento de pessoal, onde seria incluído também os dados de composição para relacionar as diferentes tabelas armazenadas na cadeia de bits que contém nome do servidor, número de matrícula, data, entre outros se tornando um dado fundamental para que o documento manifestado na tela seja correspondente aos dados armazenados.

A partir dos conhecimentos elencados a respeito das características do documento arquivístico digital, faz-se necessário apresentar os conceitos de confiabilidade e autenticidade apontados pela diplomática. Estes dois conceitos estão diretamente ligados à preservação digital, que usa a própria diplomática como base para seus conceitos.

Segundo o CONARQ (2020), para um documento arquivístico ser confiável, ele precisa ter a capacidade de sustentar os fatos que atesta. Sendo assim, a confiabilidade é relacionada ao momento de criação do documento e sua veracidade, podendo então o documento ser mais ou menos confiável. Rondinelli (2013) ainda complementa que a confiabilidade é de total responsabilidade do autor do documento e também do responsável pela gestão do mesmo.

A partir disso, faz-se necessário apresentar alguns conceitos a respeito da autenticidade dos documentos, onde Rondinelli (2005) argumenta que:

> A autenticidade de um documento está diretamente ligada ao modo, à forma e ao status de transmissão desse documento, bem como às condições de sua preservação e custódia. Isso quer dizer que o conceito de autenticidade refere-se à adoção de métodos que garantam que o documento não foi adulterado após a sua criação e que, portanto, continua sendo tão fidedigno quanto era no momento em que foi criado (RONDINELLI, 2005, p. 66).

Complementando o entendimento da autora, tem-se na visão do CONARQ (2012) que a autenticidade ainda envolve três aspectos em relação aos documentos arquivísticos, que são eles: a) Legal; b) Diplomático; c) Histórico. O aspecto legal do documento é “aquele que dá testemunho sobre si em virtude da intervenção durante ou após sua produção, garantindo assim sua genuinidade” (CONARQ, 2012, p. 3).

Por outro lado, o aspecto autêntico diplomático do documento considera que a escrita precisa estar de acordo com a prática do tempo e do lugar indicado no texto, assinado pelas pessoas competentes para sua produção (CONARQ, 2012). Por

último, há ainda os documentos historicamente autênticos, “que servem para atestar eventos ou informações verdadeiras que de fato aconteceram” (CONARQ, 2012, p. 3). Para as autoras Rocha e Rondinelli (2016, p. 68) estes três aspectos são “independentes de tal modo que um documento pode ser considerado autêntico de acordo com um e não autêntico conforme o outro”.

Por fim, para complementar o entendimento sobre autenticidade, destaca-se que esta estaria ameaçada por: a) Vulnerabilidade dos suportes e sistemas que não garantirão se vai haver intervenções autorizadas ou não documentadas; b) Ausência de ações de gestão arquivística de documentos; c) ausência de procedimentos controlados de preservação digital (PROJETO INTERPARES apud BAGGIO, 2011, p. 56).

Ao compreender as características do documento arquivístico digital e os elementos vinculados à autenticidade, na sequência da pesquisa são apresentados os resultados obtidos acerca das iniciativas que apresentam as medidas protetivas que possibilitariam a garantia da autenticidade e da confiabilidade a respeito dos documentos arquivísticos digitais na nuvem, bem como os elementos necessários para garantia destes aspectos.

4.3 INICIATIVAS PARA GARANTIA DA AUTENTICIDADE DE DOCUMENTOS NA NUVEM

A partir das colocações elencadas no subcapítulo anterior a respeito da autenticidade e confiabilidade do documento arquivístico digital, pode-se considerar que essas duas características se mostram cruciais para garantia do valor de prova deste. Rocha e Silva (2007) ainda complementam:

> No entanto, se não houver procedimentos adequados de segurança e de preservação, a confiabilidade, a autenticidade e o acesso desses documentos ficam ameaçados e, portanto, eles não terão mais valor como prova das atividades. O grande desafio apresentado pelos documentos digitais é a garantia da produção de documentos confiáveis e a manutenção de sua autenticidade e acesso de longo prazo.

Com isso, pode-se dizer que para que o documento digital seja considerado também como documento arquivístico, ou seja, como fonte de prova, a autenticidade e a confiabilidade são características essenciais para este fim. A partir dessa colocação, Rogers (2016, tradução nossa) argumenta que para maior garantia de

confiabilidade e autenticidade do documento digital, é necessário que haja procedimentos que sirvam para fortalecer o vínculo arquivístico.

Cabe salientar ainda que o termo vínculo arquivístico utilizado no Brasil, seria uma tradução para o termo *archival bond,* onde Rocha (2011) argumenta que:

> Apesar de não constar dos dicionários de arquivologia brasileiros, alguns arquivistas se referem ao conceito de archival bond como vínculo arquivístico. Entretanto, existe um outro termo utilizado tradicionalmente pelos arquivistas brasileiros, com o mesmo significado de archival bond, que é o de relação orgânica. Este termo utilizado no Brasil é derivado do termo organicidade, ao qual archival bond está relacionado. O conceito de archival bond é compreendido e incorporado na prática arquivística dos países de língua espanhola e portuguesa, mas nem todos têm um termo para este conceito, em outras palavras, nem sempre existe uma palavra especial, com significado específico, utilizada pelos arquivistas para expressar o conceito de archival bond (ROCHA, 2011, p. 85-86).

Praxedes e Rangel (2018) seguem a mesma abordagem em relação ao documento digital, ao destacarem que:

> Identificar a substância e a estrutura do documento digital, ou seja, seu vínculo arquivístico, é premissa básica para presumir sua autenticidade, uma vez que os elementos que se relacionam ao vínculo arquivístico também se relacionam à identidade (PRAXEDES; RANGEL, 2018, p. 64).

A partir desse entendimento, os autores ainda complementam que a autenticidade é uma qualidade presente em alguns elementos desde a sua criação, tornando-se assim necessário, utilizar ferramentas capazes de executar ou pelo menos demonstrar o controle sobre o documento (PRAXEDES; RANGEL, 2018).

Para garantir estas características ao longo do tempo, se faz necessário o uso dos metadados, que se definem por “dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo” (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 36). Resumidamente, os metadados poderiam ser compreendidos como componentes dos documentos arquivísticos digitais que serviriam para descrever suas propriedades.

4.3.1 Metadados

Os metadados, na visão de Praxedes e Rangel (2018, p. 64), são como “um mecanismo capaz de registrar toda e qualquer ação realizada na produção e manutenção do documento arquivístico nato digital”.

Desta forma, é com base nos metadados que seria possível a obtenção dos

dados relacionados à criação e manutenção do documento ao longo do tempo, contribuindo assim para a sua garantia de autenticidade, confiabilidade e acessibilidade. Neste sentido, Praxedes e Rangel (2018, p. 67) salientam a "importância de agregação dos metadados ao considerar a necessidade de captura destes dados que se referem a criação e uso além da forma, conteúdo e estrutura do documento".

Duranti (2002, tradução nossa) ainda salienta que os metadados capturados nem sempre serão ligados ao vínculo arquivístico em sua totalidade, gerando imprecisão sobre os registros a respeito de sua identidade e integridade. Praxedes e Rangel (2018) ainda complementam salientando a importância de serem estabelecidos metadados suficientemente capazes de registrar o vínculo arquivístico no ato de produção e manutenção do documento nato digital, bem como ao longo de sua temporalidade.

Após compreender a relevância dos metadados no contexto da autenticidade dos documentos digitais, é pertinente apresentar a sua classificação. Neste escopo, a publicação do *National Information Standards Organization* (NISO, 2004, p. 6, tradução nossa) identificou os metadados como: a) Metadados Descritivos; b) Metadados Estruturais; c) Metadados Administrativos. A partir deste entendimento, Sayão (2010) também identifica a mesma classificação para os metadados. Com base nestes autores, apresenta-se o Quadro 5 com a identificação dos tipos de metadados.

Quadro 5 – Classificação dos metadados

(continua)

Classificação	**Sayão (2010)**	**NISO (2004)**
Metadados Descritivos	Descrevem um recurso com o propósito de descoberta e identificação; podem incluir elementos tais como título, autor, resumo, palavras-chave e identificador persistente.	Elementos ou propriedades que identificam um documento digital e ajudam a localizá-lo ou interpretá-lo;

(conclusão)

Classificação	Sayão (2010)	NISO (2004)
Metadados Estruturais	Informações que documentam como os recursos complexos, compostos por vários elementos, devem ser recompostos e ordenados. Por exemplo, como as páginas de um livro, digitalizadas separadamente, são vinculadas entre si e ordenadas para formar um capítulo.	Registrar as relações estruturais entre as fontes digitais, por exemplo a estrutura do arquivo na qual a fonte digital está, ou os links entre as páginas em websites;
Metadados Administrativos	Informações que apoiam os processos de gestão do ciclo de vida dos recursos informacionais. Incluem, por exemplo, informações sobre como e quando o recurso foi criado e a razão da sua criação.	Usados para gerenciar o documento. Incluem metadados que oferecem informação sobre o contexto técnico do documento, informações sobre direitos e obrigações embutidas na fonte digital, como copyright, autoria; restrições de uso e de segurança, e metadados de preservação com requisitos para a preservação dos documentos através do tempo e de mudanças tecnológicas.

Fonte: Adaptado de SAYÃO, 2010, p. 5 e NISO, 2004, p. 6.

Depois da classificação dos metadados e de identificar que estes configuram-se como um importante aspecto para a garantia da autenticidade e acessibilidade dos documentos digitais, sejam eles armazenados em nuvem ou em repositórios digitais, apresenta-se a seguir alguns padrões utilizados para este fim (METS, PREMIS, Dublin Core) e também a linguagem de marcação chamada de XML – eXtensible Markup Language.

Começando pela linguagem XML - eXtensible Markup Language, utilizada para a criação de padrões e metadados, que segundo Almeida (2002, p. 5) é conhecida

como uma “linguagem de marcação que se entende por um conjunto de convenções utilizadas para a codificação de textos”. O autor explica que o XML possui uma função relevante na internet, pois permite a troca de dados na internet ao “associar atributos aos elementos como nome e valor, onde nome seria a propriedade do elemento e valor seria a característica propriamente dita” (ALMEIDA, 2002, p. 11-12).

O primeiro padrão a ser analisado, o METS, é definido como “um esquema XML projetado como uma infraestrutura para codificar todos os tipos de metadados associados a um objeto digital” (SAYÃO, 2010, p. 26). Além disso, o autor ainda complementa que “o METS estabelece um padrão útil para a gestão de objetos digitais no âmbito de um repositório e o intercâmbio deles entre repositórios (ou entre repositórios e seus usuários)” (SAYÃO, 2010, p. 26).

Este padrão foi desenvolvido através de uma iniciativa da DLF - Digital Library Federation (Federação de biblioteca digital), que utilizou como base o trabalho do projeto MOA2 que visava apresentar um formato de codificação para os metadados administrativos e estruturais. Diante disso, o grupo do METS, passou a desenvolver um formato XML para codificação dos metadados necessários para gestão de repositórios, possibilitando também a troca dos dados armazenados entre diferentes repositórios. (LIBRARY OF CONGRESS, METS, 2021)

A partir destas definições elencadas, a depender de sua utilização, o METS pode ser utilizado no papel de um Pacote de Submissão de informação (PSI), Pacote de Arquivamento de Informação (PAI) ou um Pacote de Disseminação de Informação (PDI) no contexto do OAIS (FREIRE; BORBINHA, 2016, p. 1).

Considerando o exposto acima, Sayão (2010) complementa que o METS possui cinco seções: a) Grupo de Arquivos; b) Metadados Administrativos; c) Metadados Descritivos; d) Mapa Estrutural; e) Comportamento. Por outro lado, Freire e Borbinha (2016) salientam que ainda há mais 2 seções, que seriam: a) Cabeçalho METS; b) Ligações Estruturais.

Diante do exposto sobre as seções do METS, entende-se como pertinente apresentar no Quadro 6 abaixo as definições elencadas pelos autores.

Quadro 6 – Seções do padrão de metadados METS

Seções do METS	**Definição**
Cabeçalho METS	O cabeçalho METS contém metadados descrevendo o documento METS em si, incluindo informação como o criador, editor, etc... (FREIRE; BORBINHA, 2016, p. 1)
Ligações Estruturais	A secção de Ligações Estruturais do METS permite aos criadores METS registar a existência de hiperligações entre nós na hierarquia esboçada no Mapa Estrutural. Esta secção tem um valor particular na utilização do METS para arquivar sites. (FREIRE; BORBINHA, 2016, p. 1)
Grupo de Arquivos	É um inventário de todos os arquivos associados com o objeto digital e de suas versões eletrônicas. (SAYAO, 2010, p.27)
Metadados Administrativos	Essa seção aninha as informações técnicas sobre: como os arquivos foram criados e armazenados, a gestão de direitos, o objeto original da qual o objeto deriva e a proveniência dos arquivos que compõem o objeto. Pode apontar para metadados externos ao documento METS. (SAYAO, 2010, p.27)
Metadados Descritivos	Essa seção inclui informações sobre o conteúdo intelectual do item –incluindo informações bibliográficas -necessárias para a sua recuperação e avaliação por parte do usuário. (SAYAO, 2010, p.27)
Mapa Estrutural	Indica de forma hierárquica como os vários componentes do item se relacionam mutuamente, permitindo, dessa forma, que seus elementos constituintes possam ser navegados pelos usuários. (SAYAO, 2010, p.27)
Comportamento	Essa seção pode ser usada para associar comportamentos executáveis com o conteúdo no objeto METS. (SAYAO, 2010, p.27)

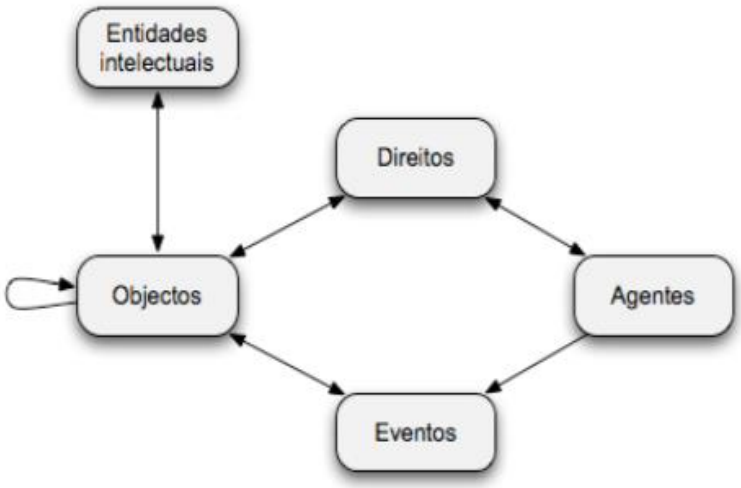
Fonte: FREIRE; BORBINHA, 2016, p. 1; SAYÃO, 2010, p.27.

Além do METS, há também o padrão PREMIS – *Preservation Metadata: Implementation Strategies,* (Metadados de Preservação: Estratégias de implementação) que em tradução para o português é “Metadados de preservação: estratégias de implementação”. Este padrão foi desenvolvido por um grupo de experts patrocinados pelo OCLC - *Non profit Library Organization* (Organização de bibliotecas sem fins lucrativos) e RLG - *Research Library Group* (Grupo de pesquisa bibliotecária)

para ser implementado nos projetos de preservação digital ao redor do mundo. Atualmente se mantém ativo através do PREMIS *Maintenance Activity* que busca centralizar todas as informações oficiais e não oficiais sobre a iniciativa. (LIBRARY OF CONGRESS, PREMIS, 2021).

O resultado de trabalho do grupo, foi o dicionário de dados PREMIS, que identificou ao total cinco principais componentes: a) Entidades intelectuais; b) Agentes; c) Eventos; d) Objetos; e) Direitos. Para melhor representação dos componentes apontados pelo grupo apresenta-se uma figura representativa (Figura 1):

Figura 1 – Componentes do dicionário de dados PREMIS



Fonte: FERREIRA, 2009, p. 41.

O dicionário de dados apresentado pelo grupo, apresenta as descrições detalhadas para cada componente associado. A partir disso, no Quadro 7 são apresentadas as definições dos componentes apresentadas pelo PREMIS:

Quadro 7 – Componentes do PREMIS

Componentes	Definição
Entidade Intelectual	Conjunto coerente de conteúdos que é reconhecido como uma unidade, por exemplo, livros, artigos, bases de dados;
Objeto	Unidade discreta de informação em forma digital, constituindo o que realmente é armazenado e gerenciado pelo repositório, por exemplo, um arquivo PDF.
Evento	Ações que envolvem ou afetam os objetos no repositório, por exemplo, uma ação de migração;
Agente	Pessoa, organização ou programa de computador que desempenha papéis associado com um Evento ou declarações de Direitos;
Direitos	Direitos e permissões vinculadas ao objeto e relevantes para a preservação, por exemplo, permissão para se fazer uma cópia em PDF.

Fonte: SAYÃO, 2010, p. 24-25.

Estes componentes definidos pelos PREMIS apresentam a descrição dos itens necessários para o registro dos metadados. Estes permitem, auxiliar na preservação do documento arquivístico digital dentro dos repositórios digitais complementando, dessa forma, a integridade do documento ao longo do tempo.

Além do PREMIS, há também o padrão Dublin Core que segundo Souza et al. (2000, p.93) se define por ser um “conjunto de elementos de metadados planejado para facilitar a descrição de recursos eletrônicos”. Este padrão de metadados considera o total de dezoito elementos, que passaram por uma adaptação após serem detectadas certas necessidades pelos profissionais envolvidos.

Com isso, apresenta-se a relação dos elementos descritos por Souza et al. (2000, p. 94): “Título; Autor ou Criador; Palavras-chave; Categoria; Descrição; Publicador; Colaborador; Data; Tipo; Formato; Acesso; Identificador de Recurso; Fonte; Idioma; Relação; Cobertura; Direito Autoral; Contato”. Estes são os elementos necessários para o padrão Dublin Core que busca manter certa “simplicidade na descrição de seus recursos” (Souza et al., 2000).

4.3.2 OAIS

Com base nos conhecimentos abordados nas seções 2.4 e 4.1, busca-se apresentar o OAIS enquanto padrão para auxiliar na preservação digital dos documentos à longo prazo. Diante de problemas relacionados à garantia de autenticidade e acessibilidade dos documentos arquivísticos digitais ao longo do tempo, a preservação digital se define por um processo ou conjunto de ações que visam superar os obstáculos tecnológicos que surgem com o passar dos anos. Neste escopo, faz-se necessário apresentar o OAIS.

O modelo de referência OAIS – *Open Archival Information System,* foi aprovado como norma ISO (14721) em 2003 e no Brasil como norma ABNT (15472) em 2007, publicado como SAAI – Sistemas espaciais de dados e informações. A norma é “um esquema conceitual que disciplina e orienta um sistema para a preservação e manutenção do acesso à informação digital por longo prazo” (THOMAZ; SOARES, 2004, p. 8). Os autores ainda complementam explicitando os objetivos do modelo:

> O objetivo do modelo é ampliar a consciência e a compreensão dos conceitos relevantes para a preservação de objetos digitais, especialmente entre instituições não arquivísticas; definir terminologias e conceitos para descrever e comparar modelos de dados e arquiteturas de arquivos; ampliar o consenso sobre os elementos e os processos relacionados à preservação e acesso à informação digital; e criar um esquema para orientar a identificação e o desenvolvimento de padrões (THOMAZ; SOARES, 2004, p. 8).

Complementando o exposto acima, a norma SAAI como modelo de referência aborda:

> Um conjunto completo de funções arquivísticas para a preservação da informação, incluindo sua admissão, arquivamento, gerenciamento de dados, acesso e disseminação. Aborda também a migração da informação digital para novas mídias e formatos e também os modelos de dados usados para representar a informação (NBR 15472 2007, p. 6).

Neste contexto, faz-se necessário entender o ambiente ao qual o arquivo SAAI está inserido, onde contempla quatro entidades participantes: a) Produtores; b) Consumidores; c) Administração; d) Arquivos. A partir disso, os produtores serviriam para fornecer a informação a ser preservada, já os consumidores usufruiriam da informação preservada enquanto a administração seria a entidade responsável pelo estabelecimento das políticas gerais do arquivo. (THOMAZ; SOARES, 2004, p. 8)

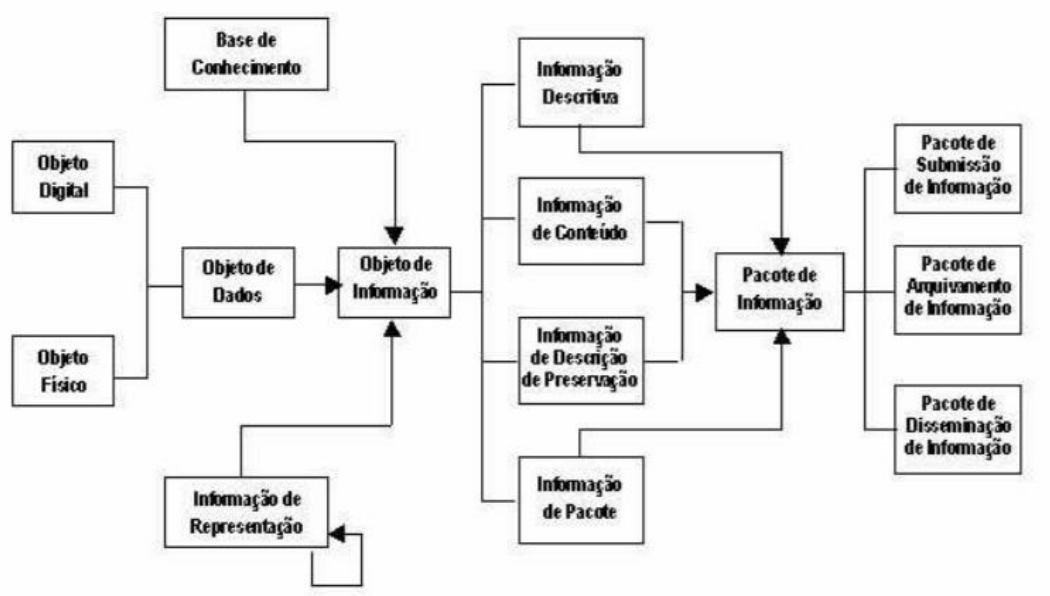
Elucidando o disposto acima, os autores apresentam uma representação gráfica (Figura 2) para melhor exemplificação:

Figura 2 – O ambiente SAAI

Fonte: THOMAZ; SOARES, 2004, p. 10

A partir da compreensão do ambiente SAAI, faz-se necessário apresentar o modelo de informação da norma, que para melhor entendimento apresenta-se na Figura 3, abaixo:

Figura 3 – Modelo de informação OAIS



Fonte: THOMAZ; SOARES, 2004, p. 11

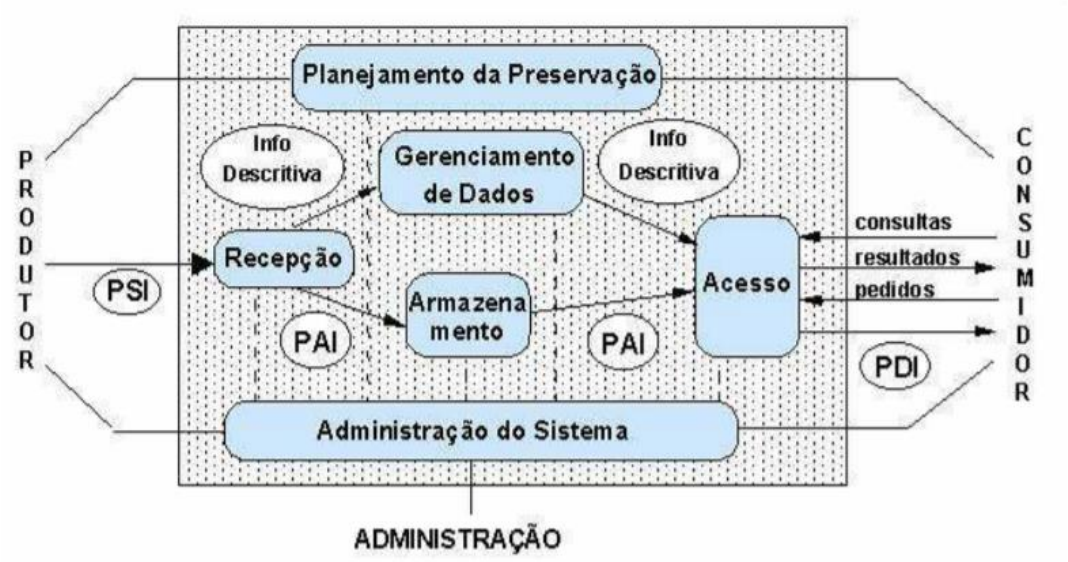
Este modelo de informação ainda descreve os requisitos de metadados para garantia de preservação e acesso ao longo prazo, considerando três pacotes de informação: a) Pacote de informação de Submissão – SIP (Submission Information

Package); b) Pacote de informação de Arquivamento – AIP (Archive Information Package); c) Pacote de informação de Disseminação – DIP (Dissemination Information Package) (THOMAZ e SOARES, 2004).

Conforme os autores, o SIP é o pacote enviado do Produtor para o Arquivo, o AIP é o pacote de informação armazenado dentro do arquivo e o DIP é o pacote transferido do Arquivo para o consumidor em resposta a uma solicitação.

Além do modelo de informação, o OAIS/SAAI é estruturado num esquema funcional, conforme salientam Thomaz e Soares (2004). Os autores identificam seis entidades funcionas: a) Recepção; b) Armazenamento; c) Gerenciamento de Dados; d) Administração do Sistema; e) Planejamento de Preservação; f) Acesso. Para melhor compreensão das entidades, faz-se necessária a apresentação do esquema gráfico na figura 4, abaixo:

Figura 4 – Modelo funcional SAAI



Fonte: THOMAZ; SOARES, 2004, p. 12.

Este modelo define o fluxo da informação partindo do produtor do documento e passando pela administração do sistema, bem como pelo planejamento de preservação. Esse fluxo então chega ao consumidor final através de consultas, resultados ou pedidos. Para uma melhor compreensão da função das entidades do esquema funcional, são apresentadas as respectivas definições no Quadro 8 abaixo:

Quadro 8 – Definição das entidades do Modelo Funcional SAAI

Entidades	**Definição**
Admissão	Serviços e processos necessários para aceitar pacotes de submissão de informação (PSI) dos produtores e preparar os conteúdos para arquivamento e gerenciamento;
Arquivamento	Serviços e processos necessários para arquivar, manter e recuperar os pacotes de arquivamento da informação;
Gerenciamento de Dados	Serviços e processos necessários para incluir, manter e acessar tanto a informação descritiva quanto os dados administrativos;
Administração do Sistema	Serviços e processos necessários para gerenciamento do sistema como um todo;
Planejamento da Preservação	Oferece o necessário para monitorar o ambiente e fornecer as recomendações necessárias para assegurar a acessibilidade da informação à longo prazo mesmo que o ambiente computacional se torne obsoleto;
Acesso	Serviços e processos necessários para apoiar os consumidores na determinação da existência, descrição, localização e liberação da informação armazenada, além de permitir que os consumidores solicitem e recebam produtos de informação.

Fonte: NBR 15472 (2007, p. 20).

A partir das informações dispostas no quadro 8, nota-se uma pequena divergência de nomenclatura em relação às entidades elencadas por Thomaz e Soares e a NBR 15472. Porém cabe salientar que o sentido do modelo é o mesmo e que visa gerenciar o fluxo da informação entre o produtor, a administração e o consumidor final. Thomaz e Soares (2004, p. 13) ainda salientam que as entidades:

> Vistas juntas, identificam os processos chave típicos da maioria dos arquivos dedicados à preservação de informação digital. Um arquivo digital deverá, provavelmente, conter componentes funcionais similares àqueles descritos acima, embora cada implementação específica tenha suas peculiaridades.

A partir da apresentação do modelo OAIS como recurso para auxílio da preservação digital, tem-se um caráter de autenticidade ao ambiente em que o documento se encontra, corroborando para transmissão do mesmo pelos obstáculos impostos pela obsolescência da tecnologia. Dessa forma, dando sequência aos

resultados da pesquisa, faz-se necessário apresentar a partir das iniciativas apontadas ao longo do trabalho, os aspectos necessários para a garantia de autenticidade e acessibilidade dos documentos digitais na nuvem ao longo do tempo.

4.3.3 PaaST

Com o intuito de apresentar o PaaST enquanto iniciativa voltada para contribuir com a autenticidade de documentos na nuvem, antes será destacada uma contextualização do que já foi apresentado até o momento, para então adentrar neste modelo.

Levando-se em conta as definições apontadas nesta pesquisa a respeito da autenticidade, cabe apontar que esta é compreendida como a “adoção de métodos que garantam que o documento não foi adulterado após a sua criação e que, portanto, continua sendo tão fidedigno quanto era no momento em que foi criado” (RONDINELLI, 2005, p. 66).

Além disso, faz-se necessário relembrar a definição de documento digital, que para o glossário da CTDE (CONSELHO NACIONAL DE ARQUIVOS, 2020, p. 25) é a “informação registrada, codificada em dígitos binários, acessível e interpretável por meio de sistema computacional”. A partir desse conceito, relembra-se também os serviços atualmente disponíveis na nuvem elencados neste estudo, que são: SaaS, PaaS, IaaS, DaaS, CaaS, EaaS, DBaaS, FaaS e PaaST.

Contudo, ainda se faz necessário relembrar que os metadados garantem o *archival bond* (vínculo arquivístico[7]) dos documentos digitais e sua autenticidade na computação na nuvem. Com isso, recomenda-se então que para o documento preservar sua autenticidade e acessibilidade na nuvem seja necessário manter os metadados gerados pelos pacotes de informação propostos pelo modelo OAIS. Ainda, recomenda-se que seja também vinculado à um repositório digital, atendendo assim ao que é proposto pelo PaaST, apontado na seção 4.1 da pesquisa como resultado do Projeto InterPARES.

O PaaST, desenvolvido na última fase do Projeto InterPARES, configura-se como um elemento para a garantia de confiança dos documentos digitais na nuvem, complementando assim o modelo OAIS.

Salienta-se que o termo confiança é recente no contexto do documento digital,

[7] Destaca-se que no Brasil o termo equivalente é relação orgânica.

se comparado com outros conceitos, como autenticidade, confiabilidade e acurácia. É mais aplicado, conforme o Projeto InterPARES, à documentação na nuvem. Com isso, faz-se necessária a apresentação do conceito de confiança:

> Crença de uma parte na outra, a partir do alinhamento de valores no que diz respeito a ações específicas ou benefícios, e envolvendo uma relação de vulnerabilidade voluntária, dependência e confiabilidade, com base em avaliação de risco (PROJETO INTERPARES, 2021).

A partir dessa definição, como apresentado anteriormente, o PaaST se diferencia do modelo OAIS por respeitar quais métodos e tecnologias poderão ser usados na implementação do modelo que é desenvolvido para facilitar a elaboração de *softwares* para este fim. Neste aspecto, diferencia-se do modelo OAIS "que é usado como modelo de referência para definir as funções e informações necessárias para a preservação, mas não define como realizar a implementação" (DURANTI et al., 2016, p.13, tradução nossa).

Para uma melhor compreensão das diferenças entre os modelos PaaST e OAIS, faz-se necessária a apresentação de um quadro comparativo entre os dois modelos:

Quadro 9 – Comparativo entre os modelos OAIS e PaaST

	OAIS	**PaaST**
Alcance	Qualquer tipo de objeto de informação;	Somente objetos digitais de informação, com ênfase nos documentos digitais;
Intenção	Modelo de referência;	Guia para facilitar a implementação;
Funcionalidade	Funções abrangentes relacionadas à preservação;	Funções específicas para preservação
Solução abordada	Sistema coerente para a preservação;	Preservação como um conjunto de serviços que podem ser desenvolvidos e implementados de forma independente;
Implementação	Neutra;	Plataforma independente desenvolvida para otimizar a automação.

Fonte: Duranti et al. (2016, p.13, tradução nossa)

A partir dessa abordagem, percebe-se que o modelo proposto pelo projeto InterPARES possui muito mais ênfase na preservação dos documentos digitais, buscando assim facilitar sua implementação. Dessa forma, o modelo PaaST define então cinco principais tópicos para a criação, gerenciamento, acesso ou armazenamento dos documentos digitais na internet. Para melhor compreensão apresenta-se um quadro dos tópicos e suas respectivas definições apontadas por Duranti et al. (2016, tradução nossa):

Quadro 10 – Tópicos abordados pelo PaaST

Tópico	**Definição**
Infraestrutura	Relacionada à arquitetura do sistema que afeta os documentos criados, manejados ou armazenados em ambientes digitais;
Segurança	Proteção dos documentos nos ambientes digitas;
Controle	Manejo dos ambientes em que se encontram os documentos digitais;
Acesso	Acesso aberto ou dados abertos e armazenados na internet;
Legal	Problemas jurídicos que surgem a partir da criação, armazenamento, manejo e uso dos documentos digitais.

Fonte: Duranti et al. (2016, p.7-8, tradução nossa)

Os tópicos apontados por Duranti et al. (2016) mostram as principais seções abordadas pelo modelo visando a preservação dos documentos digitais à longo prazo. Todavia, a autora salienta que “para um documento ser autêntico, ele precisa ser capaz de comunicar a mensagem da qual foi originalmente transmitida” (DURANTI et al., 2016, p. 17, tradução nossa)

Com isso o modelo definido pelo projeto e exposto pela autora Duranti et al. (2016, p. 19-20, tradução nossa) define que há dois tipos de informação sobre os documentos digitais que são necessárias para a preservação: a) Propriedades permanentes do documento; b) Informações contextuais. As propriedades permanentes são aquelas que devem ser preservadas sem alterações pelo tempo em que os documentos forem preservados. Já as informações contextuais são necessárias para saber as relações do documento com o contexto em que o mesmo está inserido, como por exemplo sua proveniência.

A partir disso, a autora define que as diferenças na identificação destes aspectos implicam nas variações de preservação para diferentes tipos de objetos a serem preservados. Duranti et al. (2016) ainda define uma base de conhecimentos necessários para um modelo mais “funcional”. Estes conhecimentos “definem não só a capacidade, mas também os metadados e as informações necessárias para a preservação digital dos documentos e a reprodução de cópias autenticadas do mesmo” (DURANTI et al., 2016, p. 22, tradução nossa).

Dando continuidade à base de conhecimentos mencionada, Duranti et al. (2016) esclarece que:

> O primeiro conhecimento é saber o que será preservado e suas propriedades permanentes. Já o segundo, é conhecer como os objetos da preservação estão codificados em objetos de dados. O terceiro é saber como objetos de dados estão armazenados e o quarto, impõe que para manter a autenticidade é necessário ter a habilidade de aplicar os requerimentos específicos para a preservação digital relacionados às propriedades permanentes do documento, considerando as mudanças nos dados, *hardwares* e *softwares* relacionados (DURANTI et al., 2016, p. 22, tradução nossa).

Há, ainda, mais dois conhecimentos apontados por Duranti et al. (2016, tradução nossa). O quinto conhecimento necessário é saber que as mudanças no armazenamento, codificação ou nas tecnologias não corromperão os objetos da preservação digital. O sexto consiste na manutenção das ligações completas entre os objetos de preservação relacionados, suas informações contextuais e suas representações da informação. Por último, se faz necessário saber como produzir as cópias autênticas dos documentos digitais preservados.

Além da base de conhecimentos, o PaaST (Duranti et al., 2016, tradução nossa) define quatro funções primárias envolvidas na preservação digital. As três primeiras estão relacionadas diretamente com a preservação e a quarta é referente ao do acesso. Para uma melhor definição das funções primárias, apresenta-se o Quadro 11:

Quadro 11 – Funções primárias do PaaST

Função	**Definição**
Initial Holder (Detentor inicial)	No início das atividades relacionadas à preservação, este, detém, possui ou controla os possíveis objetos que serão preservados digitalmente;
Preservation Director (Diretor de preservação)	Responsável pela preservação dos objetos, decidindo quais processos de preservação serão executados;
Preservation Service Provider (Provedor do serviço de preservação)	Provê os recursos e serviços tecnológicos necessários para a preservação digital;
Access Client (Acesso ao cliente)	Parte que deseja obter ou obtém acesso às informações preservadas.

Fonte: Duranti et al. (2016, p. 24, tradução nossa).

Diante dos conhecimentos elencados nesta seção da pesquisa, percebe-se que para a garantia de autenticidade e acessibilidade dos documentos digitais na nuvem, não há somente um item que garantirá estes aspectos, mas sim um conjunto de ações que levarão à longevidade documental.

Essas ações, dependem de vários fatores como especificam os modelos OAIS e PaaST. Além disso, cabe também salientar a importância dos metadados para garantia destes aspectos, pois são considerados “um mecanismo capaz de registrar toda e qualquer ação realizada na produção e manutenção do documento arquivístico nato digital” (PRAXEDES, RANGEL, 2018, p. 64).

Por fim, em conformidade com o que foi apresentado ao longo deste capítulo, pode-se inferir que o conjunto de ações voltados para implementação dos metadados e dos modelos OAIS e PaaST configuram-se como elementos para garantir a autenticidade e a confiabilidade dos documentos arquivísticos digitais na nuvem.

Após apresentação dos resultados da pesquisa, a seguir tem-se o capítulo das conclusões que finaliza o estudo.

5 CONCLUSÕES

A partir do objetivo geral do estudo, que consiste em examinar a garantia da autenticidade dos documentos arquivísticos digitais na nuvem, a partir dos serviços disponibilizados para computação na nuvem e sua respectiva segurança perante os documentos arquivísticos digitais na internet., compreende-se que: com base nos resultados apresentados, esta pesquisa obteve o atingimento dos objetivos do estudo, assim como respondeu a problemática da pesquisa. Este entendimento está baseado na percepção que o estudo pôde identificar ações voltadas, a partir dos serviços na nuvem, que corroboram para a garantia da autenticidade e a confiabilidade dos documentos arquivísticos digitais na nuvem.

Em relação aos diferentes tipos de serviços na nuvem, foram identificados ao total quatro modelos de nuvens: Pública; Privada; Híbrida e Comunitária. Além disso, foi identificado também a totalidade de nove serviços disponíveis na nuvem: SaaS, PaaS, IaaS, DaaS, CaaS, EaaS, DBaaS, FaaS e PaaST.

Além disso, como objetivo específico deste trabalho, foi necessário analisar o documento arquivístico digital, visando identificar suas características, as quais são: forma fixa; conteúdo estável; relação orgânica; contexto identificável; apoiar ou participar de uma ação e o envolvimento de até 5 pessoas.

Além das características do documento arquivístico digital, foram compreendidos aspectos de autenticidade vinculados ao mesmo. Deste modo, com base em pesquisa bibliográfica, pôde-se entender que a autenticidade do documento está diretamente ligada ao modo, forma e status da transmissão do documento, assim como suas condições de preservação e custódia. Ainda se compreendeu que a autenticidade do documento envolve três principais aspectos: Legal, Diplomático e Histórico.

A partir deste entendimento, identificou-se que o documento digital para ser também considerado documento arquivístico necessita de procedimentos que sirvam para fortalecer a sua relação orgânica, visando a manutenção da autenticidade e a confiabilidade enquanto características essenciais do documento arquivístico. A partir disso, os metadados caracterizam-se como uma característica fundamental para garantia destes aspectos ao longo do tempo, pois apresentam dados estruturados que descrevem e permitem encontrar, gerenciar e/ou preservar documentos arquivísticos ao longo do tempo (CONSELHO NACIONAL DE ARQUIVOS, 2020).

Em relação aos metadados, foi identificado, neste estudo a classificação dos metadados, que se dividem em Descritivos, Estruturais e Administrativos. A partir disso, foram apresentados quatro principais padrões de metadados: METS, PREMIS, Dublin Core e XML. Esses padrões possuem características próprias, podendo adequar-se a diferentes aplicações.

No que diz respeito a identificação de iniciativas para garantir a autenticidade e a confiabilidade dos documentos arquivísticos digitais na nuvem, foi possível identificar o modelo OAIS. Este, consiste num modelo voltado para preservação digital dos documentos organizados em um modelo funcional para a preservação da informação, contemplado diferentes entidades (produtores, consumidores, administração e arquivos. O modelo ainda descreve os requisitos de metadados para a garantia de preservação e acesso ao longo prazo, a partir de pacotes de informação (SIP, AIP e DIP).

Outra iniciativa, além dos metadados e do OAIS, que pode auxiliar na garantia de autenticidade e confiabilidade dos documentos arquivísticos digitais na nuvem é o modelo PaaST. Este foi desenvolvido pelo Projeto InterPARES, sendo um elemento para garantia de confiança dos documentos digitais na nuvem complementando o modelo OAIS.

Esse modelo, denominado *Preservation as a service for Trust* define uma base de conhecimentos necessária para a preservador, que vai desde saber o que será preservado e suas propriedades permanentes, até saber que as mudanças no armazenamento, codificação ou nas tecnologias não irão corromper os objetos da preservação digital. Além disso, ainda é necessário a realização da manutenção das ligações completas entre os objetos da preservação relacionados, suas informações contextuais e suas representações da informação.

A partir destes conhecimentos elencados, salienta-se que não há somente um aspecto ou ação que garantirá a autenticidade e acessibilidade dos documentos digitais ao longo do tempo, mas sim um conjunto de ações que levarão à longevidade documental conforme especificam os modelos OAIS e PaaST.

Todavia, é relevante salientar que houve dificuldades encontradas para obtenção de materiais em português sobre o tema, visto que os materiais disponíveis no Brasil ainda estão em fase embrionária, necessitando ser mais explorado pelas áreas relacionadas, como a Arquivologia, que no Brasil ainda não desenvolveu muitos conteúdos acerca do tema.

Salienta-se também a dificuldade da escrita sobre alguns temas abordados neste estudo, visto que só haviam trabalhos em inglês disponíveis, onde coube ao autor desta pesquisa à realização da tradução de alguns textos para melhor compreensão sobre os temas deste trabalho. Dessa maneira, encerra-se aqui a pesquisa com a ênfase em enaltecer este assunto para a geração de mais conteúdos sobre o tema no Brasil.

REFERÊNCIAS

ARQUIVO NACIONAL**. Dicionário Brasileiro de Terminologia Arquivística.** Rio de Janeiro, 2005. (Publicações Técnicas, 51). Disponível em: http://www.arquivonacional.gov.br/images/pdf/Dicion_Term_Arquiv.pdf> Acesso em: 07 out. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma Brasileira 15472**, 2007. Disponível em: https://pt.scribd.com/document/104091335/ABNT-NBR-15472. Acesso em: 03 jan. 2022.

Alecrim, E. **O que é Cloud Computing** (Computação nas Nuvens), 2008. Infowester. Disponível em: https://www.infowester.com/cloudcomputing.php#:~:text=A%20cloud%20computing%20%E2%80%94%20ou%20computa%C3%A7%C3%A3o,tipos%20a%20partir%20da%20internet.&text=A%20evolu%C3%A7%C3%A3o%20constante%20da%20computa%C3%A7%C3%A3o,vez%20mais%20r%C3%A1pido%20e%20disseminado. Acesso em: 07 out. 2021.

ALMEIDA, M. B. Uma introdução ao XML, sua utilização na Internet e alguns conceitos complementares. **Ciência da Informação**, Brasília, v. 31, n. 2, p. 5-13, maio/ago. 2002. Disponível em: <https://mba.eci.ufmg.br/downloads/12903.pdf> Acesso em: 28 dez. 2021.

BAGGIO, C. C. **Preservação de documentos digitais em arquivos: desafios do sec. XXI.** Universidade Federal de Santa Maria, 2011. Disponível em: https://repositorio.ufsm.br/handle/1/13728. Acesso em: 22 dez. 2021.

BORGES, H. P.; SOUZA, J. N.; SCHULZE, Bruno; MURY, Antonio Roberto. **Computação em nuvem**, 2011. Livro Aberto. Disponível em: https://livroaberto.ibict.br/handle/1/861. Acesso em: 07 out. 2021.

CONSELHO NACIONAL DE ARQUIVOS. **Glossário**. Câmara Técnica de Documentos Eletrônicos. Arquivo Nacional: Rio de Janeiro, 2020. Disponível em: <https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf>. Acesso em: 29 nov. 2021.

CONSELHO NACIONAL DE ARQUIVOS. **e-ARQ Brasil**. Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Arquivo Nacional: Rio de Janeiro, 2020. Disponível em: <https://www.gov.br/conarq/pt-br/assuntos/noticias/conarq-abre-consulta-publica-visando-a-atualizacao-do-e-arq-brasil/EARQ_v2_2020_final.pdf>. Acesso em: 06 jan. 2022.

DAWOUD, W.; TAKOUNA, I.; MEINEL, C. Infrastructure as a servisse security: Challenges and solutions, 2010. **IEEE Xplore.** Disponível em: <https://ieeexplore.ieee.org/abstract/document/5461732/>. Acesso em: 07 out. 2021.

DURANTI, L. Records and Archives in the Commercial Cloud. In: **Regulating the Cloud: Policy for Computing Infrastructure (Information Policy).** Cambridge,

2015. p.197-214. Disponível em: <https://www.researchgate.net/publication/301491304_Digital_Records_and_Archives_in_the_Commercial_Cloud> Acesso em: 17 out. 2021.

DURANTI, L. et al.. Preservation as a Service for Trust (PaaST). **CRC Press**, London, UK. 2016. Disponível em: <https://www.researchgate.net/publication/301490739_Preservation_as_a_Service_for_Trust_PaaST>. Acesso em: 15 dez. 2021. ?????

DURANTI, L; EASTWOOD, T; MACNEIL, H. **Preservation of the Integrity of Electronic Records.** Estados Unidos: Vancouver. [E-book]. Disponível em: <https://link.springer.com/book/10.1007/978-94-015-9892-7#toc> Acesso em: 11 dez. 2021.

DURANTI, L. ROGERS, C. Trust in records and data online. In: **Integrity in Government through Records Management**. Routledge, 2014. p. 227-238. Disponível em: <https://www.researchgate.net/publication/290042093_Trust_in_Online_Records_and_Data> Acesso em: 17 out. 2021.

FERREIRA, M. Introdução à preservação digital: conceitos, estratégias e actuais consensos. **Revista Brasileira de Biblioteconomia e Documentação**, v. 12, n. 1, p. 117-119, 2016. Disponível em: <http://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>. Acesso em: 13 dez. 2021.

FREIRE, N. **METS**: An Overview & Tutorial. Biblioteca Nacional de Portugal [s.l.]. 2003. Disponível em: <https://www.loc.gov/standards/mets/METSOverview.v2_port.html>. Acesso em: 10 jan. 2022.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4 ed. São Paulo: Atlas, 2002. Cap. 4 p. 41-55.

INDOLFO, A. C.; LOPES, V. H. Entrevista com Luciana Duranti. **Acervo**, v. 28, n. 2, p. 11-18, 27 nov. 2015. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/636>. Acesso em: 07 out. 2021.

METS. Metadata Encoding and Transmission Standard. **Home**. 2021. Disponível em: <https://www.loc.gov/standards/mets/> Acesso em: 28 dez. 2021.

PEDROSA, P; NOGUEIRA, T. **Computação em Nuvem.** UNICAMP, São Paulo, 2011. Disponível em: <https://pt.scribd.com/document/111484678/ARTIGO-Computacao-em-Nuvem-Pedrosa-Paulo-H-C>. Acesso em: 30 dez. 2021.

PONTES, G. **Arquivando nas Nuvens:** Um recurso estratégico para preservação de documentos arquivísticos digitais, 2014. Biblioteca Digital UEPB. Disponível em: <http://dspace.bc.uepb.edu.br/jspui/handle/123456789/3661>. Acesso em: 07 out. 2021.

PRAXEDES, K; RANGEL, K. Relações entre o vínculo arquivístico e a autenticidade de documentos nato digitais: alguns apontamentos a respeito dos metadados. **Revista do Arquivo:** Revista do Arquivo Público do Estado de São Paulo, São Paulo. n. 6, p. 63-76, abril, 2018. Disponível em: <http://www.arquivoestado.sp.gov.br/revista_do_arquivo/06/pdf/PRAXEDES_K_V__et_al_-_Relacoes_entre_o_vinculo_arquivistico_e_a_autenticidade_de_documentos_nato_digitais.pdf>. Acesso em: 26 dez. 2021.

PREMIS. Preservation Metadata: Implementation Strategies. **Home**. 2021. Disponível em: <https://www.loc.gov/standards/premis/>. Acesso em: 28 dez. 2021.

PROJETO INTERPARES 3. **Dicionário de Terminologia**. Disponível em: <http://www.interpares.org/ip3/ip3_terminology_db.cfm?letter=az>. Acesso em: 19 dez. 2021.

PROJETO INTERPARES iTrust(AI). **Terminology Database**. 2018. Disponível em: https://interparestrustai.org/terminology>. Acesso em: 19 dez. 2021.

RILEY, J. **Understanding Metadata, What is metadata and what is it for?.** 2004. NISO. Disponível em: <https://groups.niso.org/apps/group_public/download.php/17446/Understanding%20Metadata.pdf> Acesso em: 07 out. 2021.

ROCHA, C. PROJETO InterPARES: Entrevista com Luciana Duranti. **PontodeAcesso**, [S. l.], v. 3, n. 1, p. 82–92, 2009. Disponível em: <https://periodicos.ufba.br/index.php/revistaici/article/view/3316>. Acesso em: 07 out. 2021.

ROCHA, C. L. Glossário multilíngue do projeto interpares 3. **Encontros Bibli:** Revista Eletrônica de Biblioteconomia e Ciência da Informação. n. esp. 1. sem., p. 76-90, 2011. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2011v16nesp1p76/18064>. Acesso em: 19 dez. 2021.

ROCHA, C. L.; RONDINELLI, R. C. Gestão e preservação de documentos arquivísticos digitais revisitando alguns dos conceitos que as precedem. **Acervo,** Rio de Janeiro, v. 29, n. 2, p. 61-73, jul/dez., 2016. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/709/744>. Acesso em: 02 jan. 2022.

ROCHA, C. L.; SILVA, M. Padrões para garantir a preservação e o acesso aos documentos digitais. **Acervo**, v. 20, n. 1/2, p. 113-124, 2007. Disponível em: <https://revista.an.gov.br//index.php/revistaacervo/article/view/76/76>. Acesso em: 28 dez. 2021.

ROGERS, C. A Literature Review of Authenticity of Records in Digital Systems: From 'Machine-Readable' to Records in the Cloud. **Acervo**, v. 29, n. 2, p. 16-44, 17 nov. 2016. Disponível em:

<http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/715>. Acesso em: 15 dez. 2021.

RONDINELLI, R. C. **Gerenciamento Arquivístico de Documentos Eletrônicos**. Fundação Getúlio Vargas: Rio de Janeiro, 2005.

RONDINELLI, R. C. **O documento arquivístico ante a realidade digital**. 3 ed. Fundação Getúlio Vargas**:** Rio de Janeiro, 2020. Cap. 4, p. 231-259.

SAYÃO, L. F. Uma outra face dos metadados: informações para a gestão da preservação digital. **Encontros Bibli:** revista eletrônica de biblioteconomia e ciência da informação, Florianópolis, v.15, n. 30, p. 1-31, ago., 2010. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2010v15n30p1>. Acesso em: 14 dez. 2021.

SANTOS, F. U. O que é Computação em Nuvem e quais os principais tipos? In: **ProfissionaisTI**, 2020. Disponível em: <https://www.profissionaisti.com.br/o-que-e-computacao-em-nuvem-e-quais-os-principais-tipos/>. Acesso em: 20 dez. 2021.

SILVA, E. L; MENEZES, E. M. **Metodologia da Pesquisa e Elaboração de Dissertação**. Laboratório de Ensino a Distância da UFSC, Florianópolis, ed. 3, 2001. Disponível em: <https://cursos.unipampa.edu.br/cursos/ppgcb/files/2011/03/Metodologia-da-Pesquisa-3a-edicao.pdf>. Acesso em: 29 dez. 2021.

SOUZA, M. I. F.; VENDRUSCULO, L. G.; MELO, G. C. Metadados para a descrição de recursos de informação eletrônica: utilização do padrão Dublin Core. **Ciência da Informação**, Brasília, v. 29, n. 1, 2000. Disponível em: <https://www.scielo.br/j/ci/a/tcW3q4WvNBQNTqTyLK8qfFF/?format=pdf&lang=pt>. Acesso em: 28 dez. 2021.

TAURION, C. **Cloud Computing. Computação em Nuvem**. Rio de Janeiro: Ed. 1, 2009, 228 p.

THOMAZ, K. P; SOARES, A. J. A preservação digital e o modelo de referência Open Archival Information System (OAIS). **DataGramaZero**, v. 5, n. 1, 2004. Disponível em: <https://pt.scribd.com/document/96453309/A-preservacao-digital-e-o-modelo-de-referencia-Open-Archival-Information-System>. Acesso em: 29 nov. 2021.

VAQUERO, L. RODERO-MERINO, L. CACERES, J. LINDNER, M. **A break in the clouds: towards a cloud definition**, 2008. ACM Digital Library Disponível em < https://dl.acm.org/doi/abs/10.1145/1496091.1496100>. Acesso em: 07 out. 2021.

VERAS, M. **Cloud Computing:**. Nova Arquitetura da TI. Rio de Janeiro: Ed. 1, 2012, 240 p.