Artigos

Custódia de documentos arquivísticos digitais: o dilema entre repositórios e nuvens.[1]

Custody of digital archival documents: the dilemma between repositories and clouds.

Claudio Paulino de Oliveira| mestre em Gestão de Documentos e Arquivos pela UNIRIO; técnico da Diretoria de Gestão de Documentos e Arquivos do Arquivo Nacional; Rio de Janeiro, RJ, Brasil; ORCID 0009-0005-9091-2680 E-mail: claudio.oliveira@an.gov.br

Mariana Lousada Pinha | doutora em Ciência da Informação pela UNESP; professora do programa de Pós-Graduação em Gestão de Documentos e Arquivos da UNIRIO; Rio de Janeiro, RJ, Brasil; ORCID 0000-0001-5395-683X; E-mail: mariana.lousada@unirio.br

Brenda Couto Brito Rocco | doutora em Ciência da Informação pelo IBICT/UFRJ; professora do Programa de Pós-Graduação em Gestão de Documentos e Arquivos da UNIRIO; Rio de Janeiro, RJ, Brasil; ORCID 0000-0002-4447-7906; E-mail: brenda.rocco@unirio.br

Resumo:

O presente artigo versa sobre o estudo realizado no tocante à custódia dos documentos arquivísticos produzidos em meio digital, especificamente no Estado do Rio de Janeiro. Tem por objetivo discutir o conceito de custódia na Arquivologia e a sua importância para a preservação e acesso dos documentos arquivísticos digitais, temas bastante debatidos no Arquivo Público do Estado do Rio de Janeiro, a partir de 2020. Por meio de levantamento bibliográfico e documental, foi trazida a conceituação de custódia, além das concepções de repositório arquivístico digital confiável e da computação na nuvem, dois modelos que estão nas discussões no Governo do Estado do Rio de Janeiro. Compreendeu-se o entendimento do funcionamento dessas estruturas, as diferenças e semelhanças de atuação de cada modelo, identificando qual realizará a preservação de documentos arquivísticos digitais, e se poderão atuar em conjunto na custódia dos arquivos.

Palavra(s)-chave: custódia de documentos arquivísticos digitais, repositório arquivístico digital confiável, computação na nuvem.

Abstract:

This article discusses a study about the custody of archival documents produced in digital media, specifically in the State of Rio de Janeiro. It aims to broach the concept of custody in Archivology and its importance for the preservation and access of digital archival documents, subjects that have been widely debated in the Public Archive of the State of Rio de Janeiro since 2020. Through bibliographic and documentary research, the concept of custody is introduced, in addition to the concepts of reliable digital archival repository and cloud computing, two models that are being analyzed by the Government

[1] Artigo apresenta parte dos resultados da pesquisa realizada no âmbito do Programa de Pós-Graduação em Gestão de Documentos e Arquivos, Universidade Federal do Estado do Rio de Janeiro, 2023. Oliveira, Claudio Paulino de. Recomendações para a preservação de documentos arquivísticos digitais produzidos pelo Estado do Rio de Janeiro / Claudio Paulino de Oliveira. – 2023. 219 f. Orientadora: Mariana Lousada Pinha. Coorientadora: Brenda Couto Brito Rocco. Produto técnico-científico (Mestrado).

of the State of Rio de Janeiro. The functioning of these models, with their differences and similarities in performance was summarized, identifying which of them are better suited to carry out the preservation of digital archival documents and whether they can act together in the custody of those files.

Keyword(s): *custody of digital archival documents, digital archival repository, cloud computing.*

Introdução

As funções arquivísticas atuam como uma grande engrenagem, destarte elas dependem umas das outras para que os documentos possam produzir os seus efeitos com plenitude. Os atos de produzir, classificar, avaliar, adquirir, conservar, descrever e difundir estão interligados e, mesmo com características bem definidas, precisam caminhar em conjunto para que os documentos e fundos arquivísticos consigam desempenhar os seus propósitos: legal, histórico, social e democrático. Para isso, as organizações deverão realizar com responsabilidade o arquivamento dessas informações.

Desde 2020, o conceito de custódia de documentos arquivísticos ganhou destacada atenção, principalmente em meio digital, nas discussões entre o Arquivo Público do Estado do Rio de Janeiro (APERJ) e o Governo deste Estado. Apresentou-se urgentemente, embora nunca tivesse deixado de ser visível, a necessidade de se encontrarem meios de preservar e armazenar os documentos arquivísticos digitais.

Assim, foram identificadas como possibilidades de armazenamento o Repositório Arquivístico Digital Confiável (RDC-Arq), defendido pelo APERJ, e a Computação na Nuvem[2], eleita dos governantes do Estado do Rio de Janeiro, mesmo sem consulta ao Arquivo ou realização de algum estudo apurado sobre o tema, como local de arquivamento único e oficial de toda a estrutura do Poder Executivo.

Dito isso, o presente artigo procurou compreender o conceito de custódia de documentos arquivísticos e analisará a estrutura do RDC-Arq e da Computação na Nuvem (CN), utilizando como procedimentos metodológicos a pesquisa bibliográfica e a pesquisa documental, realizados em publicações e estudos que tratassem a respeito desses temas, para a confecção de uma análise qualitativa. Possui caráter exploratório, abordando temas pouco debatidos na Arquivologia, como a custódia de documentos e computação na nuvem; e tem caráter descritivo, por avaliar e contemplar a oportunidade de diálogo com a análise exploratória, oferecendo subsídios para novas percepções arquivísticas.

Como resultados, ratificou-se a importância da custódia e as suas nuances no processo decisório em atividades arquivísticas, bem como a identificação das características do RDC-Arq e da CN, a probabilidade de arquivamento único na nuvem, e a possibilidade desses dois modelos de arquivamento trabalharem na custódia dos documentos arquivísticos digitais.

O conceito de custódia de documentos arquivísticos

Os arquivos têm intrinsecamente uma afinidade muito estreita com o termo custódia, que por sua vez também é associada à preservação. Segundo o Dicionário Brasileiro de Terminologia Arquivística (DIBRATE), custódia é a "responsabilidade jurídica de guarda e proteção de arquivos, independentemente de vínculo de propriedade" (Arquivo Nacional, 2005, p.62). Em sua tese de doutorado, Silva (2015, p. 31) traz à tona um debate sobre as relações que envolvem o arquivo e o seu lugar de custódia, sinalizando a sua inerente polarização na Arquivologia.

[2] Múltiplas infraestruturas e serviços distribuídos em rede (tipicamente através da *internet*) que são escaláveis sob demanda e que são criados para apoiar a gestão de grandes volumes de materiais digitais (IBICT, 2022).

> Na década de 1990, a custódia polarizou a comunidade arquivística. Esse tema foi identificado como central para discutir a fundamentação teórica da Arquivologia, especialmente os conceitos de arquivo e documento arquivístico e, também se, no novo cenário da revolução tecnológica, a abordagem custodial, ainda seria válida para enfrentar os desafios da preservação digital.

A autora destaca que havia uma discussão em que a custódia enfatizaria a preservação voltada para a guarda física, cabendo aos documentos digitais uma abordagem diferente. No entanto, é manifesto que a preservação incide sobre qualquer documento, independentemente de qualquer suporte, tendo a custódia como aliada para proporcionar a sua segurança.

O termo custódia é utilizado em várias línguas, com seus respectivos significados, em léxicos ou dicionários e glossários, porém analisaremos a terminologia arquivística. Mesmo em vocabulários arquivísticos, a definição de custódia possui distintas interpretações. No entanto, em todas elas existem três elementos essenciais: a guarda, a proteção e o aspecto relacional entre o material custodiado e o custodiante. Silva (2015, p.46) corrobora esses entendimentos e ressalta também as finalidades de preservação e integridade que a custódia carrega consigo.

> Desta forma, em todas as definições encontradas nos dicionários e glossários arquivísticos sobre custódia, fica implícito que os documentos precisam de proteção porque são frágeis tanto do ponto de vista físico como intelectual, sujeitos a vários tipos de perigos à sua durabilidade e manutenção enquanto documentos arquivísticos, e que sua perda, adulteração, falsificação ou mesmo desorganização pode impossibilitar a sua utilização como testemunhos das ações. Além disso, essa proteção tem por finalidade manter preservado e íntegro o material custodiado.

A pessoa ou instituição que tiver a custódia de documentos arquivísticos terá a responsabilidade de protegê-los, organizá-los e deixá-los acessíveis para que possam cumprir as suas funcionalidades em determinado contexto, tanto no meio analógico, quanto no digital. Ou seja, a guarda dos documentos arquivísticos está associada à sua preservação, requisito necessário para que se cumpra o inter-relacionamento entre eles e a possibilidade de tomadas de decisão, pesquisas, comprovação de direitos, dentre outras finalidades.

Esse encargo pode ser desempenhado pelo próprio produtor, ou por terceiro que tenha autorização para isso e cumpra todas as condições necessárias. No meio digital, premissas como normatização, ambiente de custódia adequado, manutenção da cadeia de preservação[3] digital contínua, e equipe técnica capacitada para agir em caso de sinistro são determinantes para a preservação e acessibilidade dos documentos arquivísticos.

Importante destacar que no serviço público a custódia não pode ser realizada por empresas privadas. De acordo com o que é estabelecido no art. 1° da Lei Federal n° 8.159/1991, “é dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos”. Outro dispositivo que endossa essa determinação legal é o art. 2º da Resolução nº 6, de 15 de maio de 1997, do Conselho Nacional de Arquivos (CONARQ), onde se preconiza que “a guarda dos documentos públicos é exclusiva dos órgãos e entidades do Poder Público, visando garantir o acesso e a democratização da informação, sem ônus, para a administração e para o cidadão”.

[3] Sistema de controles que se estende por todo o ciclo de vida dos documentos, a fim de assegurar sua autenticidade ao longo do tempo (CONARQ, 2020, p.14).

A possibilidade de delegar massas documentais acumuladas para corporações privadas de armazenamento, com serviços para documentos convencionais e digitais, destacando-se nas soluções informatizadas as ofertas de repositórios e serviços na nuvem, é muito atraente para resoluções instantâneas em arquivos desorganizados. No entanto, os dispositivos legais clarificam que é vedada a terceirização da guarda dos documentos arquivísticos públicos.

Percebemos, então, que a custódia não é o mero ato de depositar os documentos arquivísticos em locais sem planejamento e critérios, com o intuito de deixar para depois a organização de acervos. O fato de adiar ações que proporcionem a proteção desses documentos, prejudicando a recuperação e acessibilidade de informações, demonstra o descaso com os objetivos da instituição que os produziu e, concomitantemente, os anseios de pesquisas oriundas da sociedade.

Silva (2015, p. 222) colabora afirmando a importância da custódia, mas descartando que ela só tenha sentido de aplicabilidade quando os documentos estejam prestes a serem acessados pelos usuários.

> O lugar não é um depósito qualquer, onde os documentos são meramente armazenados, mas significa a condição de poder manter a sua preservação e o seu acesso. A definição da autoridade e da responsabilidade é requisito para a preservação, mas esta não se reduz apenas à custódia. A preservação de acervos convencionais e digitais envolve também as responsabilidades compartilhadas entre produtores e o preservador, bem como a definição das diferentes ações que precisam ser desempenhadas desde o início do ciclo de vida dos documentos até a sua disponibilidade para os usuários finais.

As responsabilidades legais precisam ser definidas, bem como as atuações conjuntas dos que produzem e preservam os documentos, percorrendo todo o seu ciclo vital. A custódia por si só não é a garantia de proteção aos arquivos. Medidas como a confecção de políticas de gestão de documentos e de preservação, aliadas ao investimento acentuado no ambiente e nos materiais para a guarda, são estratégias que indicam a tenacidade na execução de boas práticas arquivísticas.

Assim, o custodiador, sendo produtor ou não, além da responsabilidade jurídica pelo documento arquivístico, deverá sustentar o seu percurso pelas idades documentais, cumprindo prazos e a sua destinação, eliminação ou guarda permanente, com as ações necessárias de preservação e garantindo as relações entre os demais documentos e, simultaneamente, com aquele que os detém.

Dessa forma, ao definirmos custódia e suas características de atuação nos documentos, apresentamos a sua ligação íntima com a preservação e o acesso. Veremos a seguir as características de dois meios de apoio que atualmente são mencionados nas tratativas no Poder Executivo do Estado do Rio de Janeiro, para que se consiga realizar a guarda documental com eficácia e segurança.

A complexidade estrutural do Repositório Arquivístico Digital Confiável (RDC-Arq).

Em meio às mudanças de produção e representação dos documentos arquivísticos, a concepção de um arquivo nunca foi esquecida. Direcionam-se agora as atenções para outras perspectivas de armazenamento das informações. Não se quer dizer esquecer o passado por meio do documento convencional, e sim desenvolver uma parceria sólida entre a produção do documento não digital e do digital, relacionando as suas variações na formação do acervo de qualquer organização. Nesse prisma, surge o repositório digital que

> (...)é um ambiente de armazenamento e gerenciamento de materiais digitais. Esse ambiente constitui-se de uma solução informatizada em que os materiais são capturados, armazenados, preservados e acessados. Um repositório digital é, então, um complexo que apoia o gerenciamento dos materiais digitais, pelo tempo que for necessário, e é formado por elementos de hardware, *software* e metadados, bem como por uma infraestrutura organizacional e procedimentos normativos e técnicos (cONARQ, 2015, p. 9).

Santos e Flores (2015b, p. 206) complementam a definição de repositório digital, emanada pelo CONARQ, salientando a sua importância quanto à preservação digital, pois

> Com o auxílio de repositórios digitais é possível manter os formatos de arquivos sempre atualizados, desta forma, as estratégias de migração serão mais eficazes. Além disso, os repositórios facilitam a inserção de metadados, definida no próprio repositório, assim estes metadados serão preservados ao longo do tempo juntamente com os documentos digitais.

Masson também dialoga com o tema expondo que o repositório digital, de acordo com a instituição que o construir, poderá oferecer outras possibilidades de uso, saindo da visão meramente técnica para se tornar um aliado na produção e gestão de conhecimento.

> Repositórios digitais são frequentemente conceituados em relação às suas funções de reunir, preservar, dar acesso e disseminar o conhecimento de uma instituição científica, ou de uma área do conhecimento, aumentando sua visibilidade e se constituindo numa ferramenta de gestão do conhecimento científico (Masson, 2008, p. 112).

Para dar continuidade ao assunto, precisaremos alinhar algumas considerações. Os repositórios digitais foram definidos como aqueles que absorverão os materiais produzidos em meios tecnológicos. Sua estruturação deve seguir preceitos bem definidos e com estratégias pertinentes no gerenciamento do seu conteúdo. O CONARQ (2015, p. 9-10) ajudará novamente na conceituação do tema, defendendo que “Um repositório arquivístico digital é um repositório digital que armazena e gerencia esses documentos (documentos arquivísticos), seja nas fases corrente e intermediária, seja na fase permanente”; ... “um repositório digital confiável é um repositório digital que é capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário”; ... e “um repositório arquivístico digital confiável deve ser capaz de atender aos procedimentos arquivísticos em suas diferentes fases e aos requisitos de um repositório digital confiável”.

Os repositórios digitais passaram a ser requeridos e se tornaram indispensáveis para os procedimentos de custódia e preservação dos documentos arquivísticos digitais. Outro atributo que integrará o rol das especificidades desse ambiente tecnológico é a confiabilidade. Para atingir essa qualidade, os envolvidos no processo precisarão cumprir funções predeterminadas, sendo elas envolvidas com a satisfação ou aplicação dos serviços.

Thomaz (2007, p. 81) indica que neste sentido a confiança se desenvolve em diversos níveis para repositórios digitais, que são no mínimo três: produtores, consumidores e fornecedores. Para isso é fundamental verificar se os produtores estão enviando as informações corretas, se os consumidores estão recebendo essas informações, e se os fornecedores estão prestando os serviços adequados. O autor conclui referenciando o termo confiança ao elucidar que

> Um repositório digital confiável é mais do que uma organização encarregada de armazenar e administrar objetos digitais. Um repositório digital confiável é "aquele cuja missão é fornecer acesso confiável, por longo prazo, a recursos digitais administrados à sua comunidade-alvo, agora e no futuro" (Thomaz, 2007, p.88).

Dentro dessa perspectiva e posicionando os arquivos, Lampert e Flores (2013, p. 9) pressupõem uma especificidade determinante e bem delineada para a captura e armazenamento dos materiais digitais, quando indicam que

> [...] o termo repositório digital incorporou outras funcionalidades, sendo identificado como Repositório Arquivístico Digital. Este, por sua vez, é um repositório digital que armazena documentos arquivísticos, nas fases corrente e intermediária (associado com um SIGAD) ou permanente, de acordo com normas arquivísticas para gestão documental.

Rocha (2015, p. 188-189) afirma que além de acompanhar as normas arquivísticas, o RDC-Arq deve proporcionar navegação multinível, implementação de metadados, autenticidade e relação orgânica entre os documentos.

> A relação orgânica e a identidade caracterizam o documento arquivístico como tal, e o distingue de outros tipos de informação. Assim, além de dar garantias da autenticidade do documento, considerando sua identidade e integridade, um repositório digital para documentos arquivísticos deve ser capaz de organizar e recuperar os documentos de modo a manter a relação orgânica entre eles. As funções de arranjo e descrição reforçam a relação orgânica, pois são uma maneira de perpetuar e autenticar essa rede de relações dos documentos arquivísticos. Dessa maneira, o repositório deve apoiar a organização hierárquica dos documentos digitais a partir de (1) um plano de classificação de documentos (nas fases corrente e intermediária) ou (2) da estrutura de arranjo dos fundos (na fase permanente). Do mesmo modo, a gestão documental e a implementação de metadados no repositório devem estar em conformidade com as práticas e as normas de arquivo, particularmente de gestão documental e de descrição multinível de documentos – *General International Standard ArchivalDescription* – ISAD(G) e Norma brasileira de descrição arquivística (Nobrade).

A doutrina em Arquivologia orienta que todo documento arquivístico produzido numa instituição precisa ser subsidiado por uma política de gestão de documentos. No meio digital, essas atividades deverão ser gerenciadas por um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), com o intuito de administrar as informações desde a produção até a sua destinação final. Isso fortalecerá a qualidade arquivística, especificará o tempo de arquivamento necessário e quais os documentos constituirão o patrimônio documental da organização produtora.

Santos (2022, p. 8) substancia esse entendimento dialogando que a inserção de uma política de preservação digital de documentos arquivísticos deve ser interpretada como uma parceria, abrangendo diversas ações e instrumentos:

- 1) Política arquivística formalizada, com conformidade legal e técnica, contemplando:
  - » - Plano de classificação e tabela de temporalidade;
  - » - Regras de acesso e de tratamento de documentos sigilosos;

- » - Normas e procedimentos de transferência, recolhimento e descarte.
- » - Política de preservação digital de documentos arquivísticos.

- 2) Política arquivística implementada por meio de:
  - » - Ações de sensibilização, capacitação, treinamento e atualização;
  - » - Monitoramento da aplicação e atualização da política, instrumentos e práticas;
  - » - Comissão de avaliação e de acesso de documentos;
  - » - Sigad;
  - » - RDC-Arq;
  - » - Sistema de difusão.

- 3) Política de segurança da informação, sistematizada em planos de ação.

Observamos o quão é complexa a missão de garantir a um fundo arquivístico a integralidade e o desenvolvimento de todas as etapas de gestão e manutenção de documentos arquivísticos. Em um cenário perfeito, as instituições deverão aliar a política arquivística com a de preservação. No âmbito digital, deve-se atentar para a produção de novos documentos, mas também é necessário se envolver com os que já foram produzidos, em sua grande maioria, sem os requisitos arquivísticos necessários.

Uma possibilidade de resolução do problema anterior é a captura desses documentos sem requisitos arquivísticos em um SIGAD, cientificando-se a data de produção, para fins de gestão de documentos, e a data de registro no sistema, com o intuito de informar os responsáveis pelo processo e os motivos que levaram à inserção. Essa viabilidade de alcance e atuação na documentação confeccionada pelas instituições proporcionou, concomitantemente, a ampliação da propriedade receptiva de um RDC-Arq.

Inicialmente, o RDC-Arq foi planejado para sustentar as propriedades dos documentos permanentes. No entanto, com o passar dos anos, viu-se a necessidade de o repositório compreender os documentos pertencentes às fases corrente e intermediária dos arquivos. Sendo assim, mesmo com a imprescindibilidade de um SIGAD e de dar suporte as três fases arquivísticas, os repositórios podem tratar documentos nato-digitais (oriundos de um SIGAD ou sistemas específicos com o mínimo de requisitos de presunção de autenticidade) ou representantes digitais (documentos produzidos em meio não digital e convertidos por processo de captura eletrônica).

Santos (2022, p. 8-9) fortalece a ideia de atuação do RDC-Arq em todas as fases do ciclo vital dos documentos ao citar a Orientação Técnica nº 3/2015, do CONARQ, que especifica três possíveis cenários:

> **a.** uso do RDC-Arq no ciclo vital completo: aqui há a expectativa que os sistemas de negócio gerem documentos arquivísticos que são capturados pelo Sigad, para gerenciamento, e depositados em um RDC-Arq nas fases correntes e intermediária e, quando destinados à preservação permanente, depositados em outro RDC-Arq, o histórico.
>
> **b.** uso do RDC-Arq nas fases corrente e intermediária, permite três cenários:
>
> **b1.** Neste cenário, também é possível utilizar um storage institucional em conjunto com o RDC-Arq, mantendo no primeiro, por exemplo, documentos de curto prazo de guarda;
>
> **b2.** integração de um sistema de negócio com o Sigad e deste com o RDC-Arq e/ou sistema de storage;
>
> **b3.** sistema de negócio incorpora funções de um Sigad e interopera diretamente com um RDC-Arq e/ou sistema storage.

> **c.** uso do RDC-Arq na fase permanente: de adoção obrigatória, quer os documentos sejam provenientes de sistema de negócio ou de Sigad, devem ser depositados e geridos quanto a sua autenticidade e relações orgânicas no RDC-Arq.

Cabe salientar que a realidade dos arquivos brasileiros está bem aquém da estrutura referencial de plenitude de um fundo arquivístico. Ou seja, até que se consiga a implementação de um RDC-Arq, as mentalidades e ações das instituições precisam ser revistas e inclusivas ao potencial arquivístico dos acervos.

Em um contexto ideal, a idealização de um RDC-Arq possui uma série de regras e normas para que se alcance a preservação dos materiais digitais. É quase consenso, por todos aqueles que trabalham com a atividade de preservação digital, que se aplique o modelo de referência internacional *"Open Archival Information System (OAIS)"*. Santos e Flores (2015b, p. 207) asseguram que:

> O modelo OAIS é um modelo de referência conceitual que especifica os requisitos para um arquivo de materiais digitais o qual tem a responsabilidade de preservar informações e disponibilizá-las para uma comunidade específica. [...] A documentação é armazenada no OAIS porque sua necessidade de preservação é considerada de longo prazo, mesmo se o próprio modelo não for permanente. Pode-se definir longo prazo como o tempo suficiente para se preocupar com os impactos da evolução das tecnologias.

Rocha (2015, p. 184) corrobora que o modelo OAIS deve ser o primeiro elemento de uma estratégia organizacional de preservação digital e conta alguns detalhes dessa norma.

> Convém evidenciar que o primeiro atributo apontado é o cumprimento com o modelo Oais, uma das normas mais importantes no que diz respeito à preservação digital e a repositórios digitais. O modelo Oais foi desenvolvido sob a coordenação do Comitê Consultivo para Sistemas de Dados Espaciais (CCSDS) da Nasa, que contou com a colaboração da comunidade científica internacional. Sua elaboração levou dez anos. Uma primeira versão foi publicada em 1999, outra em 2002, e em 2003 transformou-se na norma ISO 14721:2003.

No Brasil, o CONARQ sugere esse modelo como a norma mais importante para a aplicação de procedimentos para construção de repositórios arquivísticos digitais confiáveis. Por outro lado, Santos e Flores (2015b, p. 208), apesar de concordarem com a importância e confiança do modelo OAIS nesse processo, alertam para os cuidados na adoção das ferramentas que executarão as atividades do ambiente, quando defendem que

> A conformidade dos repositórios digitais com o modelo OAIS adiciona confiança nas ações de preservação visto que este modelo é fortemente conceituado na comunidade de preservação digital. Além disso, o modelo OAIS apresenta-se como um modelo conceitual, ou seja, a sua implementação poderá ser orientada a um repositório genérico. Com o modelo OAIS é possível escolher um padrão entre diversos padrões de metadados, assim como os *software*s responsáveis pelas estratégias de preservação. Desta forma, a garantia de acesso em longo prazo dependerá da eficácia das ferramentas que executam as estratégias, por isto é de extrema importância que exista uma avaliação criteriosa e uma verificação constante destas ferramentas.

O planejamento correto e as escolhas bem definidas auxiliarão na formação de um RDC-Arq, atendendo os requisitos necessários e alcançando os anseios de um público-alvo. Braga et al (2022, p. 10) substanciam essa linha de pensamento dispondo que "apenas por meio de estratégias sólidas de preservação, associadas a ferramentas apropriadas, é que a sociedade atual estabelecerá os mecanismos que proporcionarão o acesso futuro de forma irrestrita aos conhecimentos existentes atualmente".

Existem parâmetros convencionados e obrigatórios para a preservação dos documentos arquivísticos digitais, e caberá a cada instituição aumentar o nível de segurança, de acordo com as suas condições técnicas e orçamentárias. No entanto, para a criação de um RDC-Arq, é imprescindível a confecção de uma política de preservação digital[4], definindo todas as estratégias e atributos relacionados ao ambiente digital da instituição, com alto grau de precisão e atualização às novidades tecnológicas, em caso de necessidade.

Ao complementar uma política de preservação digital, o RDC-Arq coloca em prática os critérios deliberados para erguer bases resistentes e pertinentes para o armazenamento dos documentos arquivísticos digitais. Sempre salientando que um RDC-Arq não é apenas uma simples solução informatizada de arquivamento; trata-se de um complexo mecanismo formado por hardwares, *software*s, metadados, infraestrutura organizacional, e procedimentos normativos e técnicos.

Referente aos órgãos públicos, Rocha (2015, p. 189) identifica também que, além de uma sedimentação basilar que direcione e apoie a estrutura tecnológica de uma organização, os repositórios digitais são imprescindíveis para a gestão dos documentos públicos:

> Nesse cenário, destaca-se a necessidade da criação de repositórios digitais confiáveis projetados especificamente com o propósito de gerenciar os documentos arquivísticos produzidos pelo governo. Somente desta maneira será possível dar acesso a documentos digitais autênticos, precisos e confiáveis, assim como aos dados e informações derivados destes. No entanto, a criação de repositórios digitais confiáveis inclui muitas variáveis, compromissos a longo prazo e a necessidade de investimentos altos em infraestrutura tecnológica, pesquisa e recursos humanos. Assim, é preciso uma política nacional que viabilize e apoie esse caminho.

Diante dessas afirmativas, Santos e Flores (2015b, p. 209) apontam alguns itens que legitimam e evidenciam a instauração de um RDC-Arq: a adoção de padrões de metadados; o alinhamento com o modelo de referência OAIS; a análise e certificação da eficácia dos instrumentos utilizados no processo; a confecção de políticas institucionais; a custódia confiável ininterrupta dos documentos durante todo o ciclo de vida; a escolha das estratégias de preservação digital; a interação entre os procedimentos de gestão, preservação e acesso; a manutenção da cadeia de preservação digital; profissionais capacitados e tecnologias apropriadas para a preservação; recursos financeiros em longo prazo; simultaneidade com as normas e práticas recomendadas pela comunidade de preservação digital; e transparência à comunidade das medidas utilizadas no armazenamento e na preservação dos materiais digitais, proporcionando confiança e referência.

A auditoria dos métodos e a realização de testes para desenvolver um ambiente tecnológico confiável não podem ser desconsideradas. Manuais de utilização e boas práticas, somando-se aos relatórios das atividades realizadas, também aparecem como elementos-chaves para um RDC-Arq ainda mais consolidado.

[4] É um documento que define as diretrizes e objetivos de uma instituição para a implantação de um programa de preservação digital. Deve abranger todos os elementos relacionados à Preservação Digital e estar alinhada com os objetivos da instituição e com as outras políticas, tais como digitalização, acesso, TI, investimentos, etc (IBICT, 2022).

Retrataremos a seguir os requisitos conceituais que devem ser cumpridos na estruturação de um repositório digital, conforme disposto na publicação "Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis" (CONARQ, 2014):

- **a) <u>Infraestrutura organizacional</u>:** é o ambiente em que o repositório digital vai se estabelecer (CONARQ, 2014, p. 12-13), sendo dividido em:
  - » **Governança e viabilidade organizacional:** trata-se da definição dos preceitos e representantes que viabilizarão o compromisso de um RDC-Arq (preservação, gerenciamento e acesso dos documentos arquivísticos digitais).
  - » **Estrutura organizacional e de pessoal:** definição da equipe gabaritada, em número que atenda às necessidades e com qualificação para tal, que garantirá que o RDC-Arq funcione de maneira plena, incluindo-se um plano de capacitação permanente.
  - » **Transparência de procedimentos e arcabouço político:** demonstrar claramente requisitos, decisões, desenvolvimento e ações visando à preservação de longo prazo e o acesso ao conteúdo do RDC-Arq.
  - » **Sustentabilidade financeira:** o RDC-Arq deve atender aos preceitos basilares de preservação digital, reconhecidos pela comunidade internacional, em contrapartida, precisa-se conseguir mantê-lo dentro das limitações orçamentárias e técnicas da organização.
  - » **Contratos, licenças e passivos:** é a fase de registro e disponibilização aos interessados quanto aos papéis, às responsabilidades, aos prazos e às condições, firmados entre o repositório e os produtores dos documentos digitais e/ou fornecedores dos serviços. Precisam estar claros todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial no que diz respeito à propriedade intelectual e a restrições de uso.

- **b) <u>Gerenciamento do documento digital</u>:** é o conjunto de ações que devem estar de acordo com o modelo de referência OAIS, estabelecendo três pacotes de informação**: SIP - submissão** (admissão dos documentos digitais e seus metadados associados), **AIP - arquivamento** (acondicionamento e armazenamento dos documentos digitais e seus metadados associados) e **DIP - disseminação** (acesso aos documentos digitais e seus metadados associados).

O gerenciamento do documento no RDC-Arq é categorizado em seis grupos funcionais (CONARQ, 2014, p. 13-17):

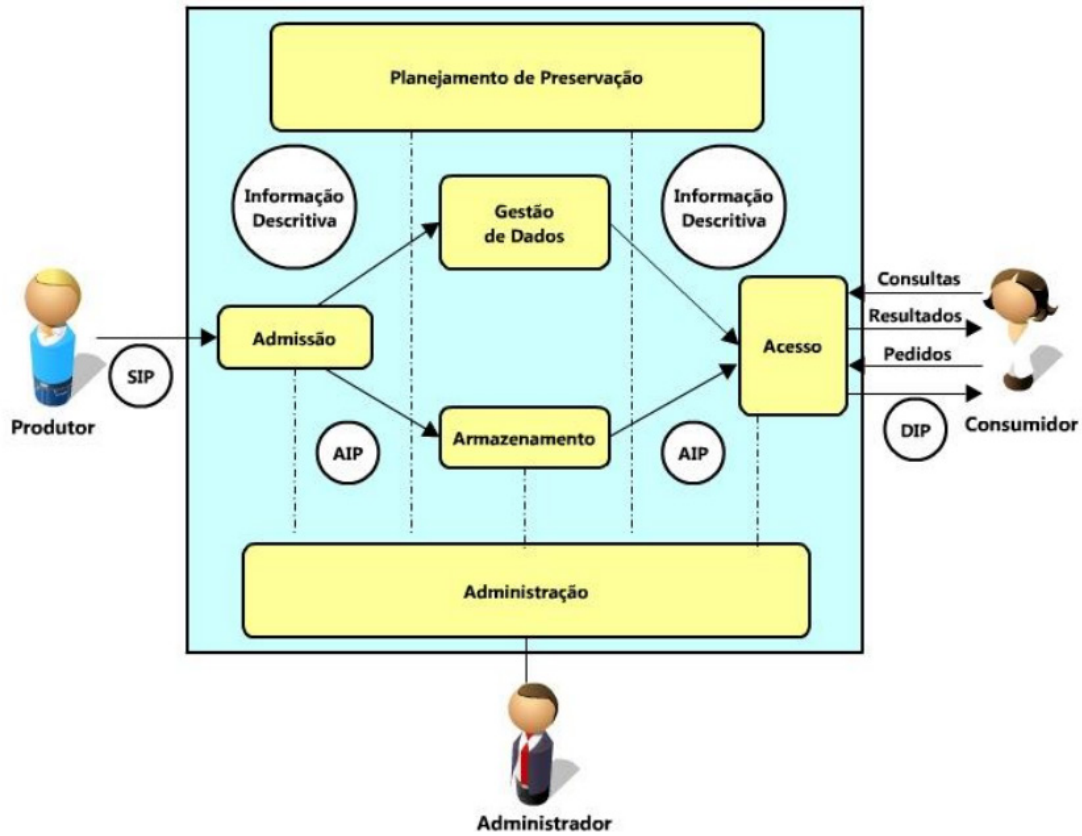
- » **Admissão: captura de documentos digitais** – entrada dos documentos arquivísticos digitais no repositório (pacote SIP). Essa etapa varia de acordo com as regras de negócio e a especificação dos metadados de entradas, seguindo o preconizado pelo E-arq Brasil, nas fases corrente e intermediária, e pela Norma Brasileira de Descrição Arquivística (NOBRADE), na fase permanente.
- » **Admissão: criação do pacote de arquivamento** – padronização em que todo o documento capturado junto ao RDC-Arq precisa ganhar o formato de arquivamento e preservação de longo prazo (pacote AIP).
- » **Planejamento da preservação** – é realizado a partir de uma política de preservação digital e visa enfrentar os problemas de obsolescência tecnológica e fragilidades dos suportes.
- » **Armazenamento e preservação / manutenção do AIP** – o RDC-Arq deve atender um conjunto de condições para garantir um bom desempenho da preservação de longo prazo do pacote AIP.
- » **Gerenciamento de informação** – trata-se da gestão das informações descritivas (metadados) dos documentos admitidos no repositório, apoiando o acesso e a recuperação dos documentos com qualidade.
- » **Gerenciamento de acesso** – é o controle do acesso das informações produzidas pelo pacote DIP. Nessa etapa são relatadas as falhas do processo; a aceitação ou rejeição da consulta do usuário; o atendimento da requisição do usuário, de acordo com a sua solicitação; dentre outras condições.

- **c) <u>Tecnologia, infraestrutura técnica e segurança</u>:** Este requisito tem como objetivo descrever as melhores práticas das áreas de gestão de dados e segurança, que devem ser atendidas por um repositório digital confiável. São divididas em (CONARQ, 2014, p. 17-18):
  - » **Infraestrutura de sistemas** – o RDC-Arq tem que possuir uma infraestrutura tecnológica robusta, de maneira a apoiar a confiabilidade dos AIPs nele mantidos.
  - » **Tecnologias apropriadas** – adoção de tecnologia de hardware e *software* apropriada para os serviços que presta, com possibilidade de mudanças na tecnologia utilizada ao longo do tempo.
  - » **Segurança** – etapa em que não se abrangem apenas as tecnologias do repositório, mas também a estrutura física do local e as ações das pessoas.

Alicerçando os requisitos conceituais, a construção de repositórios digitais confiáveis tem como referência os seguintes padrões e normas (CONARQ, 2014, p. 19-25):

- **Modelo de referência OAIS (2003) -** modelo conceitual que define um repositório digital, identificando o ambiente, os componentes funcionais, suas interfaces internas e externas, os objetos de dados e informações. (Figura 1).

Figura 1 - Modelo conceitual OAIS



Fonte: CONARQ (2015, p.20).

- **Relatório da** Research Library Group (RLG) e da Online Computer Library Center **(OCLC) - Repositórios digitais confiáveis: atributos e responsabilidades (2002**)- o relatório estabeleceu as características essenciais e as responsabilidades para a criação e manutenção de repositórios digitais confiáveis que atendessem aos acervos de instituições culturais e científicas, garantindo seu acesso a longo prazo, sua integridade e confiabilidade.

- **Certificação e auditoria de repositórios confiáveis: critérios e** check list **– TRAC (2007) -** o documento apresenta um conjunto de critérios e um checklist que são tomados como referência para a certificação e auditoria de repositórios digitais.
- **Requisitos técnicos para entidades de auditoria e certificação de organizações candidatas a serem repositórios digitais confiáveis – CCSDS (2011).**
- **Metadados de preservação – PREMIS (2012) -** norma internacional que apresenta um conjunto básico (core) de elementos de metadados de preservação para apoiar sistemas que gerenciam objetos digitais.
- **Norma Geral Internacional de Descrição Arquivística – ISAD(G) (2000)**- norma internacional que estabelece diretrizes gerais para a preparação de descrições arquivísticas.
- **Norma Brasileira de Descrição Arquivística – NOBRADE (2006)** - norma adaptada e em conformidade com a ISAD(G) e a "Norma Internacional de Registro de Autoridade Arquivística para Entidades Coletivas, Pessoas e Famílias – ISAAR(CPF)".
- **E-ARQ Brasil (2022) -** modelo de requisitos para sistemas informatizados de gestão arquivística de documentos, elaborado pela Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (CTDE/CONARQ) e adotado pelo Sistema Nacional de Arquivos.
- **Protocolo para coleta de metadados – OAI-PMH (2002)**- protocolo que permite a interoperabilidade entre repositórios.
- **Padrão de codificação e transmissão de metadados – METS -** esquema XML que permite a codificação e o intercâmbio dos metadados descritivos, administrativos e estruturais relativos a objetos digitais.
- **Descrição arquivística codificada – EAD (2002) -** codificação desenvolvida e utilizada para a descrição de metadados arquivísticos baseados na linguagem de marcação XML, que permite a descrição, estruturação e interoperabilidade dos metadados arquivísticos referenciais, possibilitando a decodificação e a apresentação das informações referenciais de forma estruturada aos usuários.

Dessa forma, identificamos os conceitos e requisitos de um RDC-Arq. O repositório necessita de pessoas responsáveis que estruturem sua formalística, em especial arquivistas e profissionais de tecnologia da informação. São indispensáveis o tratamento arquivístico e a preservação digital.

O RDC-Arq deve ter independência e possibilitar acesso direto aos documentos que estão sob sua custódia. Aliado a isso, a interoperabilidade é fundamental no contexto, pois é necessária a conexão com outros sistemas informatizados e repositórios, permitindo-se a absorção confiável dos documentos arquivísticos.

Entende-se que o projeto de um RDC-Arq requer planejamento, leva tempo e possui um custo elevado. Por outro lado, os benefícios que serão alcançados são imensuráveis e compensarão os recursos investidos, proporcionando a preservação de informações, a formação da memória, e construção do patrimônio arquivístico de uma sociedade.

No Brasil, ainda não possuímos repositórios arquivísticos considerados confiáveis, pois não existe órgão que certifique os procedimentos arquivísticos e de segurança que os qualifiquem. No entanto, isso não deve ser impeditivo para que as instituições continuem desenvolvendo e aprimorando suas estruturas tecnológicas e seus dispositivos normativos, com vistas à obtenção de um RDC-Arq.

Cloud computing – Computação na Nuvem: o funcionamento e os modelos de utilização.

Um arquivo precisa ser capaz de oferecer condições para proporcionar longevidade aos documentos arquivísticos. Aos que foram produzidos em meio digital, como visto nas características de um RDC-Arq, é necessário estabelecer critérios condizentes com as especificidades dos registros custodiados; reunir equipe técnica qualificada para realizar as operações necessárias de apoio ao acervo; aplicar investimento contínuo para a atualização e manutenção de sistemas e equipamentos que concentrem fundo(s) de arquivo; e escolher linhas de ação que favoreçam o desenvolvimento do arquivo, potencializando seus atributos informacionais.

Abordaremos agora a *Cloud computing* (Computação em Nuvem), uma solução tecnológica com grande anuência em nossos tempos. A intenção aqui não é fazer uma exaustiva apuração sobre este modelo de armazenamento, mas observar se a Computação em Nuvem (CN) possui características que possam preservar os documentos arquivísticos digitais em seu ambiente.

Borges *et al* (2011, p. 39) mencionam as vantagens e a aceitação da CN em nossa sociedade, quando afirmam que:

> A computação em nuvem, nos diversos aspectos que lhe dizem respeito, tais como infraestrutura, plataforma e *software* como serviço tem apresentado uma grande aceitação tanto no meio empresarial quanto no científico devido às diversas vantagens que apresenta em relação ao modelo tradicional.

O modelo tradicional apresentado pelos autores diz respeito às instituições possuírem ambientes tecnológicos dentro de suas estruturas. O foco atual é possuir serviços fora das dependências dos produtores de documentos arquivísticos digitais, que armazenem e garantam a acessibilidade a essa documentação.

Do ponto de vista técnico o *National Institute of Standards and Technology* (NIST) define a CN como um modelo acessível em qualquer lugar, desde que contenha os requisitos para tal.

> A computação em nuvem é um modelo para permitir o acesso onipresente, conveniente e sob demanda a uma rede compartilhada de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser provisionados e liberados rapidamente com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços (NIST, 2011, p. 2, tradução nossa).

Essa definição indica que o acesso aos registros na nuvem quase não possui fronteiras. Velte *et al*. (2012, p. 32) relata que a "computação em nuvem é uma ideia que permite utilizar as mais variadas aplicações via *internet*, em qualquer lugar e independentemente da plataforma, com a mesma facilidade de tê-las instaladas no computador". Os autores compreendem a CN como uma solução que se compara à própria *internet*, onde, num sentido topológico, agrega clientes, *data centers* e servidores interligados.

Contribuindo para elucidar as diferenças entre o modelo tradicional e a utilização da CN, Hedler et al (2016, p. 190-191) apresentam um comparativo sobre esses dois modelos (Tabela 1).

Tabela 1 - Diferenças entre o modelo tradicional e a computação em nuvem

Trabalho sem computação em nuvem	Trabalho com computação em nuvem
Utiliza-se o computador no local de trabalho para acessar o servidor da organização.	Utilizam-se quaisquer tipos de dispositivos digitais conectados à *Internet* para acessar a nuvem de informações da organização em qualquer momento e em qualquer lugar.
Todos os *softwares* e serviços da organização estão instalados no dispositivo do trabalhador.	O trabalhador não precisa ter os *softwares* instalados. Realiza o acesso a partir de um navegador de *Internet*.
Recorre ao suporte interno de TI sempre que há um problema.	A própria nuvem resolve o problema por meio da colaboração e da larga extensão do uso das ferramentas, que acaba por minimizar incidências de erros e problemas.
Tem limite de armazenamento e processamento.	Entra num processo de escalonamento de demanda quanto ao armazenamento e processamento.

Fonte: o próprio autor.

Analisando na perspectiva de negócios, Marston et al (2011, apud Hedler et al, 2016, p. 194) definem a CN como um serviço que é disponibilizado e pago conforme a demanda do usuário.

> [...] um modelo de serviço de tecnologia da informação onde os serviços de computação (*hardware* e *software*) são entregues sob demanda para os clientes em uma rede na forma de autoatendimento, independente do dispositivo e localização. Os recursos necessários para fornecer o requisito Níveis de Qualidade de Serviço são compartilhados, dinamicamente escaláveis e rapidamente provisionados, virtualizados e liberados com interação mínima com o provedor de serviço. Os usuários pagam pelo serviço como despesa operacional, sem incorrer em despesas de capital inicial significativo, com os serviços de nuvem empregando um sistema de medição que divide o recurso de computação em blocos apropriados.

Com um olhar mais estrutural, Veras (2012, p. 31) introduz que a "computação em nuvens significa mudar fundamentalmente a forma de operar a TI, saindo de um modelo baseado em aquisição de equipamentos para um modelo baseado em aquisição de serviços". O entendimento aqui é reduzir custos operacionais, permitindo que os setores de tecnologia da informação se concentrem em projetos mais estratégicos, em vez de cuidarem de *data centers*, *storages* e outros equipamentos.

Percebe-se como interesse inicial para a adoção da CN, além da redução de custos operacionais, o arquivamento dos documentos arquivísticos em espaços virtuais, com a facilidade de acesso desses documentos

em qualquer lugar, propiciando aos produtores utilizarem seus próprios recursos tecnológicos para outras finalidades. Cândido e Araújo Júnior (2022, p. 67-68) acreditam que a CN tem um caráter complementar e possui outra funcionalidade principal.

> A *cloud computing* por ser um recurso complementar às novas tecnologias de visualização de dados, recuperação da informação e até mesmo para a Inteligência Artificial, aponta para a sua principal funcionalidade que é a melhoria contínua do desempenho no gerenciamento e integração dos dados, fator decisivo para a agilidade nas decisões empresariais.

A CN pode ser entendida como uma solução que auxiliará as instituições que se utilizam desse serviço, no acesso de forma rápida aos documentos arquivísticos que ali estejam custodiados. Ressalta-se que a gestão e a preservação digital desses documentos deverão ser definidas em políticas internas das instituições produtoras, não cabendo à prestadora do serviço o compromisso de elaborá-las, mas sim executar o que for acordado.

Outro ponto a se destacar no modelo de CN é definir a participação dos agentes no processo. Pedrosa e Nogueira (2011, p. 1) destacam três grupos.

> Estes podem ser divididos em três grandes grupos: Provedor de serviço, Desenvolvedor e Usuário. O provedor é responsável pela tarefa de disponibilizar, gerenciar e monitorar toda a infraestrutura da nuvem, garantindo o nível do serviço e a segurança adequada de dados e aplicações. Já o desenvolvedor deve ser capaz de prover serviços para o usuário final, a partir da infraestrutura disponibilizada pelo provedor de serviço. Enquanto o usuário final é o consumidor que irá utilizar os recursos oferecidos pela nuvem computacional.

Com a disposição bem delimitada dos participantes desse novo modelo de armazenamento, as instituições não poderão se esquecer de que a primazia desse processo continuará sendo o atendimento ao seu usuário final.

No entanto, apesar das vantagens apresentadas, vem à tona a apreensão quanto à preservação digital dos documentos arquivísticos no âmbito da nuvem. Cândido e Araújo Júnior (2022, p. 68) inferem os prós desse modelo, mas sinalizam para as barreiras que a CN encontra, principalmente, em questão à segurança.

> Dentre as vantagens deste modelo computacional destaca-se o potencial de redução de custos, uso sob demanda e flexibilidade no atendimento das demandas informacionais dos usuários, aspecto essencial na gestão da informação e do conhecimento organizacional. Entre os desafios da adoção de *cloud*, a questão da segurança foi e ainda tem sido uma argumentação forte em termos de barreiras à sua adoção.

Podemos elencar, além da segurança e a privacidade dos documentos armazenados em um ambiente compartilhado, fora do controle da instituição, outros pontos de preocupação que podem afetar a preservação dos documentos arquivísticos digitais na CN, tais como dúvidas de propriedade e controle dos dados ou mesmo da infraestrutura, os obstáculos do processo de migração, o desempenho e a garantia de acessibilidade ao acervo na nuvem a qualquer hora, a proteção das informações e a observância de normas, padrões e requisitos para o arquivamento de documentos arquivísticos digitais.

A estrutura da CN precisa seguir alguns parâmetros para entregar o que vende aos seus clientes, que é o armazenamento seguro e o acesso condizente para o modelo que se contrata. Mas será isso suficiente para conseguir proporcionar preservação digital aos documentos arquivísticos?

De acordo com o NIST, as características essenciais da CN são:

a. **Autoatendimento sob demanda:** os usuários podem fornecer recursos de computação, como por exemplo, tempo do servidor e rede, armazenamento, conforme necessário, sem assistência do provedor de serviços (NIST, 2011, p. 2). Segundo Pedrosa e Nogueira (2011, p. 2), "para suportar este tipo de expectativa, as nuvens devem permitir o acesso em autoatendimento (self-service) para que os usuários possam solicitar, personalizar, pagar e usar os serviços desejados sem intervenção humana".

b. **Amplo acesso à rede:** "disponibilidade na rede com acesso por meio de dispositivos padrão acessíveis à *Internet*, como por exemplo, telefones celulares, laptops, etc." (NIST, 2011, p. 2). Borges et al (2011, p. 5) entendem essa característica como virtualização de recursos, em que se possibilita "uma separação dos serviços de infraestrutura dos recursos físicos como hardware ou redes".

c. ***Pool* de recursos:** "um modelo multilocatário que agrupa recursos entre usuários" (NIST, 2011, p. 2). Pode-se entender essa característica como Customização. Segundo Pedrosa e Nogueira (2011, p. 2), "no atendimento a múltiplos usuários verifica-se a grande disparidade entre a necessidade dos mesmos, tornando essencial a capacidade de personalização dos recursos da nuvem".

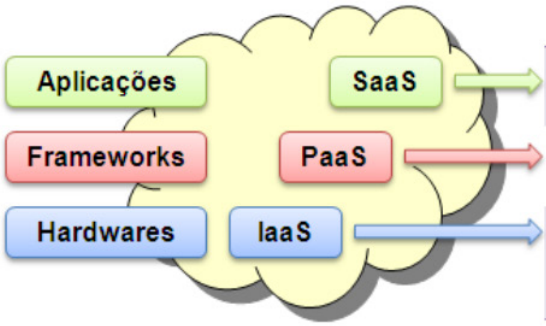
d. **Elasticidade rápida:** "capacidade dos usuários de aumentar ou diminuir rapidamente os recursos da nuvem sob demanda" (NIST, 2011, p. 2). Borges et al (2011, p. 6) ampliam esse entendimento como Elasticidade ("capacidade de disponibilizar e remover recursos computacionais em tempo de execução, independentemente da quantidade solicitada") e Escalabilidade ("relacionada com o requisito de aumento da capacidade de trabalho através da adição proporcional de recursos"). Os autores complementam enunciando que "os recursos parecem ser ilimitados e podem ser adquiridos em qualquer quantidade, ou seja, a demanda do usuário deve determinar a liberação e aquisição dos recursos e isto deve ser executado de forma rápida, transparente e sem intervenção humana".

e. **Medição dos serviços:** "o uso de recursos é monitorado, controlado e reportado, permitindo que os usuários sejam cobrados com base em seu uso para cada tipo de serviço, como por exemplo, armazenamento, processamento, largura de banda etc. (NIST, 2011, p. 2 – tradução nossa). "Por esta razão, as nuvens devem implementar recursos que garantam um eficiente comércio de serviços, tais como tarifação adequada, contabilidade, faturamento, monitoramento e otimização do uso" (Pedrosa e Nogueira, 2011, p. 2).

Outra importante característica desse modelo é a sua configuração como um repositório de recursos físicos e virtuais que podem ser atribuídos e configurados dinamicamente de acordo com a demanda de cada cliente, que mesmo não conhecendo a localização física dos recursos computacionais, pode especificar sua prioridade de localização com relação ao país e centro de dados.

O NIST (2011, p. 3-4) também define três modelos de serviços de CN (figura 2): infraestrutura como Serviço (IaaS), plataforma como um serviço (PaaS), e *software* como um serviço (SaaS).

Figura 2 - Modelos de serviços



Quem utiliza	Serviços
Usuário final	Email, Aplicativos de escritório, Blog, CRM, etc.
Desenvolvedores e implantadores	Desenvolvimento, integração, implantação e testes
Gerentes de Sistemas	Máquinas virtuais, sistemas operacionais, redes, CPU, memória, etc.

Fonte: Borges et al (2011, p. 6).

A infraestrutura como serviço (IaaS) é onde "são oferecidos os serviços de infraestrutura sob demanda, isto é, oferece recursos 'de *hardware*' virtualizados como computação, armazenamento e comunicação" (Pedrosa e Nogueira, 2011, p. 2). Para Borges et al (2011, p. 8) o IaaS "representa a camada inferior do modelo conceitual, sua base, ela é composta por plataformas para o desenvolvimento, teste, implantação e execução de aplicações proprietárias". O NIST (2011, p. 3 – tradução nossa) explica que "o consumidor não gerencia ou controla a infraestrutura de nuvem subjacente, mas possui controle sobre sistemas operacionais, armazenamento e aplicativos implantados; e, possivelmente, controle limitado de componentes de rede selecionados". Resumindo, é a capacidade que um provedor tem de oferecer uma infraestrutura de processamento e armazenamento de forma transparente.

A plataforma como serviço (PaaS) é a camada intermediária do modelo conceitual. Borges et al (2011, p. 9) informam que esse modelo "fornece ambientes de desenvolvimento de *software* e facilita a implantação de aplicações sem os custos e complexidades relativos à compra e gerenciamento do *hardware* e de *software* adjacentes que são necessários ao ambiente de desenvolvimento". Pedrosa e Nogueira (Pedrosa e Nogueira, 2011, p. 2) dialogam que os modelos PaaS e IaaS em conjunto fornecem "uma infraestrutura com alto nível de integração compatível com diversos sistemas operacionais, linguagens de programação e ambientes de desenvolvimentos".

A camada mais externa do modelo conceitual é o *software* como um serviço (SaaS). Ela é composta por aplicativos que são executadas no ambiente na nuvem. O NIST (2011, p.3) explica que essas aplicações são acessíveis a partir de vários dispositivos clientes através de uma interface, como um navegador da *Web* ou uma interface de programa. Borges et al (2011, p. 10) reforçam essa ideia ao interpretar que "os sistemas de *software* devem estar disponíveis na *internet* através de uma interface com um navegador *Web*, logo devem ser acessíveis de qualquer lugar a partir dos diversos dispositivos dos usuários". Sendo assim, essa camada disponibiliza aplicações completas ao usuário final.

Após as recomendações do NIST (2011), diversos modelos de nuvem poderão ser encontrados na literatura. Todavia, serão debatidos os mais utilizados e que são objeto dessa publicação do referido instituto internacional. São elas: nuvem pública, nuvem privada, nuvem comunidade e nuvem híbrida. Tonin et al (2019, p. 4) resumem a concepção das nuvens pública, privada e híbrida.

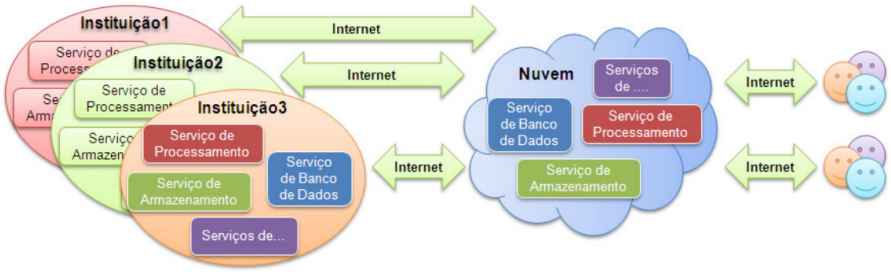
> Quanto à implementação nas organizações, o *cloud computing* pode ser público, privado ou híbrido, a nuvem pública é uma opção de custo mais acessível, cuja infraestrutura de *cloud* é compartilhada entre diversos clientes e toda a interação se dá por meio de protocolos da *internet*. Já a nuvem privada, permite a organização

> incorporar a infraestrutura dedicada às suas necessidades, normalmente ligada aos seus *datacenters* internos, seu uso está mais ligado à necessidade de controle do material que circula pelos servidores de uma empresa, com foco em maior segurança. Já o híbrido, mistura os dois conceitos, ampliando a possibilidade de uso, de maneira a possibilitar a guarda de dados sensíveis em uma aplicação na nuvem privada e interconectar em uma nuvem pública.

Os autores não discutem a nuvem comunidade (Figura 3), outro modelo bastante utilizado. Segundo o NIST (2011, p. 3, tradução nossa), esse modelo é definido como específico para aqueles que dividem as mesmas preocupações e objetivos.

> A infraestrutura dessa nuvem é provisionada para uso exclusivo de uma comunidade de consumidores de organizações que compartilham preocupações (por exemplo, missão, requisitos de segurança, política e considerações de conformidade). Pode ser propriedade, administrado e operado por uma ou mais organizações da comunidade, um terceiro partido, ou alguma combinação deles, e pode existir dentro ou fora das instalações.

Figura 3 - Modelo de nuvem comunidade

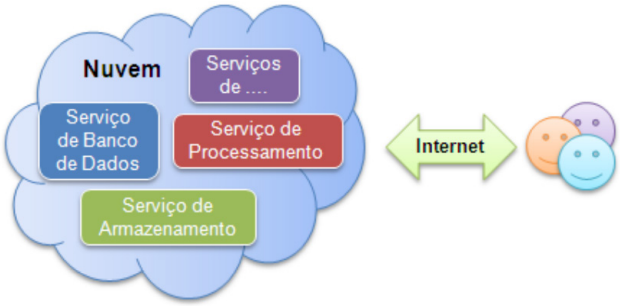


Fonte: Borges et al (2011, p. 12).

É importante destacar que embora a nuvem comunidade seja utilizada por vários membros, uma dessas organizações deverá se responsabilizar por sua administração.

Quanto à nuvem pública (Figura 4), trata de uma infraestrutura que pertence a determinada instituição que venda seus serviços para o público em geral. Borges et al (2011, p. 12) explicam que essas nuvens "tentam fornecer aos clientes elementos de TI livres de complexidades, onde o provedor da nuvem assume as responsabilidades de instalação, gerenciamento, disponibilização e manutenção". Ela pode ser operada por uma empresa, uma instituição acadêmica, um órgão público, ou uma combinação entre eles.

Figura 4 - Nuvem pública

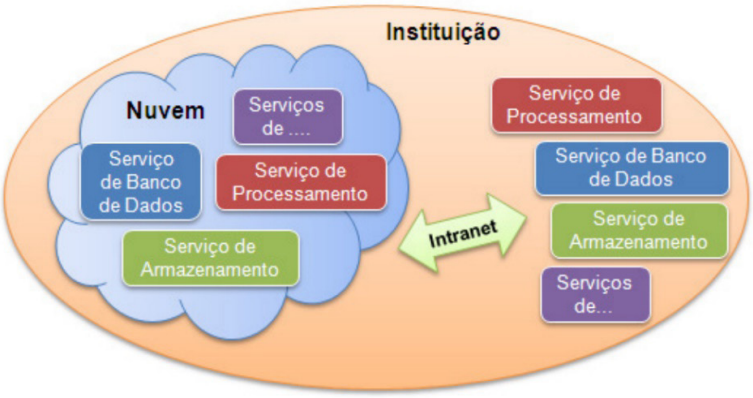


Fonte: Borges et al (2011, p. 12)**.**

Como alerta, devido ao seu acesso pelo público em geral, essa solução não é recomendada para aqueles que necessitam de segurança elevada e restrições regulamentares.

Ao contrário das nuvens pública e comunidade, a nuvem privada (Figura 5) é proprietária ou alugada por uma única organização, podendo ser local ou remota. Pedrosa e Nogueira (2011, p. 3) esclarecem que "o gerenciamento da rede pode ser feito pela própria organização ou por terceiros. No caso de ser feito por terceiros, a infraestrutura utilizada pertence ao usuário, desta maneira, ele é responsável pelo controle sobre a implementação das aplicações na nuvem".

Figura 5 - Nuvem privada



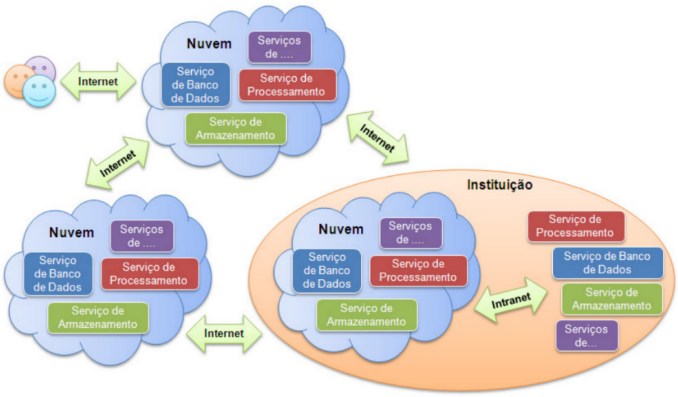
Fonte: Borges et al (2011, p. 11).

Taurion (2009, apud Borges et al, 2011, p. 11) que uma das vantagens da nuvem privada é "o fato da restrição de acesso, pois a mesma se encontra atrás do firewall da empresa, sendo uma forma de aderir à tecnologia, beneficiando-se das suas vantagens, porém mantendo o controle do nível de serviço e aderência às regras de segurança da instituição".

Por sua descrição, esse modelo aparenta ser o mais indicado para as políticas arquivísticas, principalmente como auxiliar na preservação digital. O controle mais detalhado sobre os vários recursos que constituem a nuvem, dando à empresa todas as opções de configuração possíveis, são pontos positivos para a sua utilização.

Por último, a nuvem híbrida (Figura 6) que é a solução que envolve duas ou mais nuvens simultaneamente, "sendo que cada nuvem permanece como uma entidade única, mas que estão unidas pelo uso de tecnologia proprietária ou padronizada, garantindo a portabilidade de dados e aplicações" (Pedrosa e Nogueira, 2011, p. 3). Ou seja, as características de cada modelo são mantidas, mas atuando em conjunto.

Figura 6 - Nuvem híbrida



Fonte: Borges et al (2011, p. 13).

Borges et al, (2011, p. 11) citam como limitação desse modelo a administração de uma solução desse porte, pois "serviços de diferentes fontes devem ser obtidos e disponibilizados como se fossem originados de um único local, e as interações entre componentes públicos e privados podem tornar a implementação ainda mais complicada".

Ao analisarmos o serviço de CN, e diante das ofertas apresentadas, não é possível indicar aquele considerado o ideal. Cada organização procurará atender as suas peculiaridades e, caso seja necessário, aplicar a plataforma que auxiliará nas demandas arquivísticas. No entanto, destaca-se a dificuldade em encontrar publicações na Arquivologia que tratem especificamente do assunto. O que chega a ser surpreendente, pois é um tema que age diretamente na área, levantando questões importantes sobre a preservação digital e custódia de documentos arquivísticos.

RDC-Arq e a Computação na Nuvem na custódia de documentos arquivísticos digitais.

Diante das concepções do RDC-Arq e da CN, será que é possível a atuação em conjunto desses dois modelos na custódia de um arquivo institucional? Antes de respondermos à pergunta é importante esclarecermos alguns pontos essenciais.

No tocante à CN, a informação que antes era armazenada dentro das estruturas informatizadas das instituições, localizar-se-á na nuvem em local físico que não se tem precisão onde é e nem que tipos de dados dividirão espaço junto a ela. A autenticidade dos documentos arquivísticos digitais é um item de suma importância, devendo ser levada em consideração na adoção da CN.

É manifesto que inúmeros fatores deverão ser elencados para a implantação da CN como aliada dos arquivos, tais como a definição de responsabilidades, o grau de absorção de informação e confiança no serviço de armazenamento adotado, e o acesso e perfil de cada usuário envolvido. Todavia, é fundamental realizar algumas perguntas para subsidiar a escolha ou a recusa dos serviços prestados pela solução de CN:

a. Qual modelo de nuvem adotar?
b. Se for um serviço pago e tiver que reduzir o espaço ou cancelar o contrato, o que acontecerá com as informações e como faremos a retirada?
c. A nuvem dará alguma garantia quanto à preservação digital ou é só armazenamento seguro?
d. Em caso de perda de informações, qual a garantia da empresa da nuvem?
e. Existirá autonomia para a sua utilização? (sem limite de tempo ou horário; no horário que quiser acessá-la; etc.)?
f. Possuirá suporte técnico e pessoal para treinar os servidores ou empregados do cliente?
g. A comunicação entre o cliente e o prestador de serviço terá criptografia ponta a ponta?

Esses questionamentos são fundamentais para o planejamento e desenvolvimento de uma estrutura em ambiente virtual. A CN não deve ser considerada uma estratégia única e definitiva para o arquivamento dos documentos arquivísticos digitais. Trata-se de um recurso complementar às políticas arquivísticas das instituições.

Por outro lado, o RDC-Arq é uma infraestrutura complexa que atuará como apoio na guarda dos documentos arquivísticos digitais, proporcionando que se alcancem níveis ideais de preservação digital. Lembrando que um repositório para ser arquivisticamente confiável, precisará conter requisitos técnicos, organizacionais e arquivísticos.

Os requisitos técnicos serão voltados para a segurança, equipamentos e tecnologias utilizadas; os organizacionais refletirão a governança, disponibilização de pessoal, arcabouço político, sustentabilidade financeira e contratos e licenças de fornecedores dos dispositivos informatizados; e o alinhamento arquivístico atuará nos pacotes de informação (SIP, AIP e DIP), refletindo a captura, o gerenciamento e o acesso dos documentos arquivísticos digitais.

Desse modo, conseguimos perceber semelhanças e diferenças na adoção entre o RDC-Arq e a CN (Tabela 2):

Tabela2 - Semelhanças e diferenças entre o RDC-Arq e a CN

Item	RDC-Arq	CN	Observações
Poderá controlar a preservação dos documentos arquivísticos digitais.	Sim	Não	Na CN, ficará a cargo do detentor da nuvem. No entanto, não há garantias que sustentem a preservação de documentos arquivísticos digitais nessa plataforma.
Infraestrutura tecnológica complexa a serviço de uma instituição.	Sim	Sim	Ambas possuem essa característica.
Pode ser acessado de qualquer lugar, bastando ter o *link* com a *internet.*	Não	Sim	A CN é oferecida pela *internet.*
Deverá acompanhar uma política de preservação digital.	Sim	Sim	Ambas possuem essa obrigação.
A infraestrutura tecnológica estará dentro da instituição.	Sim	Não	Os dois só possuirão essa característica, caso a mesma instituição os detenha.
Poderá ser terceirizado.	Não	Não	A CN não poderá ser terceirizada, pois, de acordo com a Resolução CONARQ nº 06/1997, caracteriza-se como guarda de documentos arquivísticos, e esse é um dever do Poder Público. O RDC-Arq pode ser construído por empresa privada, desde que bem definidas as condições, os deveres e as ações da contratada e o acompanhamento efetivo do órgão público.
Proporciona a redução de custos com a manutenção de equipamentos.	Não	Sim	Os custos não serão reduzidos, caso a instituição detenha os dois meios de custódia.
Visa o atendimento ao produtor/cidadão.	Sim	Sim	Ambas possuem essa característica.

Fonte: o próprio autor.

As características do RDC-Arq e da CN evidenciam suas ações para com os documentos arquivísticos digitais. Enquanto o RDC-Arq tem um direcionamento bem definido para a custódia e preservação digital; a

CN, embora possua atributos que permitam entendê-la como um local de guarda documental, tem a sua funcionalidade mais voltada à acessibilidade, já que pode ser pesquisada em qualquer lugar.

Assim, infere-se que o RDC-Arq e a CN não se excluem dentro de um cenário que contemple a custódia de documentos. São atores que podem atuar perfeitamente em sinergia e fortalecer as atividades a serem desempenhadas em documentos arquivísticos digitais.

Considerações finais

A custódia sempre esteve presente nas rotinas dos arquivos, procurando-se qualificar a guarda, a proteção e as relações de significância e poder entre o material custodiado e o custodiador. Todavia, com o crescimento da produção dos documentos arquivísticos digitais, vieram à tona dúvidas de como poderemos gerenciá-los e preservá-los. Sendo assim, as instituições precisam envidar esforços para garantir a custódia adequada em ambiente digital e proporcionar a manutenção da autenticidade e longevidade de seus acervos.

No cerne desse contexto, após pertinentes discussões na Arquivologia, e com o intuito de se atingir a salvaguarda ideal dos documentos, elencou-se o RDC-Arq como o modelo capaz de proporcionar níveis de excelência para a preservação dos documentos arquivísticos digitais, englobando os aspectos normativos, a definição de responsabilidades e os requisitos tecnológicos. Sempre ressaltando que o RDC-Arq não é uma mera solução tecnológica, mas sim uma grande engrenagem que envolve decisões, qualificação profissional e tecnologia condizentes com as necessidades de cada instituição.

Por outro lado, diferentemente do que é preconizado pelos repositórios institucionais, em que cada produtor deverá manter a estrutura tecnológica dentro de suas dependências, a CN apresentou-se como estratégia terceirizada e econômica para o arquivamento e a preservação dos documentos arquivísticos digitais. Entretanto, mesmo com as facilidades de utilização e possibilidades infinitas de armazenamento, ainda não existem evidências conclusivas que garantam que os arquivos estarão seguros em serviços prestados nessa plataforma. Sendo assim, não é recomendável a utilização da CN como meio único para a custódia dos documentos arquivísticos.

Atualmente, os órgãos públicos ainda estão impedidos de terceirizarem a custódia de seus documentos. No entanto, entendendo-se a dificuldade de obter profissionais especializados em seus quadros de servidores, nada pode impedi-los de contratarem serviços para a construção de uma infraestrutura que abranja o RDC-Arq e a CN, através de planejamento bem definido e investimentos condizentes com cada realidade. Essas ações proporcionarão o emprego adequado de esforço, tempo, e recursos financeiros na custódia, preservação e acessibilidade dos documentos arquivísticos digitais.

Por fim, ainda precisamos de mais debates sobre a aplicabilidade e extensão dos serviços da CN nos arquivos. Entretanto, é necessária a compreensão sobre como os dois modelos podem ser parceiros, cada um com a sua incumbência, definindo-se antecipadamente as regras de negócio, em que o RDC-Arq proporcionará a preservação digital, enquanto os serviços ofertados na nuvem fornecerão a acessibilidade dos documentos arquivísticos.

REFERÊNCIAS

ARQUIVO NACIONAL (Brasil). **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005.

BORGES, Hélder Pereira; SOUZA, José Neuman de; SCHULZE, Bruno; MURY, Antônio Roberto. **Computação em nuvem**. Brasil, 2011. Disponível em: https://livroaberto.ibict.br/handle/1/861. Acesso em: 28 fev 2023.

BRAGA, Tiago Emmanuel Nunes; HOLANDA, Alex Pereira; CANELHAS, Tatiana. Resolução RDC- ArqConarq: uma análise dos novos requisitos informacionais propostos. **Revista Brasileira de Preservação Digital**, Campinas, SP, v. 3, n. 00, p. e022004, 2022. DOI: 10.20396/rebpred.v3i00.16583. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/16583. Acesso em: 11 fev. 2023.

BRASIL. Lei n. 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial [da] República Federativa do Brasil.** Brasília, DF, 09 de jan. de 1991. Seção 1, p. 457. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8159.htm. Acesso em: 10 abr. 2021.

CÂNDIDO, Ana Clara; ARAÚJO JÚNIOR, Rogério Henrique de. Potencialidades do desenvolvimento de *cloud computing* no âmbito da gestão da informação. **Perspectivas em Ciência da Informação**, [S. l.], v. 27, n. 1, 2022. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/25731. Acesso em: 28 fev. 2023.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ).Câmara Técnica de documentos eletrônicos (CTDE). Orientação Técnica n.º 3, novembro/2015**:** Cenários de uso de RDC-Arq em conjunto com o SIGAD. Disponível em: https://bit.ly/3Pa5FjU. Acesso em: 23fev 2023.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Câmara Técnica de** Documentos Eletrônicos (CTDE). **Glossário:** Documentos arquivísticos digitais (versão 8.0). Rio de Janeiro, 2020. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glossario-da-ctde. Acesso em: 08 jan. 2021.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 06, de 15 de maio de 1997.** Dispõe quanto à terceirização de serviços arquivísticos públicos. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-6-de-15-de-maio-de-1997. Acesso em: 05 jan. 2023.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ**). Resolução nº 39, de 29 de abril de 2014**. Estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos- SINAR. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-39-de-29-de-abril-de-2014. Acesso em: 10 abr. 2021.

HEDLER, Helga Cristina et al. Aplicação do Modelo de Aceitação de Tecnologia à Computação em Nuvem. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 6, n. 2, p. 204-217, jul./dez. 2016.

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA (IBICT). **Glossário da Rede Cariniana** (recurso eletrônico). Campinas, UNICAMP/BCCL; IBICT, 2022. Disponível em: https://glossario.cariniana.ibict.br/vocab/index.php. Acesso em: 02 dez de 2022.

LAMPERT, Sérgio Renato; FLORES, Daniel. O repositório digital como instrumento para preservação e acesso ao patrimônio arquivístico documental . **Anais do VII SIMP**: Convenção do Patrimônio Imaterial: 10 anos depois [2003-2013], 6 a 8 de novembro de 2013. Disponível em: https://repositorio.furg.br/bitstream/handle/1/7748/92455edb492a8134308145ead253c3ad.pdf?sequence=1. Acesso em: 10 abr. 2021.

MASSON, Silvia Mendes. Os repositórios digitais no âmbito da sociedade informacional. **Prisma.com** (Portugal), n. 7, p. 105-152, 2008. Disponível em: https://brapci.inf.br/index.php/res/v/62295. Acesso em: 10 abr. 2021.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) 800-145 (2011). The NIST definition of *cloud computing*. **Recommendations of the National Institute of Standards and Technology**, Peter Mell and Timothy Grance, USA, 2011. Disponível em: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf. Acesso em 28 fev de 2023.

OLIVEIRA, Claudio Paulino de. **Recomendações para a preservação de documentos arquivísticos digitais produzidos pelo Estado do Rio de Janeiro.** 2023. 225p. Produto técnico-científico (Mestrado em Gestão de Documentos e Arquivos) — PPGARQ, Universidade Federal do Estado do Rio de Janeiro, Rio de Janeiro, 2023. Disponível em: https://www.unirio.br/ppgarq/tccs/turma-2021/oliveira-claudio-paulino-de-recomendacoes-para-a-preservacao-de-documentos-arquivisticos-digitais-produzidos-pelo-estado-do-rio-de-janeiro/view. Acesso em: 05 mai 2024.

PEDROSA, Paulo; NOGUEIRA, Tiago. **Computação em Nuvem**. 2011. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531-t2.pdf. Acesso em: 02 fev 2023.

ROCHA, Claudia. Lacombe. Repositórios para a preservação de documentos arquivísticos digitais. **Acervo**-Revista do Arquivo Nacional, v. 28, n. 2, p. 180-191, 2015. Disponível em: https://brapci.inf.br/#/v/40764. Acesso em: 10 abr. 2021.

SANTOS, Henrique Machado dos; FLORES, Daniel. Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo. **Perspectivas em Ciência da Informação**, v. 20, n. 2, p. 198-218, 2015. Disponível em: https://brapci.inf.br/#/v/36891. Acesso em: 10 abr. 2021.

SANTOS, Vanderlei Batista. Preservação digital de documentos arquivísticos potenciais: reconhecendo e enfrentando o problema. **Revista Brasileira de Preservação Digital**, Campinas, SP, v. 3, n. 00, p. e022005, 2022. DOI: 10.20396/rebpred.v3i00.16584. Disponível em: https://econtents.bc.unicamp.br/inpec/index.php/rebpred/article/view/16584. Acesso em: 11 fev. 2023.

SILVA, Margareth. **O arquivo e o lugar**: a custódia arquivística como responsabilidade pela proteção aos arquivos. 2015. Tese (Doutorado em História Social)- Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/8/8138/tde-22122015-093801/publico/2015_MargarethDaSilva_VCorr.pdf. Acesso em: 23 ago 2023.

TAURION, Cezar. **Entendendo o modelo multi-**tenancy**.** 2010. Disponível em: https://imasters.com.br/*cloud*/entendendo-o-modelo-multi-tenancy. Acesso em: 24 fev 2023.

THOMAZ, Kátia de Pádua. Repositórios digitais confiáveis e certificação. **Arquivística.net**, v. 3, n. 1, 2007. Disponível em: https://brapci.inf.br/#/v/50354. Acesso em: 10 abr. 2021.

TONIN, Laís Bueno; CANCIAN, Wainer; CHIARATO, Ana Cláudia. O uso do *cloud computing* para armazenamento de dados e informações em organizações: benefícios e desafios. **Revista Scientia Alpha**. V.1, nº 1. Umuarama. PR. 2019. Disponível em: https://revista.alfaumuarama.edu.br/index.php/rsa/article/view/10. Acesso em: 24 fev. 2023.

VELTE, Anthony; VELTE, Toby; ELSENPETER, Robert. Computação em nuvem: uma abordagem prática. Rio de Janeiro: Alta Books, 2012. Disponível em: https://silo.tips/download/computaao-em-nuvem-uma-abordagem-pratica#. Acesso em: 22 fev 2023.

VERAS, Manoel. *Cloud computing*: Nova Arquitetura da TI. Rio de Janeiro: BRASPORT, 2012.