DOI: 10.5433/1981-8920.2021v26n4p424

AUDITORIA E CERTIFICAÇÃO AO LONGO DA CADEIA DE CUSTÓDIA DIGITAL ARQUIVÍSTICA

AUDIT AND CERTIFICATION THROUGHOUT THE ARCHIVAL DIGITAL CHAIN OF CUSTODY

Tânia Barbosa Salles Gava [a]
Daniel Flores [b]

RESUMO
Objetivo: Discutir a importância do processo de auditoria e certificação em todos os ambientes envolvidos nas três entidades externas do Modelo OAIS, analisando o cenário brasileiro. **Metodologia**: Pesquisa exploratória, bibliográfica e documental, tendo como principais fontes documentais e bibliográficas a documentação produzida por diferentes organizações, normativas do Conselho Nacional de Arquivos e artigos científicos de pesquisadores nacionais e internacionais**. Resultados**: Discussão sobre os modelos conceituais de requisitos e de auditoria e certificação, no cenário brasileiro, para os três ambientes envolvidos no Modelo OAIS: o ambiente do produtor, que é o ambiente de gestão dos documentos; o ambiente do administrador, que é o ambiente de preservação dos documentos; o ambiente do consumidor, que é o ambiente de acesso e difusão dos documentos. **Conclusões**: No cenário brasileiro há modelos de requisitos para o ambiente de gestão dos documentos, mas não estabelece requisitos de auditoria e certificação; o ambiente de preservação apresenta tanto requisitos funcionais, não funcionais e regras de negócio, quanto requisitos de auditoria e certificação; o ambiente de acesso e difusão dos documentos ainda não possui diretrizes estabelecidas.

Descritores: Auditoria e Certificação. Cadeia de Custódia Digital Arquivística. Ambiente de Gestão de Documentos. Ambiente de Preservação. Ambiente de Acesso e Difusão.

1 INTRODUÇÃO

Desde a década de 1990, quando a sociedade começou a passar por uma transformação digital cada vez mais rápida, os documentos passaram a ser

[a] Doutora em Engenharia Elétrica - Automação, na área de Inteligência Artificial Aplicada pelo Programa de Pós-Graduação em Engenharia Elétrica (PPGEE) da Universidade Federal do Espírito Santo (UFES). Professora do Departamento de Arquivologia da Universidade Federal do Espírito Santo (UFES). E-mail: tania.gava@ufes.br.

[b] Doutor em Ciência da Informação pela Universidade Federal do Rio de Janeiro (UFRJ). Professor do Programa de Pós-Graduação em Ciência da Informação da Universidade Federal Fluminense (PPGCI-UFF). E-mail: df@id.uff.br.

migrados ou gerados exclusivamente no formato digital. Embora esses documentos digitais, representantes digitais ou nato digitais, tenham trazido grandes vantagens como a facilidade de criação, acesso e compartilhamento, eles se tornaram altamente complexos e específicos, trazendo muitas vulnerabilidades ligadas principalmente a sua rápida degradação física, obsolescência tecnológica, complexidade e alto custo para sua preservação a longo prazo (SANTOS; FLORES, 2015a). Essas vulnerabilidades trouxeram uma grande preocupação em relação à autenticidade e confiabilidade dos documentos digitais, pois para que eles sirvam de fonte de prova, evidência, testemunho, memória, patrimônio, garantia de direitos e exercício pleno da cidadania, eles devem ser mantidos autênticos e confiáveis pelo tempo que for necessário.

Segundo as Diretrizes do Produtor do Projeto InterPARES 2, a "Autenticidade refere-se ao fato de que os documentos arquivísticos são o que eles dizem ser e que não foram adulterados ou corrompidos de qualquer outra forma." (INTERPARES 2 PROJECT, 2010a, p. 03). O projeto InterPARES 2 também afirma que, em relação aos documentos arquivísticos digitais, a autenticidade refere-se à confiabilidade dos documentos enquanto tais e que para assegurar que a autenticidade possa ser presumida e mantida ao longo do tempo, deve-se definir e conservar a identidade dos documentos arquivísticos e proteger sua integridade. Já a confiabilidade é definida como a credibilidade do material digital enquanto conteúdo ou declaração de um fato, sendo estabelecida com base na completeza e acurácia do material, e no grau de controle exercido no processo de sua produção (INTERPARES 2 PROJECT, 2010a).

Ressalta-se que esses cuidados não são exclusivos para os documentos nato digitais, devendo também ser considerados na produção dos representantes digitais, que são a representação em formato de arquivo digital de um documento originalmente não digital. Ou seja, a digitalização dos documentos também deve garantir a autenticidade e confiabilidade dos documentos não somente no ato da digitalização, mas a manutenção dessas características ao longo do tempo.

Essa transformação digital, desafiada pela vulnerabilidade do ambiente digital, instigou as organizações ao redor do mundo a pensarem na preservação digital dos documentos. Como resultado desse trabalho surgiram vários modelos, normas e padrões internacionais, tais como a ISO 16363:2012, que é a norma que permite a certificação de confiança para Repositórios Digitais Confiáveis (RDC) de organizações públicas ou privadas; o Modelo OAIS (ISO 14721:2012), que é um modelo conceitual que visa identificar os componentes funcionais que deverão fazer parte de um RDC, e que descreve as interfaces internas e externas do sistema (produtor, administrador e consumidor), como também os objetos de informação que são manipulados no seu interior; e a ISO 16919:2014, que é uma recomendação técnica, criada pelo *Consultative Committee for Space Data Systems* (CCSDS), que estabelece requisitos para as entidades de auditoria e certificação de um RDC.

Em relação ao Brasil, a preocupação com a preservação do patrimônio arquivístico digital se deu principalmente a partir da publicação, em 2005 pelo Conarq, da Carta para a Preservação do Patrimônio Digital da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), manifestando a necessidade dos Estados-membros, incluindo o Brasil, estabelecerem políticas e ações para a proteção do patrimônio digital (CONSELHO NACIONAL DE ARQUIVOS, 2005). Assim, a Carta deu início a uma série de publicações técnicas do Conselho Nacional de Arquivos, tais como o e-ARQ Brasil (CONSELHO NACIONAL DE ARQUIVOS, 2011), que apresenta um modelo de requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, e a Resolução n.º 43 (CONSELHO NACIONAL DE ARQUIVOS, 2015a), que estabelece as diretrizes para a implementação de Repositórios Arquivísticos Digitais Confiáveis.

Em relação ao cenário brasileiro, essa evolução conceitual se deu muito em direção ao ambiente de preservação dos documentos, com modelos conceituais que abrangem tanto seus requisitos funcionais, não funcionais e regras de negócio, quanto requisitos de auditoria e certificação. No entanto, o mesmo não aconteceu com os ambientes de gestão de documentos e de acesso e difusão, principalmente em relação aos requisitos de auditoria e certificação.

Nesse contexto, este artigo tem como objetivo principal discutir a importância do processo de auditoria e certificação em todos os ambientes envolvidos nas três entidades externas do Modelo OAIS, analisando o cenário brasileiro. Do ponto de vista arquivístico, essas entidades estão em todo o ciclo de vida dos documentos arquivísticos digitais, em três ambientes principais: o ambiente de gestão de documentos, o ambiente de preservação (OAIS *Archive*) e o ambiente de acesso e difusão, perpassando toda a cadeia de custódia que acontece agora no ambiente digital.

Trata-se de uma pesquisa exploratória, analisando os principais aspectos envolvidos na auditoria e certificação dos ambientes de gestão de documentos, preservação, acesso e difusão dos documentos arquivísticos digitais, como também uma revisão bibliográfica para a contextualização teórica do tema proposto e fundamentação da pesquisa, "[...] desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos" (GIL, 2002, p. 44), e documental, por investigar diferentes fontes documentais (GIL, 2002). Em relação aos procedimentos metodológicos, foi feita uma pesquisa na documentação produzida por diferentes organizações, nas normativas do Conselho Nacional de Arquivos (Conarq) e em artigos científicos de pesquisadores nacionais e internacionais, especialistas nas áreas investigadas.

2 AUTENTICIDADE E CONFIABILIDADE DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Para que os documentos arquivísticos digitais sirvam para seu propósito, eles devem ser preservados pelo tempo que for necessário. Assim, a preservação digital deve manter os documentos autênticos e confiáveis ao longo do tempo. O e-ARQ Brasil (CONSELHO NACIONAL DE ARQUIVOS, 2020b), em sua versão mais recente, ainda em consulta pública, esclarece os conceitos ao apresentar que:

> Um documento arquivístico autêntico é aquele que é o que diz ser, independentemente de se tratar de minuta, original ou cópia, e que é livre de adulterações ou qualquer outro tipo de corrupção. Enquanto a confiabilidade está relacionada ao

> momento da produção, a autenticidade está ligada à transmissão do documento e à sua preservação e custódia. Um documento autêntico é aquele que se mantém da mesma forma como foi produzido e, portanto, apresenta o mesmo grau de confiabilidade que tinha no momento de sua produção. Assim, um documento não completamente confiável, mas transmitido e preservado sem adulteração ou qualquer outro tipo de corrupção, é autêntico. (CONSELHO NACIONAL DE ARQUIVOS, 2020b, p. 37).

Com a transformação digital, a autenticidade e confiabilidade dos documentos foram colocadas em risco, pois em uma cadeia de custódia digital os documentos precisam ser, invariavelmente, transmitidos através do tempo e do espaço em um ambiente digital altamente vulnerável. Isso se dá, por exemplo, quando um documento é transmitido de seu ambiente de produção para um ambiente de preservação. Sendo assim, é necessário que a autenticidade e confiabilidade dos documentos sejam mantidas não somente no momento de sua produção, mas também durante toda sua transmissão, custódia e preservação.

> A presunção de autenticidade dos documentos arquivísticos sempre fez parte do processo tradicional de avaliação desses documentos e é fortemente apoiada na análise de sua forma e de seu conteúdo, que nos documentos não digitais estão inextricavelmente ligados ao suporte – isto é, forma, conteúdo e suporte são inseparáveis. Além disso, essa presunção baseia-se na confirmação da existência de uma cadeia de custódia ininterrupta, desde o momento da produção do documento até a sua transferência para a instituição arquivística responsável pela sua preservação no longo prazo. Caso essa cadeia de custódia seja interrompida, o tempo em que os documentos não estiveram sob a proteção do seu produtor ou sucessor pode causar muitas dúvidas sobre a sua autenticidade. (CONSELHO NACIONAL DE ARQUIVOS, 2012, p. 01).

Para isso, é importante que se desenvolvam procedimentos que estabeleçam controles sobre a produção, transmissão, manutenção e preservação dos documentos arquivísticos digitais. Esses procedimentos devem incorporar controles adequados e eficazes para garantir a autenticidade e confiabilidade dos documentos arquivísticos, e devem especificamente (INTERPARES 2 PROJECT, 2010b, p. 03):

> - Manter a custódia ininterrupta dos documentos arquivísticos;
> - Implementar e monitorar procedimentos de segurança e controle;

> • Garantir que o conteúdo dos documentos arquivísticos e as anotações e elementos da forma documental não sofram alterações após a reprodução.

Assim, essa cadeia de custódia digital para os documentos arquivísticos digitais deve contemplar todo o ciclo de vida dos documentos, desde sua produção até sua destinação final, que é sua preservação ou eliminação.

Destaca-se que esse ciclo de vida contempla três ambientes: o ambiente de gestão de documentos, o ambiente de preservação e o ambiente de acesso e difusão, bem como a transição entre eles, que é feita em um ambiente digital altamente vulnerável e, portanto, sujeito a adulterações. Para que esse processo de custódia em um ambiente digital altamente vulnerável se dê de forma segura, é necessário que se criem requisitos de auditoria e certificação para cada um desses ambientes, e não somente requisitos funcionais, não funcionais e regras de negócio.

3 A IMPORTÂNCIA DA AUDITORIA E CERTIFICAÇÃO EM TODA A CADEIA DE CUSTÓDIA DOS DOCUMENTOS

Em toda e qualquer organização, o processo de certificação de normas, modelos de referência e padrões é fundamental para que os processos, produtos e serviços sejam constantemente melhorados. Para isso, a organização deve passar por um processo de auditoria, seja ela interna ou externa, para que a organização evolua de forma constante em seu desempenho na execução de atividades e otimização de processos, a fim de oferecer maior qualidade de seus serviços. O processo de auditoria, segundo a ABNT/NBR/ISO 19011 (2018, p. 01), é o “processo sistemático, independente e documentado para obter evidência objetiva e avaliá-la objetivamente, para determinar a extensão na qual os critérios de auditoria são atendidos”. Uma evidência objetiva são dados que apoiam a existência e veracidade de alguma coisa, podendo ser obtida por meio de observação, medição, ensaio ou outros meios. Para o propósito de auditoria, a evidência objetiva geralmente consiste em registros, declarações de um fato ou outra informação que seja pertinente para os critérios de auditoria e verificável. Os critérios de auditoria são o “conjunto de requisitos usados como

uma referência com a qual a evidência objetiva é comparada" (ABNT/NBR/ISO 19011, 2018, p. 02). Assim, o processo de auditoria tem como objetivo preparar a organização para que ela seja certificada por um órgão competente, conferindo a qualidade dos serviços prestados.

No processo de preservação digital, em particular numa preservação digital sistêmica (ativa), que tem como objetivo preservar os documentos autênticos e confiáveis ao longo do tempo, o processo de auditoria e certificação é muito importante. Por preservação digital sistêmica entende-se como a devida integração de um ambiente de gestão de documentos, de um ambiente de preservação de documentos e de um ambiente de acesso e difusão de documentos, visando manter a sua autenticidade e confiabilidade ao longo do tempo, ou seja, não só no momento da produção, como também durante todo o ciclo de vida dos documentos e pelo tempo que for necessário, mantendo uma cadeia de custódia digital segura e ininterrupta. O processo de auditoria, consiste em verificar e avaliar as metodologias adotadas pela instituição, e assim é possível verificar a conformidade desses ambientes com as normas, modelos e padrões que foram adotados e o comprometimento com as ações de preservação digital no que tange a infraestrutura física, técnica e tecnológica (SANTOS; FLORES, 2015b).

3.1 A Necessidade de uma Cadeia de Custódia Digital Arquivística

No ambiente analógico, a transferência física e legal dos documentos de uma instituição produtora para uma instituição arquivística custodiadora (sucessor legítimo), ou seja, do produtor para um custodiador confiável, assegurava uma cadeia de custódia ininterrupta (HIRTLE, 2001). No entanto, no ambiente digital isso não é verdade, pela especificidade e complexidade do documento digital e suas vulnerabilidades. Sendo assim, da mesma forma que os Repositórios Digitais Confiáveis precisaram ser ressignificados, necessitando de uma adjetivação arquivística, incorporando normas e princípios arquivísticos para se tornarem Repositórios Arquivísticos Digitais Confiáveis, há a mesma necessidade para uma cadeia de custódia digital, sendo necessária uma Cadeia de Custódia Digital Arquivística (CCDA), entendida por Gava e Flores (2020, p.

92) como:

> [...] uma definição de Cadeia de Custódia Digital Arquivística (CCDA) deve trazer a ideia de que a cadeia de custódia digital não pode ser interrompida, e deve ser auditada pela cadeia de preservação ou outro procedimento capaz dessa garantia no ambiente digital. Além disso, que a presunção de autenticidade deve ser mantida quando acontece a mudança de custódia de um ambiente digital, que por si só é extremamente vulnerável, para outro, como, por exemplo, de um SIGAD, SIGAD de Negócio ou qualquer outro sistema de informação digital para um RDC-Arq, independentemente da fase. Essa presunção de autenticidade deve vir apoiada pela evidência de que os documentos não foram modificados ou corrompidos em seus aspectos essenciais durante a sua transmissão de um ambiente digital para outro (GAVA; FLORES, 2020, p. 92).

Ou seja, a CCDA pode ser entendida como um princípio aplicável aos documentos digitais, considerando suas especificidades e complexidades, para garantir que esses documentos de arquivo não tenham uma ruptura em sua cadeia de custódia arquivística em um ambiente digital, mantendo-os sempre confinados em ambientes com requisitos arquivísticos homologados, desde a sua produção ou representação, transmissão, arquivamento, até a sua guarda permanente, acesso ou eliminação. Esse processo deve ser desenvolvido com o devido registro de todas as alterações ocorridas ao longo do tempo, de forma sistêmica, assegurando, assim, a garantia da autenticidade e confiabilidade dos documentos ao longo do tempo, em uma abordagem de Preservação Digital Sistêmica ou Ativa.

Um outro conceito importante neste contexto é o de cadeia de preservação, que é definida como um “Sistema de controles que se estende por todo o ciclo de vida dos documentos, a fim de assegurar sua autenticidade ao longo do tempo.” (INTERNATIONAL COUNCIL ON ARCHIVES, 2012). Embora esses dois conceitos sejam diferentes, eles se complementam. A cadeia de preservação, como o próprio nome diz, tem como objetivo garantir a preservação dos documentos arquivísticos digitais a longo prazo. O projeto InterPARES 2 apresenta um modelo de Cadeia de Preservação – *Chain of Preservation* (CoP) como uma sequência de “[...] passos para a produção, manutenção, avaliação e preservação digital de documentos autênticos” (INTERPARES 2 PROJECT, 2010b, p. 02). Essa cadeia de preservação deve

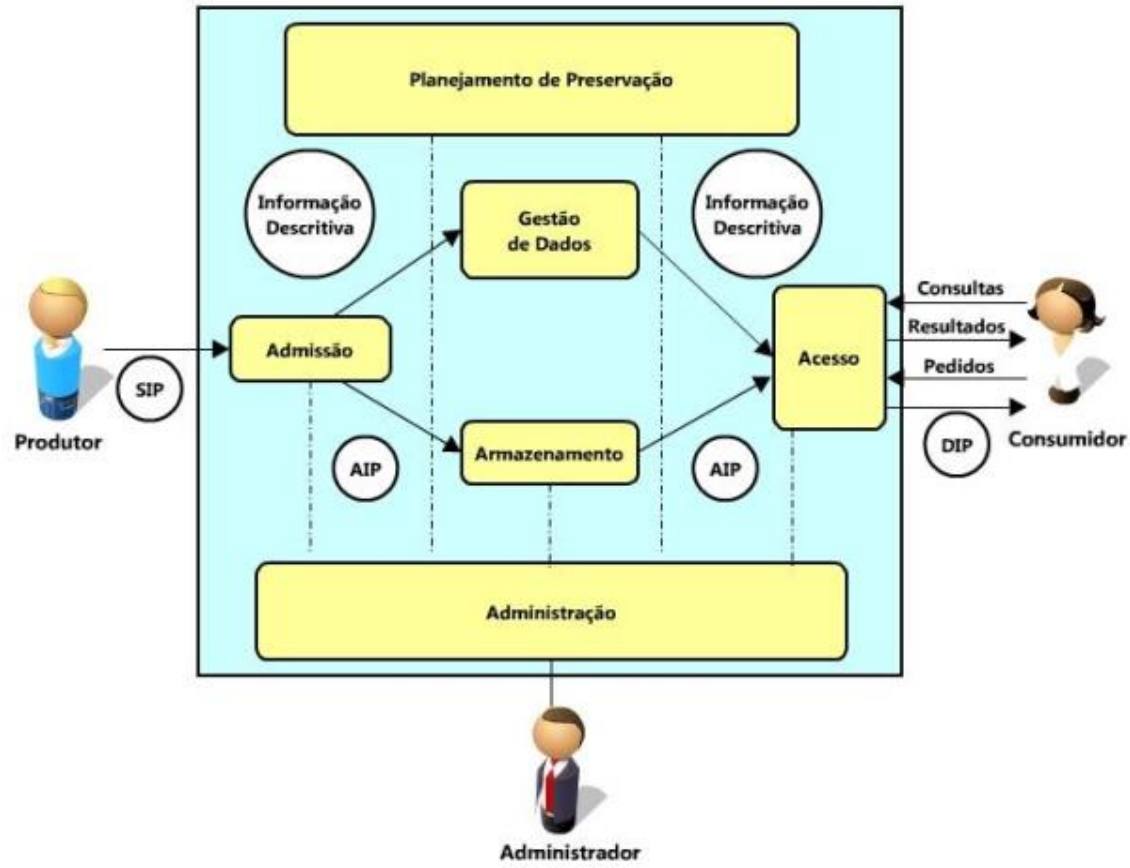
ser observada em todo o ciclo de vida dos documentos, tal como a cadeia de custódia – *Chain of Custody* (CoC). Ou seja, são dois processos que devem ocorrer concomitantemente, ambos buscando a manutenção da autenticidade dos documentos.

> [...] é possível vislumbrar que a CoP se apresenta de forma muito mais computacional, já que está focada em registrar, por meio de metadados e modelos computacionais, a sua implementação. Trata-se de uma abordagem mais técnica e tecnológica e diferente da abordagem da CoC, que por sua vez, não está focada num modelo computacional, e sim na ideia de um princípio arquivístico, de cuidado, de um querer, de um manter a linha ininterrupta, apresentando a necessidade de cotejar o documento arquivístico digital. A CoP por sua vez, é a implementação tecnológica da CoC, que agora, precisa ser ressignificada em um ambiente digital, já que a CoP não substitui a CoC enquanto princípio (GAVA; FLORES, 2020, p. 89).

Nesse contexto, o processo de auditoria e certificação será abordado para cada um dos ambientes envolvidos nas três entidades externas do Modelo OAIS: o ambiente do produtor, que é o ambiente de gestão dos documentos; o ambiente do administrador, que é o ambiente de preservação dos documentos; e o ambiente do consumidor, que é o ambiente de acesso e difusão dos documentos.

O modelo OAIS é um modelo internacionalmente aceito, e amplamente utilizado, que tem como objetivo identificar os componentes funcionais que deverão fazer parte de um sistema de informação dedicado à preservação digital. O modelo também descreve as interfaces internas e externas do sistema e os objetos de informação que são manipulados no seu interior (FERREIRA, 2006). A Figura 1 apresenta os componentes funcionais, os pacotes de informação e as entidades externas de um sistema de preservação compatível com o Modelo OAIS (CONSELHO NACIONAL DE ARQUIVOS, 2015a).

Figura 1 – O Modelo de Referência OAIS



Fonte: CONSELHO NACIONAL DE ARQUIVOS (2015a, p. 20)

3.2 Auditoria e Certificação no Ambiente de Gestão de Documentos

O processo de gestão arquivística dos documentos é definido como o "Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos arquivísticos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente." (CONSELHO NACIONAL DE ARQUIVOS, 2020a, p. 32). No Brasil, temos dois modelos de gestão de documentos: um modelo para o contexto do poder Executivo e Legislativo, que é o SIGAD (Sistemas informatizados de Gestão Arquivística de Documentos), definido pelo e-ARQ Brasil (CONSELHO NACIONAL DE ARQUIVOS, 2011), que passou recentemente por uma reformulação (CONSELHO NACIONAL DE ARQUIVOS, 2020b), estando atualmente em consulta pública. E outro modelo para o contexto

do Judiciário, que é o GestãoDoc (Sistema Informatizado de Gestão de Processos e Documentos), definido pelo MoReq-Jus (CONSELHO NACIONAL DE JUSTIÇA, 2009).

O e-ARQ Brasil (CONSELHO NACIONAL DE ARQUIVOS, 2011, p. 09) é uma "[...] especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade." O e-ARQ Brasil estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido ou implantado. Já o MoReq-Jus (CONSELHO NACIONAL DE ARQUIVOS, 2009) é o modelo que estabelece processos e requisitos mínimos que os documentos digitais e os sistemas informatizados de gestão documental (GestãoDoc) deverão cumprir com o objetivo de garantir a segurança e a preservação das informações, assim como a comunicação com outros sistemas. Como exemplo de outros modelos de sistemas de gestão no âmbito internacional temos a norma DOD 5015.2-STD[3] - *Design criteria standard for electronic records management software applications*, dos Estados Unidos da América, os *Requirements for electronic records management systems: Functional requirements*[4], do Reino Unido e a norma AS ISO 15.489/2002[5], da Austrália, dentre outros. No entanto, é importante destacar que os modelos de gestão arquivística de documentos estabelecidos no cenário brasileiro não apresentam requisitos de auditoria e certificação.

Embora a especificação de requisitos para sistemas de gestão de documentos no poder executivo, legislativo e judiciário esteja estabelecida, a prática ainda não tem acompanhado a evolução teórica desses modelos. Além disso, na iniciativa privada ainda temos um contexto de uso de Sistemas de Gerenciamento Eletrônico de Documentos (GED) e de *Enterprise Content Management* (ECM), que não implementam uma abordagem arquivística, nem em relação à questão orgânica, nem em relação à visão sistêmica da

[3] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/501502std.pdf
[4] https://www.nationalarchives.gov.uk/documents/requirementsfinal.pdf
[5] https://www.saiglobal.com/pdftemp/previews/osh/as/as10000/15000/154891.pdf

Preservação Digital ou da Cadeia de Custódia, tendo a necessidade de que esses sistemas evoluam para um sistema de gestão com requisitos arquivísticos.

No entanto, embora a especificação de requisitos para sistemas de gestão de documentos esteja bem estabelecida no cenário brasileiro, ainda não existem normativas no Brasil para a auditoria e certificação de sistemas de gestão de documentos.

3.3 Auditoria e Certificação no Ambiente de Preservação

No Brasil, a Resolução n.º 43 do Conarq (CONSELHO NACIONAL DE ARQUIVOS, 2015a) veio como uma resposta para a necessidade da criação do **Arquivo Permanente Digital,** definindo as diretrizes para a implementação de um Repositório Arquivístico Digital Confiável (RDC-Arq). Ou seja, despertou-se para a necessidade da especificação de um ambiente seguro para a preservação permanente dos documentos arquivísticos digitais, considerando sua fragilidade, especificidade e complexidade, principalmente porque era necessário garantir uma preservação permanente, de 50 anos ou mais (GLADNEY, 2009), e não mais uma preservação somente de longo prazo, ou seja, de cinco (05) anos a partir da data de produção do documento digital, como preconizada pelo Conselho Internacional de Arquivos. Mas, mais do isso, a Resolução n.º 43 também despertou sobre a necessidade do uso de um RDC-Arq em todas as fases do ciclo de vida dos documentos, e não somente na fase permanente, quando recomenda a sua adoção pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR, para o arquivamento e manutenção dos documentos arquivísticos em suas fases corrente, intermediária e permanente em formato digital, a fim de garantir a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade e a preservação dos documentos arquivísticos digitais.

Embora em 2015 o Brasil ainda estivesse iniciando com as iniciativas de implementação de um RDC-Arq, em outros países a realidade já era diferente:

> Em vários países os arquivos nacionais e outras instituições arquivísticas públicas já contam com uma solução para atuarem como repositórios digitais confiáveis para os documentos em fase permanente, e em alguns casos recebem também

> documentos em fase intermediária. Alguns deles já têm atuado fortemente no desenvolvimento de uma infraestrutura de repositórios para atender aos produtores desde o início do ciclo de vida dos documentos, como os dos Estados Unidos, Reino Unido, Austrália, Nova Zelândia, Canadá, Portugal e Noruega (ROCHA, 2015, p. 190).

A Resolução n.º 43 teve como base várias normas, modelos e padrões nacionais e internacionais. Dentre eles destacam-se:

1) Norma ISO 16363: 2012, que é uma recomendação técnica a ser usada como base para fornecer auditoria e certificação da confiabilidade dos Repositórios Digitais, fornecendo uma especificação detalhada dos critérios pelos quais os Repositórios Digitais Confiáveis devem ser auditados.

2) Modelo OAIS (*Open Archival Information System – OAIS*) - norma ISO 14721:2012, que é a norma mais importante da área da Ciência da Informação, sendo um modelo conceitual desenvolvido pelo *Consultive Committee for Space Data Systems* (CCSDS). O Modelo OAIS descreve as funções de um repositório OAIS (plataforma de preservação) e os metadados necessários para a preservação e acesso dos materiais digitais gerenciados pelo repositório, que constituem um modelo funcional e um modelo de informação.

3) TRAC (*Trustworthy Repository Audit & Certification: Criteria and Checklist)*, que foi publicada em 2007, e apresenta um conjunto de critérios e um *checklist* a serem tomados como referência para a certificação de Repositórios Digitais Confiáveis (RDC).

4) Norma ISO 16919: 2014, que estabelece requisitos para entidades certificadoras de Repositórios Digitais Confiáveis.

A legislação arquivística brasileira em relação aos RDC-Arq também evoluiu com a orientação técnica n.º 3 do CONARQ (CONSELHO NACIONAL DE ARQUIVOS, 2015b), que apresenta cenários com algumas possibilidades de implantação de um RDC-Arq integrado a um SIGAD (CONSELHO NACIONAL DE ARQUIVOS, 2020a). O documento ressalta que o uso de um RDC-Arq juntamente com um SIGAD pode se dar nas três idades dos documentos e de maneiras distintas. Para isso, o documento apresenta três cenários possíveis para essa integração:

1) No ciclo de vida completo: neste cenário tem-se o uso de um RDC-Arq para as idades corrente e intermediária, e outro para a idade permanente. O RDC-Arq da idade permanente pode ser o de uma instituição arquivística, envolvendo mudança de custódia, ou o da própria instituição produtora.

2) Nas idades corrente e intermediária: neste cenário o RDC-Arq deve estar associado ao uso de um SIGAD, a fim de garantir o controle do ciclo de vida, o cumprimento da destinação prevista e a manutenção da autenticidade e da relação orgânica. Os documentos arquivísticos armazenados no RDC-Arq podem ser, por exemplo, documentos sensíveis, sigilosos ou de temporalidade maior do que cinco (05) anos, de acordo com a política arquivística adotada.

3) Na idade permanente: neste cenário os documentos digitais em idade permanente têm que ser mantidos e preservados por um RDC-Arq, de maneira a apoiar o tratamento técnico adequado, incluindo arranjo, descrição e acesso, para assegurar a manutenção da autenticidade e da relação orgânica desses documentos.

Sendo assim, em relação ao ambiente de preservação (RDC-Arq), que é o Arquivo Permanente Digital, além do modelo de requisitos (funcionais, não funcionais e regras de negócio) de uma plataforma de preservação, que são definidos pela ISO 14721:2012 (Modelo OAIS), a Resolução n.º 43 incorpora requisitos de auditoria e certificação, por se basear na norma internacional ISO 16363:2012, que é a norma para auditoria e certificação de Repositório Digitais Confiáveis (RDC). No entanto, é importante destacar que o modelo de requisitos de auditoria e certificação contemplado pela Resolução n.º 43 segue uma norma internacional, e que embora os requisitos estejam nela citados, no Brasil ainda não existe um modelo de execução que apoie as instituições arquivísticas, de maneira efetiva, no processo de auditoria e certificação de um RDC-Arq, e nem em um processo em níveis que permita que as instituições arquivísticas se adequem à resolução de maneira gradual.

Em relação ao processo de auditoria de um RDC-Arq, Santos (2018, p. 12) corrobora quando diz que:

> O processo de auditoria torna-se essencial para demonstrar que um RDC-Arq está em conformidade com o modelo OAIS e que segue princípios arquivísticos. A realização de auditorias periódicas aliadas a uma certificação irá demonstrar que o RDC-

> Arq é confiável.

Neste sentido, o Conarq criou uma câmara técnica consultiva[6] com o objetivo de elaborar requisitos de certificação e regras de auditoria para os RDC-Arq. Os objetivos da câmara técnica são:

- Elaborar uma lista de critérios e requisitos a serem cumpridos por um RDC-Arq, para que ele seja considerado aderente às resoluções do Conarq;

- Definir a metodologia para o diagnóstico, a auditoria e a autocertificação de RDC-Arq, baseada nas normas ISO 16363:2012 e 16.919:2014 e nas resoluções do Conarq;

- Definir a metodologia para aferição da maturidade em preservação digital; e

- Definir a metodologia para monitoramento de RDC-Arq.

Assim, espera-se que trabalhos como a da câmara técnica do Conarq evoluam e culminem no desenvolvimento de um modelo de execução que apoie as instituições arquivísticas nesse importante processo de auditoria e certificação de um RDC-Arq, e que também se evolua para a certificação de entidades certificadoras de um RDC-Arq no Brasil.

A certificação de entidades certificadoras é importante porque, embora um RDC-Arq possa e deva se autoavaliar, a certificação deve ser feita por uma entidade externa. A certificação de terceiros é recomendada pela TRAC (*Trustworthy Repositories Audit & Certification: Criteria and Checklist*). O requisito A3.9 da TRAC (CRL/OCLC, 2007, p. 15, tradução nossa, grifo nosso) apresenta que:

> A3.9 O repositório se compromete com um cronograma regular de autoavaliação e certificação e, se certificado, compromete-se a notificar as entidades de certificação sobre mudanças operacionais que irão alterar ou anular seu status de certificação. **Um repositório não pode se autocertificar** porque uma medição externa e objetiva, usando um processo de certificação consistente e repetível é necessária para garantir e demonstrar que o repositório atende e provavelmente continuará a atender aos requisitos de preservação. Portanto, a certificação é o melhor indicador de que o repositório atende aos seus requisitos, cumpre sua função e adere aos padrões apropriados. O

[6] https://www.gov.br/arquivonacional/pt-br/canais_atendimento/imprensa/copy_of_noticias/conarq- aprova-criacao-de-camara-tecnica-para-estabelecer-criterios-de-certificacao-para-rdc-arq

> repositório deve demonstrar que integra a preparação e a resposta à certificação em suas operações e planejamento.

Assim, a certificação externa é uma forma de garantir transparência nos processos e aumentar a credibilidade perante a comunidade de interesse. Isso é importante visto que a sustentabilidade financeira de um RDC-Arq, por exemplo, necessita continuamente de parcerias e financiamentos. Assim, a certificação por terceiros trará mais credibilidade para os possíveis parceiros e investidores.

Além disso, haja vista que muitas instituições, no cenário atual, não têm condições de desenvolver suas próprias soluções para os ambientes de gestão de documentos, preservação e acesso e difusão, a definição de requisitos (funcionais, não funcionais, regras de negócio) irá apoiar as instituições, não somente no desenvolvimento de suas próprias soluções, como também na contratação de serviços, oferecidos geralmente por empresas do setor privado, observando um conjunto mínimo de requisitos necessários para cada uma das soluções apresentadas. Já os modelos de auditoria e certificação tem sua importância ao apresentar metodologias que possam: apoiar as instituições no processo de autoavaliação e adequação aos modelos propostos; avaliar as soluções desenvolvidas ou contratadas com base nos padrões, modelos, normas e resoluções adotados; como também fornecer ferramentas suficientes e adequadas para certificar a qualidade de cada uma dessas soluções.

3.4 Auditoria e Certificação no Ambiente de Acesso e Difusão

O ambiente de acesso e difusão é o terceiro ambiente envolvido no ciclo de vida dos documentos arquivísticos, e diz respeito à terceira entidade externa do Modelo OAIS: o consumidor (Figura 1). O consumidor é o papel desempenhado por usuários ou sistemas que interagem com o ambiente de preservação para acessar, por meio de consultas e pedidos, a informação preservada desejada. Diferentemente dos ambientes de gestão de documentos e de preservação, o ambiente de acesso e difusão não possui, até o momento, normativas na legislação arquivística brasileira que apresentem qual é o modelo

de requisitos que esses ambientes devem atender e, consequentemente, não possuem requisitos de auditoria e certificação. No entanto, há no cenário nacional e internacional diferentes padrões e normas que apresentam requisitos arquivísticos que podem ser um ponto inicial para a especificação desse modelo de requisitos. Como exemplo tem-se a ISAD(G), que é a norma geral internacional de descrição arquivística, e a NOBRADE, que é a norma brasileira de descrição arquivística.

Ou seja, as instituições arquivísticas deveriam utilizar sistemas de acesso e difusão desenvolvidos com base em um modelo de requisitos amplamente discutido pela comunidade de interesse, a exemplo do que tem acontecido com os ambientes de gestão de documentos e de preservação. Sendo assim, não se deveria dar acesso aos documentos arquivísticos por meio de *websites*, por exemplo, construídos sem requisitos arquivísticos, ou por meio de mídias externas, discos rígidos ou bancos de dados, sem contemplar uma cadeia de preservação e uma cadeia de custódia digital arquivística, mas sim em Plataformas Arquivísticas de Descrição, Acesso, Difusão e Transparência Ativa de Informações e Documentos. Uma vez definidos esses requisitos, uma segunda etapa, não menos importante, é a definição de um modelo de requisitos de auditoria e certificação, com o objetivo de medir a confiabilidade do ambiente e o atendimento ao modelo adotado.

Nesse contexto, sem a pretensão de esgotar o assunto, a seguir apresentam-se alguns requisitos arquivísticos considerados importantes na especificação de um modelo de requisitos para um ambiente de acesso e difusão. São eles:

1) Navegação Multinível: o ambiente de acesso e difusão deve ser um ambiente que permita apresentar os documentos arquivísticos de forma organizada, dentro de níveis hierárquicos (fundos, séries, dossiês/processos, itens documentais). Para isso deve adotar normas de descrição arquivística como a ISAD-G (*General International Standard Archival Description*) e a NOBRADE (Norma Brasileira de Descrição Arquivística).

2) Geração automática de instrumentos de pesquisa: o ambiente de acesso e difusão deve permitir a geração automática de instrumentos de

pesquisa, que também devem ser atualizados de forma automática todas as vezes que o ambiente receber novos documentos de uma descrição arquivística.

3) Manter a relação orgânica: relação orgânica são relações que um documento mantém com os demais documentos arquivísticos do órgão ou entidade e que trazem o contexto no qual o documento foi produzido. Sendo assim, para que o documento não perca o seu contexto, é importante que essas relações sejam mantidas. Assim, o ambiente de acesso e difusão deve ser desenvolvido de forma que preserve e apresente os documentos arquivísticos mantendo sua relação orgânica.

4) Importação/exportação amigável e em formatos padronizados: o ambiente de acesso e difusão deve permitir a importação e exportação de dados (documentos arquivísticos digitais e seus metadados) por meio de uma interface amigável, em formatos padronizados, preferencialmente formatos abertos, amplamente usados pela comunidade de interesse. Para permitir a interoperabilidade entre ambientes, é importante que esses formatos atendam a padrões internacionais amplamente aceitos.

5) Suporte a padrões de metadados e normas arquivísticas: O ambiente de acesso deve dar suporte a padrões de metadados e normas de descrição arquivística amplamente aceitos tais como: ISAD(G) - Norma geral internacional de descrição arquivística; NOBRADE - Norma Brasileira de Descrição Arquivística; ISAAR(CPF) - Norma Internacional de Registro de Autoridade Arquivística para entidades coletivas, pessoas e famílias; ISDIAH - Norma internacional para descrição de instituições com acervo arquivístico; ISDF - Norma Internacional para Descrição de Funções; PREMIS - *PREservation Metadata*: Implementation Strategies; RAD - *Rules for Archival Description* etc. Também é importante que o ambiente dê suporte a taxonomias, e seja compatível com outros padrões de metadados, mesmo que não arquivísticos, mas que sirvam para permitir a interoperabilidade entre os ambientes, tais como os padrões Dublin Core - Esquema de metadados para descrever objetos digitais; MODS - *Metadata Object Description Schema;* MADS - *Metadata Authority Description Schema;* MARC - *MAchine Readable Cataloging* etc.;

6) Acessibilidade: o ambiente de acesso e difusão deve adotar modelos de acessibilidade, com o objetivo de promover a inclusão de pessoas com necessidades especiais, promovendo sua autonomia e independência. Esse é o caso do eMAG[7], que é o Modelo de Acessibilidade em Governo Eletrônico, que tem o compromisso de ser o norteador no desenvolvimento e a adaptação de conteúdos digitais do governo federal, garantindo o acesso a todos. Seguir as recomendações de um modelo de acessibilidade permite que a implementação da acessibilidade digital seja conduzida de forma padronizada.

7) Multilíngue: para aumentar a visibilidade dos documentos digitais acessados pelo consumidor da informação em um ambiente de acesso e difusão, as interfaces do usuário, elementos e conteúdo das bases de dados devem poder ser traduzidos para diferentes idiomas. Assim, é importante oferecer ao usuário a possibilidade de exibição de uma interface multilíngue, assim como fornecer ferramentas de tradução das descrições arquivísticas em diferentes idiomas;

8) Multirepositório: o ambiente de acesso e difusão deve ser construído para ser usado por uma única instituição ou por várias instituições arquivísticas. Uma vez que o ambiente de acesso e difusão possa atender várias instituições, é importante que esse ambiente seja interoperável com qualquer repositório OAIS.

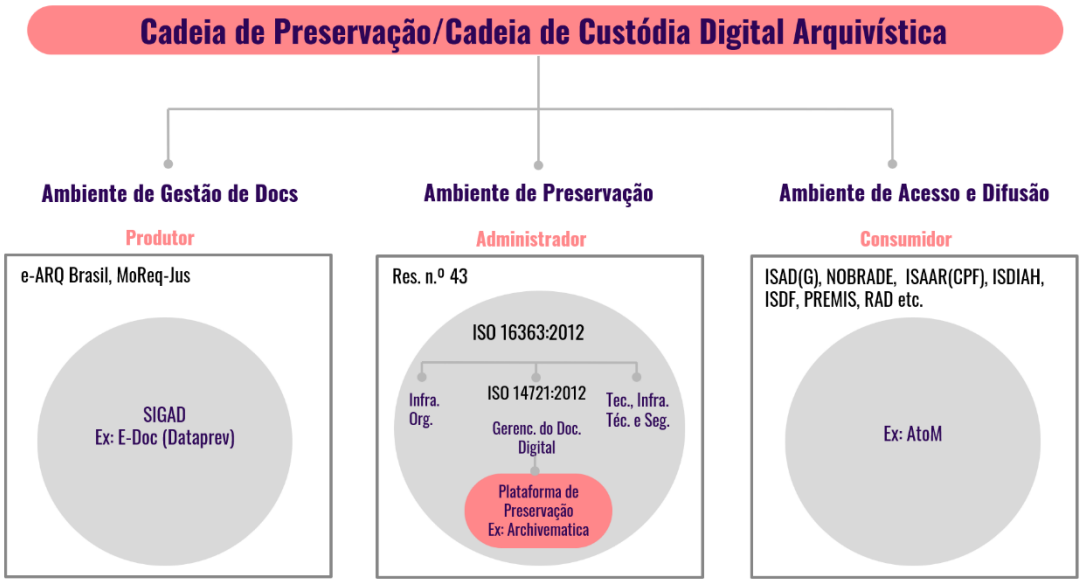
9) Permitir repopulação do ambiente: em caso de algum problema, como por exemplo uma invasão maliciosa, que faça com que o ambiente de acesso e difusão tenha perda de dados, parcial ou total, é importante que esse ambiente permita a sua repopulação imediata. Ou seja, que todos os documentos arquivísticos e metadados (objetos digitais e metadados) sejam recuperados da mesma forma em que foram apresentados pela última vez. Para isso deve ser possível uma nova importação dos dados da plataforma de preservação para o ambiente de acesso e difusão.

Vale ressaltar que só será possível pensar em um modelo de requisitos de auditoria e certificação para o ambiente de acesso e difusão, após ser definido

[7] http://emag.governoeletronico.gov.br/

um modelo de requisitos (funcionais, não funcionais, regras de negócio, além de requisitos arquivísticos). A Figura 2 apresenta um resumo dos principais elementos discutidos nesta seção.

Figura 2 – Cadeia de preservação e CCDA nos três ambientes do ciclo de vida dos documentos.



Fonte: Elaborada pelos autores

A Figura 2 apresenta os três ambientes envolvidos nas três entidades externas do Modelo OAIS, apresentando a necessidade de uma cadeia de preservação e de uma cadeia de custódia digital arquivística em todo o ciclo de vida dos documentos. Observando a Figura 2 vê-se que para o Ambiente de Gestão de Documentos há o e-ARQ, que é o modelo mais destacado no Brasil com requisitos funcionais, requisitos não funcionais e regras de negócio para os SIGAD, além do MoReq-Jus. No entanto, não existe um modelo de requisitos de auditoria e certificação para esse ambiente. Em relação ao ambiente de preservação, a Resolução n.º 43 do Conarq contempla dois modelos internacionais: a ISO 14721 e a ISO 16363. A ISO 14721 (Modelo OAIS) apresenta os critérios que uma plataforma de preservação deve contemplar. Como exemplo de uma plataforma de preservação tem-se o Archivematica[8]. A

[8] https://www.archivematica.org/pt-br/

ISO 16363 lista os critérios que um RDC deve atender, como também apresenta requisitos de auditoria e certificação para a verificação da confiabilidade do RDC. Já o ambiente de acesso e difusão não apresenta, até o momento, nenhum modelo de requisitos. No entanto, existem diferentes normas e padrões de descrição arquivística que apresentam vários requisitos arquivísticos que esses ambientes deveriam adotar. Também existem exemplos de *softwares* de descrição arquivística*,* como é o caso do *software* livre AtoM[9].

4 CONSIDERAÇÕES FINAIS

A transformação digital ocorrida nas últimas décadas desafiou as organizações a pensarem na preservação do patrimônio arquivístico digital, que é constituído dos documentos produzidos no curso de suas atividades. Isso desafiou as organizações a pensarem na preservação digital, o que culminou no desenvolvimento de diversas normas, modelos e padrões. No Brasil, desde a publicação da carta de preservação digital em 2005, o Conarq iniciou uma série de publicações sobre o tema. No entanto, a evolução dessas normativas aconteceu principalmente em direção ao ambiente de preservação dos documentos, com modelos conceituais que abrangem tanto seus requisitos funcionais, não funcionais e regras de negócio, quanto requisitos de auditoria e certificação. O mesmo não aconteceu com os ambientes de gestão de documentos e de acesso e difusão, principalmente em relação aos requisitos de auditoria e certificação.

Nesse sentido, o artigo teve como objetivo discutir sobre a importância do processo de auditoria e certificação, chamando a atenção para que esse processo ocorra em toda a cadeia de custódia digital arquivística, ou seja, em todos os ambientes envolvidos nas três entidades externas do Modelo OAIS, e não somente no ambiente de preservação. Somente definindo requisitos para os ambientes envolvidos, que são o ambiente de gestão de documentos, o ambiente de preservação e o ambiente de acesso e difusão, e estabelecendo requisitos de auditoria e certificação para cada um desses ambiente, será

[9] https://www.accesstomemory.org/pt-br/

possível manter uma cadeia de custódia digital arquivística, ou seja, uma cadeia de custódia segura e ininterrupta, que mantêm os documentos arquivísticos digitais autênticos e confiáveis ao longo do tempo.

Identificou-se que, no cenário brasileiro, há modelos de requisitos para o ambiente de gestão dos documentos, por meio, por exemplo, do e-ARQ Brasil e do MoReq-Jus, mas que o mesmo não acontece para os requisitos de auditoria e certificação. O ambiente de preservação é o mais completo, pois a Resolução n.º 43 do Conarq apresenta tanto requisitos funcionais, não funcionais e regras de negócio, quanto requisitos de auditoria e certificação. Já para o ambiente de acesso e difusão dos documentos, não há ainda um modelo de requisitos, apenas padrões e normas de descrição arquivística que podem servir como ponto inicial para sua especificação. Somente depois de se ter um modelo de requisitos definido será possível a especificação de um modelo de requisitos de auditoria e certificação.

Concluindo, verificou-se que a certificação externa é uma forma de garantir transparência nos processos e aumentar a credibilidade perante a comunidade de interesse. Uma vez que muitas instituições não têm condições de desenvolver suas próprias soluções para os ambientes de gestão de documentos, preservação e acesso e difusão, os modelos de requisitos irão apoiar as instituições, não somente no desenvolvimento de suas próprias soluções, como também na contratação de serviços. Além disso, modelos de auditoria e certificação são importantes ao apresentar metodologias que possam apoiar as instituições arquivísticas no processo de autoavaliação e adequação aos modelos propostos, na avaliação de soluções desenvolvidas ou contratadas, como também no fornecimento de ferramentas suficientes e adequadas para certificar a qualidade das soluções apresentadas.

REFERÊNCIAS

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

CENTER FOR RESEARCH LIBRARIES/ONLINE COMPUTER LIBRARY CENTER. **Trustworthy Repositories Audit & Certification:** Criteria and Checklist*.* Illinois/Ohio: CRL/OCLC, feb. 2007. v. 1. Disponível em: https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf. Acesso em: 24 jun. 2021.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Carta para preservação do patrimônio arquivístico digital**. Rio de Janeiro: Arquivo Nacional, 2005. Disponível em: http://conarq.arquivonacional.gov.br/images/publicacoes_textos/Carta_preservacao.pdf. Acesso em: 14 ago. 2019.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq.** Rio de Janeiro: Arquivo Nacional, 2015a. 31 p. Disponível em: http://conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf Acesso em: 04 nov. 2019.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais.** Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_presuncao_autenticidade_completa.pdf. Acesso em: 21 jun. 2021.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Glossário:** Documentos Arquivísticos Digitais. Versão 8.0. Rio de Janeiro: Arquivo Nacional, 2020a. 54 p. Disponível em:http://http://antigo.conarq.gov.br/images/ctde/Glossario/glosctde_2020_08_07.pdf. Acesso em: 21 jun. 2021.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil**. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: http://conarq.arquivonacional.gov.br/images/publicacoes_textos/earqbrasil_model_requisitos_2009.pdf. Acesso em: 10 jun. 2021.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil.** Rio de Janeiro: Arquivo Nacional, 2020b. v. 2. 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: 24 mar. 2021.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Orientação Técnica nº 3:** Cenários de uso de RDC-Arq em conjunto com o SIGAD. Rio de Janeiro: Arquivo Nacional, 2015b. Disponível em: http://conarq.arquivonacional.gov.br/images/ctde/Orientacoes/Orientacao_tecnica_rdcarq_2015_v8_pub.pdf. Acesso em: 04 jun. 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário.** Brasília: Conselho Nacional de Justiça, 2009. Disponível em: https://www.cnj.jus.br/programas-e-acoes/gestao-documental-e-memoria-proname/gestao-documental/moreq-jus-e-sistemas-informatizados/. Acesso em: 23 jun. 2021.

FERREIRA, M. **Introdução à preservação digital:** Conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. 88 p. Disponível em: http://eprints.rclis.org/8524/1/livro.pdf. Acesso em: 05 maio 2021.

GAVA, T. B. S.; FLORES, D. Repositórios arquivísticos digitais confiáveis (RDC-Arq) como plataforma de preservação digital em um ambiente de gestão arquivística. **Informação & Informação**, Londrina, v. 25, n. 2, p. 74-99, jul. 2020. ISSN 1981-8920. Disponível em: http://www.uel.br/revistas/uel/index.php/informacao/article/view/38411. Acesso em: 13 out. 2020. DOI: http://dx.doi.org/10.5433/1981-8920.2020v25n2p74.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo: Atlas, 2002. p. 1-175.

GLADNEY, H. Long-Term Preservation of Digital Records: Trustworthy Digital Objects. **The American Archivist**. v. 72, n. 2, p. 401-435. 2009. Disponível em: https://americanarchivist.org/doi/pdf/10.17723/aarc.72.2.g513766100731832. Acesso em: 01 jun. 2021.

HIRTLE, P. B. Archival authenticity in a digital age. **Páginas A&B, Arquivos e Bibliotecas (Portugal)**, n. 6, p. 73-90, 2001. Disponível em: https://ojs.letras.up.pt/index.php/paginasaeb/article/view/136/128. Acesso em: 29 jun. 2021.

INTERNATIONAL COUNCIL ON ARCHIVES. **Multilingual Archival Terminology.** 2012. Disponível em: https://www.ica.org. Acesso em: 14 jun. 2021.

INTERPARES 2 PROJECT. **Diretrizes do Produtor.** A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. Tradução Arquivo Nacional e Câmara dos Deputados. TEAM Brasil, 2010a. Disponível em: http://www.interpares.org/ip3/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf. Acesso em: 26 jun.

INTERPARES 2 PROJECT. **Diretrizes do Preservador.** A preservação de documentos arquivísticos digitais: diretrizes para organizações. Tradução Arquivo Nacional e Câmara dos Deputados. TEAM Brasil, 2010b. Disponível em: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf. Acesso em: 26 jun.

SANTOS, H. M.; FLORES, D. As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital. **Biblios - Revista de Bibliotecología y Ciencias de la Información**, Tacna, n. 59, p. 45-54, 2015a. Disponível em: http://biblios.pitt.edu/ojs/index.php/biblios/article/view/215. Acesso em: 26 jun. 2019.

SANTOS, H. M.; FLORES, D. Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo. **Perspectivas em Ciência da Informação** [online], v. 20, n. 2, p. 198-218, jun. 2015b. ISSN 1981-5344. Disponível em: https://doi.org/10.1590/1981-5344/2341. Acesso em: 26 jun. 2021. DOI: https://doi.org/10.1590/1981-5344/2341.

ROCHA, C. L. Repositórios para a preservação de documentos arquivísticos digitais. **Acervo - Revista do Arquivo Nacional**, Rio de Janeiro, v. 28, n. 2, p. 180-191, 2015. Disponível em: http://hdl.handle.net/20.500.11959/brapci/40764. Acesso em: 04 nov. 2019.

SANTOS, H. M. **Manual para auditoria de Repositórios Arquivísticos Digitais Confiáveis.** 2018. Disponível em: https://www.academia.edu/37334881/MANUAL_PARA_AUDITORIA_DE_REPOSITORIOS_ARQUIVISTICOS_DIGITAIS_CONFIAVEIS. Acesso em: 26 jun. 2021.

AUDIT AND CERTIFICATION THROUGHOUT THE ARCHIVAL DIGITAL CHAIN OF CUSTODY

ABSTRACT

Objective: Discuss about audit and certification throughout the entire archival digital custody chain, covering all environments involved in the three external entities of the OAIS Model, analyzing the Brazilian scenario. Discuss the importance of the audit and certification process in all environments involved in the three external entities of the OAIS Model, analyzing the Brazilian scenario. **Methodology**: Exploratory, bibliographical and documentary research, having as main documentary and bibliographic sources the documentation produced by different organizations, in the norms of the National Council of Archives and in scientific articles by national and international researchers. **Results**: Discussion about the conceptual models of requirements and audit and certification, in the Brazilian scenario, for the three environments involved in the OAIS Model: the producer environment, which is the document management environment; the administrator's environment, which is the environment for preserving documents; the consumer environment, which is the environment for accessing and disseminating documents. **Conclusions**: In the Brazilian scenario, there are models of requirements for the document management environment, but it does not establish audit and certification requirements; the preservation environment presents both functional and non-functional requirements and business rules, as well as audit and certification requirements; the environment for accessing and disseminating documents does not yet have established guidelines.

Descriptors: Audit and Certification. Digital Archival Chain of Custody. Document Management Environment. Preservation Environment. Access and Dissemination Environment.

AUDITORÍA Y CERTIFICACIÓN EN LA CADENA DIGITAL ARCHIVISTA DE CUSTODIA

RESUMEN
Objetivo: Discutir sobre auditoría y certificación a lo largo de toda la cadena de custodia digital de archivos, cubriendo todos los entornos involucrados en las tres entidades externas del Modelo OAIS, analizando el escenario brasileño. **Metodología**: Investigación exploratoria, bibliográfica y documental, teniendo como principales fuentes documentales y bibliográficas la documentación producida por diferentes organismos, en las normas del Consejo Nacional de Archivos y en artículos científicos de investigadores nacionales e internacionales. **Resultados:** Discusión sobre los modelos conceptuales de requisitos y auditoría y certificación, en el escenario brasileño, para los tres entornos involucrados en el Modelo OAIS: el entorno productor, que es el entorno de gestión documental; el entorno del administrador, que es el entorno para la conservación de documentos; el entorno del consumidor, que es el entorno para acceder y difundir documentos. **Conclusiones:** En el escenario brasileño, existen modelos de requisitos para el entorno de gestión documental, pero no establece requisitos de auditoría y certificación; el entorno de preservación presenta requisitos y reglas comerciales tanto funcionales como no funcionales, así como requisitos de auditoría y certificación; el entorno de acceso y difusión de documentos aún no cuenta con pautas establecidas.

Descriptores: Auditoría y Certificación. Cadena de custodia de archivos digitales. Entorno de gestión de documentos. Entorno de conservación. Entorno de acceso y difusión.

Recebido em: 09.09.2021
Aceito em: 09.12.2021