

CADEIA DE CUSTÓDIA PARA DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

CHAIN OF CUSTODY FOR DIGITAL RECORDS

DANIEL FLORES | Doutor em Documentação pela Universidade de Salamanca, Espanha.

BRENDA COUTO DE BRITO ROCCO | Doutoranda do Programa de Pós-Graduação em Ciência da Informação Ibict/UFRJ

HENRIQUE MACHADO DOS SANTOS | Mestrando em Patrimônio Cultural pela Universidade Federal de Santa Maria (USFM)

RESUMO

Este estudo resgata a abordagem da cadeia de custódia para documentos arquivísticos analógicos e propõe sua reformulação com o objetivo de contemplar documentos arquivísticos armazenados em ambientes digitais. Para isso, discute-se a importância da manutenção de uma linha de custódia ininterrupta na implementação de sistemas informatizados para gestão, preservação e acesso aos documentos arquivísticos.

Palavras-chave: custódia confiável; documentos arquivísticos digitais; Sigad; RDC-Arq.

ABSTRACT

This study rescues the approach of chain custody to analogic records and proposes a reformulation in order to contemplate records stored in digital environments. For this, we discuss the importance of maintaining an unbroken custody line in the implementation of computerized systems for management, preservation and access to records.

Keywords: reliable custody; digital records; Sigad; RDC-Arq.

RESUMEN

Este estudio rescata el enfoque de la cadena de custodia para documentos de archivo analógicos y propone una formulación, a fin de contemplar documentos de archivo almacenados en entornos digitales. Para ello, se discute la importancia de mantener una línea ininterrumpida de custodia en la implementación de sistemas informáticos de gestión, preservación y acceso para los documentos de archivo.

Palabras clave: custodia fiable; documentos de archivo digitales; Sigad; RDC-Arq.

INTRODUÇÃO

As denominadas tecnologias da informação e comunicação (TICs) introduziram diferentes formas de produção, tramitação e armazenamento de informação, trazendo consigo o que Dollar (1994) denominou como imperativos tecnológicos, os quais impõem novos desafios à sociedade contemporânea. Entre esses desafios, observa-se a questão da acurácia e da autenticidade dos documentos em meio digital. Embora os mecanismos de registro tenham evoluído em nível de hardware, software e suporte, ainda há incertezas quanto à integridade e à identidade dos documentos que são produzidos e armazenados em meio digital, acarretando a necessidade de um referencial de uma linha ininterrupta digital entre todos os ambientes interoperáveis dos documentos arquivísticos, desde a gênese até sua preservação e acesso.

A produção e o registro de informações exclusivamente em documentos digitais aumentaram consideravelmente, apresentando novos e grandes desafios para diversas áreas do conhecimento no que se refere ao tratamento desses documentos. Dentre essas áreas, encontra-se a arquivística, que tem se preocupado com o documento arquivístico, incluindo os digitais.

No entanto, os mecanismos para manutenção e presunção da autenticidade não têm acompanhado o ritmo dessa evolução. Este contraponto realça as vulnerabilidades dos documentos arquivísticos digitais, que podem ser facilmente adulterados sem deixar vestígios aparentes, evidenciando a complexidade e a especificidade destes registros. Tais aspectos irão impactar diretamente na credibilidade de tais documentos enquanto provas de uma ação, fontes de pesquisa e bases de conhecimento.

A complexidade dos documentos arquivísticos digitais, segundo Flores (2016, p. 5), ocorre desde “o seu sistema de gestão, o Sigad, que trata da captura, armazenamento, indexação e recuperação de todos os componentes digitais do documento arquivístico como uma unidade complexa, até os sistemas de preservação e acesso”, sendo ainda ressaltado que “um documento arquivístico digital pode ser constituído por vários componentes digitais, como, por exemplo, um relatório acompanhado de planilhas, fotografias ou plantas, armazenados em diversos arquivos digitais. Além disso, há de se considerar a relação orgânica dos documentos arquivísticos”.

Já no tocante à especificidade, o documento digital apresenta características que podem comprometer sua autenticidade, uma vez que é suscetível à degradação física dos seus suportes, à obsolescência tecnológica de hardware, software e de formatos, e a intervenções não autorizadas, que podem ocasionar adulteração e destruição. Somente com procedimentos de gestão arquivística, é possível assegurar a autenticidade dos documentos arquivísticos digitais.

Para que um documento arquivístico seja considerado íntegro, é necessário que seja inalterado e completo. Tal integridade relaciona-se diretamente aos ambientes de produção e preservação do documento, ou seja, aos seus ambientes custodiadores, denotando, assim, que, quando falamos de documentos digitais, de ambientes digitais, estamos também falando de ambientes custodiadores, de uma linha ininterrupta digital.

Dessa forma, faz-se necessária uma reflexão sobre a custódia confiável e ininterrupta para documentos arquivísticos digitais, enfatizando aspectos como a relação entre os sistemas de gestão documental e preservação em longo prazo, com garantia de acesso. Para isso, realiza-se um levantamento bibliográfico de materiais previamente publicados, que partem de uma revisão, incorporando, basicamente, referenciais das áreas da arquivologia e da ciência da informação (Gil, 2010; Luna, 1997).

Escrito com o propósito de discutir o quanto é relevante a manutenção de uma linha de custódia que seja confiável e ininterrupta, este artigo divide-se em quatro seções. Na primeira, contextualiza-se a cadeia de custódia documental. Na seção seguinte, são discutidas questões como a gestão de documentos digitais. Na terceira seção, trata-se da preservação em repositórios e sua conformidade com o modelo *Open Archival Information System* (Oais). Por fim, na última seção, esquematizam-se os aspectos a serem considerados em uma cadeia de custódia confiável para documentos arquivísticos armazenados em ambiente digital.

CADEIA DE CUSTÓDIA DOCUMENTAL: BREVE CONTEXTUALIZAÇÃO

A cadeia de custódia documental pode ser entendida como o ambiente no qual perpassa o ciclo de vida dos documentos. Em outras palavras, ela define quem é o responsável por aplicar os princípios e as funções arquivísticas à documentação.

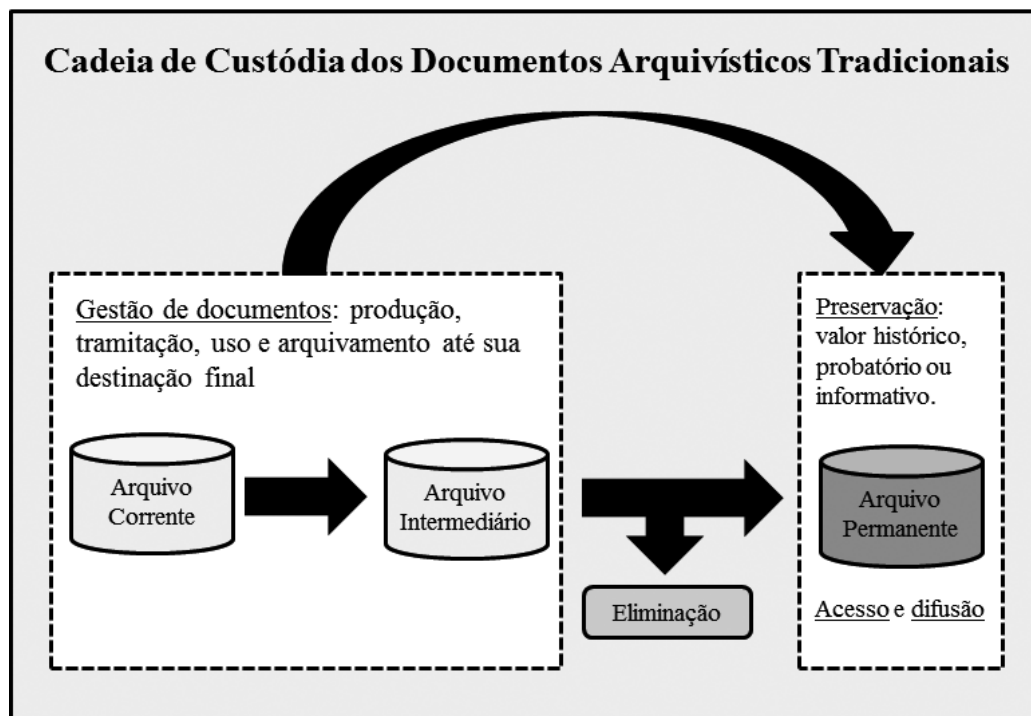
A custódia confiável de documentos arquivísticos tradicionais é mantida através de uma linha ininterrupta, a qual compreende as três idades do arquivo: fases corrente, intermediária e permanente. Dessa forma, a confiabilidade ocorre por intermédio da própria instituição, que faz a própria produção, gestão, preservação e provê acesso aos seus documentos.

A figura 1 esquematiza a abordagem de Jenkinson (1922) e apresenta uma adaptação atual. Observa-se que no âmbito mais amplo está a instituição arquivística, a qual compreende o ciclo de vida dos documentos na ótica da teoria das três idades, comportando, logicamente, as funções arquivísticas.

Nesse esquema, a gestão e a preservação estão unidas pela função de avaliação de documentos, que será a responsável por otimizar a administração. Assim, os documentos que não possuem mais valor primário são avaliados e, por consequência, recolhem-se os documentos de valor secundário e eliminam-se os demais. Ressalta-se que todo esse processo vem a ser executado por uma instituição arquivística que mantém uma linha de custódia ininterrupta e, assim, garante a confiabilidade dos materiais custodiados.

A abordagem clássica da cadeia de custódia, na arquivística, então preconizada por Jenkinson (1922), pode ser considerada suficiente para a preservação de documentos em suportes tradicionais. Todavia, considerando a questão da interoperabilidade dos documentos arquivísticos em ambientes digitais, é necessário ir além dessa abordagem. Quando Jenkinson (1922) aborda a cadeia de custódia, ele está se referindo à autenticidade dos documentos arquivísticos a partir da não interrupção desta cadeia, dos arquivos como um todo e não somente de um documento individualmente, do produtor até o preservador, no caso a instituição arquivística, o Arquivo Nacional, por exemplo.

FIGURA 1. CADEIA DE CUSTÓDIA DOS DOCUMENTOS ARQUIVÍSTICOS TRADICIONAIS



Fonte: elaborado pelos autores com base em Jenkinson, 1922

No caso desses documentos, os que forem considerados de guarda permanente, após o fim das fases corrente e intermediária, necessitam ser exportados para um ambiente confiável e idôneo. Além disso, é preciso manter a cadeia de custódia ininterrupta, mesmo que haja mudança de custodiadores. Nesse ponto, observa-se que essas possíveis mudanças não devem representar uma ruptura, pois os documentos de caráter permanente seriam apenas transferidos para outro custodiador, o qual terá a responsabilidade legal de preservar a documentação.

Tanto a gestão quanto a preservação de documentos devem ser realizadas por meio de sistemas que considerem a manutenção de requisitos arquivísticos, para que seja possível verificar sua presunção de autenticidade. Outro aspecto a ser destacado é a necessidade de que o recolhimento dos documentos de valor secundário seja realizado por instituições arquivísticas. Paralelamente, há a necessidade de um acompanhamento que garanta a manutenção de uma linha ininterrupta entre as três idades documentais e considere a possível mudança da custódia documental.

GESTÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

O advento e a proliferação da produção, tramitação e armazenamento de documentos digitais suscitaram a premência de sistemas que fizessem a gestão de tais documentos, o que culminou nos programas de gerenciamento eletrônico de documentos (doravante GED). Tais sistemas não têm em si a perspectiva arquivística. Logo, não visam gerenciar o ciclo de vida dos documentos, sua temporalidade, destinação e relação orgânica. Por outro lado, os documentos arquivísticos em ambiente digitais requerem os mesmos tratamentos e procedimentos que os documentos não digitais e, portanto, o sistema responsável por seu tratamento deve ter como principal foco a gestão arquivística.

A prática da gestão eletrônica de documentos denota a ausência de procedimentos arquivísticos, o que é justificado pela não conformidade do GED com o e-ARQ Brasil:¹ modelo de requisitos para sistemas informatizados de gestão arquivística de documentos.² Instrumento do Conselho Nacional de Arquivos (Conarq), esse modelo consiste em uma especificação de requisitos para organizações, sistemas e para os próprios documentos que são custodiados. O referido modelo tem por finalidade garantir que a gestão arquivística ocorra nos sistemas, garantindo, portanto, o acesso pelo tempo que se fizer necessário, bem como a confiabilidade e autenticidade desses documentos. Sem esses devidos requisitos, não é possível considerar que um sistema faça a gestão arquivística dos documentos, pois coloca em dúvida as características e a própria razão de ser deles.

O conjunto de requisitos propostos no e-ARQ Brasil³ fornece a base para a implementação de um sistema informatizado de gestão arquivística de documentos (doravante Sigad), comportando, assim, os requisitos para desenvolver um ambiente confiável para a gestão de documentos arquivísticos. Dessa forma, as fases corrente e intermediária serão contempladas pelo Sigad e, após o cumprimento dos prazos estabelecidos, este deverá exportar os documentos de valor permanente para um repositório arquivístico digital confiável (RDC-Arq).

Observa-se que o recolhimento desses documentos deverá ser realizado por meio de uma custódia confiável, a qual disponha de mecanismos que garantam a autenticidade (identidade + integridade) na transferência de documentos do Sigad para o repositório. Nesse sentido, o repositório digital deverá ser concebido como o ambiente autêntico para a

-
- 1 O e-ARQ Brasil foi inspirado em outros modelos de requisitos. A saber: *Design criteria standard for electronic records management software applications: DOD 5015.2-STD, 2002*; MoReq – modelo de requisitos para a gestão de arquivos eletrônicos, 2002; *Requirements for electronic records management systems: functional requirements*, United Kingdom, 2002.
 - 2 O modelo de requisitos para sistemas informatizados de gestão arquivística de documentos – e-ARQ Brasil tem sua adoção recomendada pelas resoluções n. 25, de 27 de abril de 2007 e n. 32, de 17 de maio de 2010, do Conselho Nacional de Arquivos. Ele especifica todas as atividades e operações técnicas da gestão arquivística de documentos, desde a produção, tramitação, utilização e arquivamento até a sua destinação final, aplicadas em um ambiente digital.
 - 3 Cabe ressaltar que no Brasil existe outro modelo de requisitos para sistemas informatizados de gestão arquivística de documentos, que é implementado no âmbito do Judiciário, denominado MOREQ JUS. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/modelo_de_requisitos.pdf>. Acesso em: 1 mar. 2016.

preservação de documentos digitais em longo prazo e, por isso, é fundamental manter bons níveis de interoperabilidade com o Sigad.

A interoperabilidade entre o Sigad e o RDC-Arq deve ser feita de forma automatizada, de modo que não existam manipulações não autorizadas, e não se permitam inserções ou importações de documentos ou de pacotes de documentos que não estejam contemplados pela cadeia de custódia digital, que documenta todas as atividades, rotinas, recepções, conversões, normalizações etc., em metadados que ficam encapsulados nos pacotes de interoperabilidade de documentos. É importante destacar que esta interoperabilidade consiste basicamente em um empacotamento de acordo com os padrões da área e da adoção dos metadados, também de acordo com os padrões da área.

OS REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS (RDC-ARQ)

Após o término do valor primário dos documentos arquivísticos, surge a necessidade de proceder à avaliação dos conjuntos documentais, a fim de verificar a presença de valores secundários. Tais aspectos devem ser observados enquanto os documentos ainda se encontram no SIGAD. Assim, com a avaliação, procede-se à eliminação, seguindo os devidos procedimentos e legislação, dos que não possuem mais valor primário. Posteriormente, os documentos dotados de valor secundário serão recolhidos ao arquivo permanente, que será entendido como repositório arquivístico digital confiável (RDC-Arq).

Conforme o Conarq (2015), um repositório arquivístico digital confiável (RDC-Arq) deve gerenciar documentos e metadados seguindo princípios e práticas da arquivística no que tange à gestão documental, descrição multinível e preservação. O RDC-Arq será responsável por proteger características do documento arquivístico, como a autenticidade e a organicidade, possibilitando o acesso em longo prazo destes documentos. Além disso, é preciso estar em conformidade com a ISO 16.363:2012, que trata de um conjunto de critérios para mensurar a confiabilidade do repositório digital.

Quando abordamos a característica confiável do repositório arquivístico digital, estamos falando que estes repositórios precisam ser auditados e certificados, e, nesse cenário, a resolução n. 43 do Conarq deixa clara a sua posição quanto à adoção da ISO 16.363:2012. Isso denota que a autenticidade dos documentos arquivísticos recebe mais uma camada para reforçar a cadeia de custódia digital, ou seja, da abordagem de Jenkinson (1922), da custódia focada do produtor à instituição arquivística, agora temos, além dos ambientes Sigad e RDC-Arq e da instituição arquivística, a instituição certificadora que vai garantir que a autenticidade se manteve de acordo com os requisitos estabelecidos, indo então além da instituição arquivística e reforçando esta linha ininterrupta digital.

Há cenários distintos para se implementar o RDC-Arq (Conarq, 2015). Dentre eles podem se destacar: o ciclo de vida completo, no qual haverá um RDC-Arq para as fases corrente e intermediária e outro para a fase permanente. Esse cenário poderá envolver a mudança da cadeia de custódia para o RDC-Arq da fase permanente; as idades corrente e intermediária, associadas a um Sigad. Dessa maneira, o repositório irá auxiliar na preservação de docu-

mentos que ficam por longos períodos em fase corrente/intermediária. Isso se justifica pelos acelerados ciclos de obsolescência tecnológica. Logo, haverá uma preocupação com a preservação dos documentos arquivísticos digitais; a idade permanente, para que assim os documentos arquivísticos digitais sejam preservados permanentemente. Portanto, o RDC-Arq irá atuar na manutenção da autenticidade e da relação orgânica, além de auxiliar no arranjo e na descrição, visando ao acesso.

A implementação do RDC-Arq irá depender do cenário em questão. Mas fica expressa a necessidade de um repositório com tais características para os documentos de valor permanente e a possibilidade de se implementar outro para os documentos de valor corrente e intermediário, havendo a possibilidade de se reunir os documentos das três idades em um único RDC-Arq, porém permanecendo independentes, já que o de documentos de valor corrente e intermediário quem o interopera é o Sigad, enquanto que o de valor permanente será a instituição arquivística, pois o Sigad somente interopera para o recolhimento, além da curadoria digital, auditoria e certificação. O principal a salientar, nesse caso, é que sem um RDC-Arq devidamente implementado, o documento arquivístico mais uma vez terá sua autenticidade posta em dúvida.

O MODELO OAIS E A PRESERVAÇÃO DE LONGO PRAZO

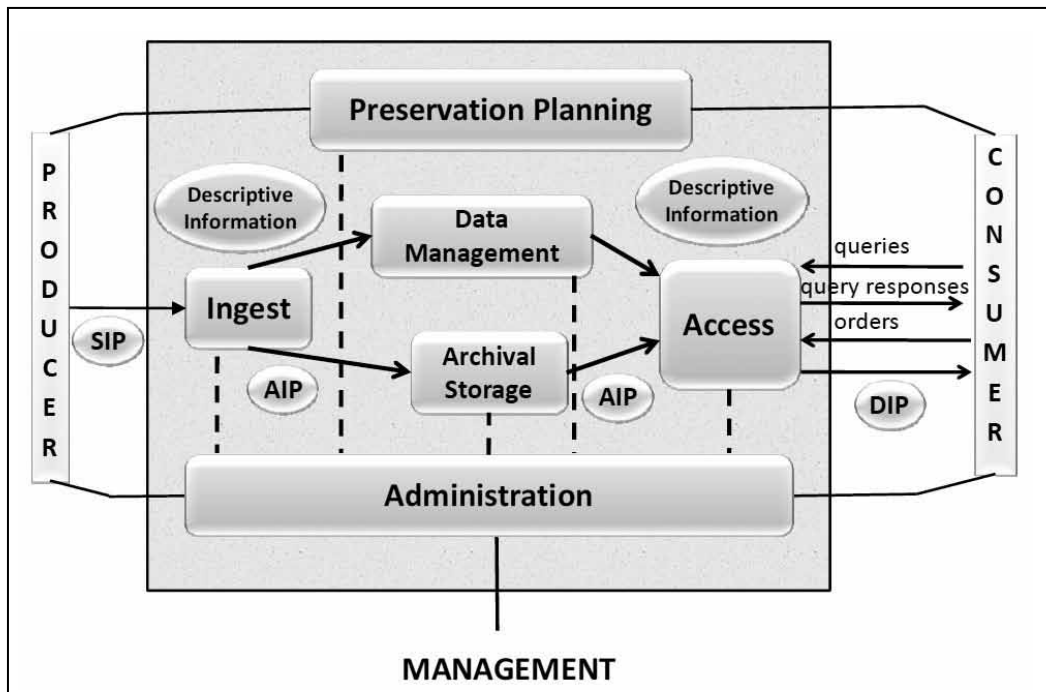
Além da implementação de estratégias, observa-se que as atividades de preservação digital em longo prazo também estão relacionadas à implementação de um repositório digital. Adicionalmente, durante o desenvolvimento de um repositório digital é fundamental que se considerem os requisitos abordados no modelo de referência Open Archival Information System (Oais).⁴

O modelo Oais especifica um conjunto de requisitos para um repositório digital que tenha a responsabilidade de preservar documentos digitais e garantir o acesso em longo prazo para uma comunidade específica de usuários. Logo, considera-se que os documentos a serem armazenados no Oais devem ser preservados em longo prazo, independente da longevidade desse modelo (CCSDS, 2012). O esquema conceitual do modelo Oais é apresentado na figura 2.

No modelo Oais, observam-se três agentes: produtor (*producer*), administrador (*management*) e consumidor (*consumer*). O produtor realiza a submissão de um pacote de informação, o qual contém documentos e informações de descrição relacionada (SIP), que é enviado para a entidade de ingestão ou submissão (*ingest*). Após aceitar o pacote SIP na etapa da ingestão, bem como inserir a informação de descrição (*descriptive info*), o SIP transforma-se em um pacote de informação para armazenamento (AIP), e aqui temos o pacote de armazenamento dos documentos de valor permanente.

4 No Brasil, o modelo Oais está traduzido sob a forma da ABNT NBR 15.472:2007 – sistemas espaciais de dados e informações – modelo de referência para um sistema aberto de arquivamento de informação (SAAI).

FIGURA 2. MODELO OAIS



Fonte: CCSDS, 2012.

Em seguida, o pacote AIP tem seus metadados extraídos e armazenados na entidade gestão de metadados (*data management*). Desse modo, os objetos digitais presentes no pacote AIP são armazenados na entidade repositório de arquivos (*archival storage*), para que as estratégias de preservação digital definidas na entidade do plano de preservação (*preservation planning*) sejam implementadas.

Após o AIP ser armazenado nas entidades de gestão de metadados e repositório de arquivos, é possível gerar o pacote de informação de disseminação (DIP). O pacote DIP possui características voltadas para facilitar o acesso, que é o objetivo final do modelo Oais. Assim, o DIP não se concentra diretamente nas atividades de preservação como o SIP e o AIP. Em outras palavras, o pacote DIP trabalha com formatos de arquivo “mais leves”, os quais são voltados para o acesso à comunidade-alvo, inclusive os metadados que estarão presentes no DIP serão diferentes dos metadados constantes do AIP. No entanto, salienta-se que estes formatos são definidos na entidade do plano de preservação e, por isso, é preciso identificar os melhores formatos a fim de facilitar o acesso aos usuários da informação.

Os documentos digitais são disponibilizados através da entidade de acesso (*access*). Dessa maneira, os consumidores podem realizar consultas (*queries*) que retornam resultados imediatos (*queries responses*). Além disso, é possível fazer solicitações (*orders*) que são enviadas para análise do administrador (*administrator*), para que, posteriormente, o acesso ao material seja liberado ou, em caso negativo, seja informado o motivo da negação.

Registre-se que o modelo Oais, mais especificamente, a entidade de acesso (*access*), tende a contribuir com a Lei de Acesso à Informação (LAI). Essa lei consiste em proporcionar o acesso aos documentos e informações relacionadas ao indivíduo e parte do pressuposto de que o acesso é entendido como uma regra geral enquanto o sigilo é uma exceção, utilizado em caso previamente justificado mediante a definição do nível de sigilo (Brasil, 2011).

Em síntese, a entidade de acesso é responsável por retornar os resultados que integram o pacote DIP. Isso compreende os materiais digitais preservados na entidade repositório de arquivos (*archival storage*) e os seus respectivos metadados armazenados na entidade (*data management*). Verifica-se que ambos são entregues ao consumidor, tendo em vista os formatos de arquivo definidos na entidade plano de preservação (*preservation planning*), para facilitar o acesso por parte do público consumidor.

Há de se ressaltar que todos os processamentos realizados no interior do repositório são gerenciados pela entidade de administração (*administration*). Essa entidade possui controle de alto nível sobre todo o modelo Oais, tendo a permissão para definir, por exemplo, os padrões de metadados, as estratégias e os formatos de arquivo para preservação e acesso.

A entidade de acesso, aqui apresentada como plataforma de acesso, segundo o modelo Oais, é externa à entidade de administração. Esse fator é importante demais à questão de segurança da informação registrada nos pacotes AIP que estarão armazenados exclusivamente na entidade de administração, em uma zona controlada, restringida, enquanto que a entidade de acesso poderá estar em uma zona desmilitarizada (cenários de uso de DMZ)⁵.

CUSTÓDIA CONFIÁVEL PARA DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

Manter uma cadeia de custódia para documentos arquivísticos produzidos no ambiente digital é uma tarefa muito complexa se comparada à realidade dos documentos tradicionais. A abordagem de Jenkinson (1922) é suficiente para os documentos tradicionais. Entretanto, no caso dos documentos digitais, é preciso lançar mão de novas teorias para preencher as lacunas teóricas e as incertezas que a própria evolução do documento arquivístico criou. Mas, ainda é com base em Jenkinson que se amplia esta teoria para o meio digital.

Em meio digital há diversas transformações, tanto de ordem teórica quanto prática. Dentre essas, pode-se destacar a guarda dos documentos digitais que possuirá uma responsabilidade compartilhada entre a instituição arquivística e a equipe de tecnologia da informação. Nesse ponto, observa-se a necessidade de se utilizar os referenciais tradicionais (Jenkinson, 1922) e, paralelamente, combiná-los com os requisitos previstos no e-ARQ Brasil e no modelo Oais. Há ainda de se considerar uma aproximação com as tecnologias da informação, mantendo uma relação interdisciplinar, visto que é fundamental que os sistemas informatizados de gestão, preservação e acesso contemplem os requisitos arquivísticos previamente definidos.

5 DMZ Zona Desmilitarizada, um cenário de uso computacional para segurança da informação.

Tendo em vista a realidade dos documentos arquivísticos digitais, ressalta-se a necessidade de que a manutenção da cadeia de custódia seja realizada por meio de “ambientes autênticos”, os quais seriam o Sigad e o RDC-Arq. É preciso que esses ambientes comportem todo o ciclo de vida dos documentos arquivísticos, assim Sigad (nas fases corrente e intermediária) e RDC-Arq (na fase permanente) devem contemplar os requisitos do e-ARQ e do Oais, respectivamente. Nesse sentido, observa-se, que após o término das fases corrente e intermediária, poderá haver alteração na cadeia de custódia. Mas, é realçado que essa alteração não consista em uma interrupção. O que acontece é a transferência dos documentos de valor permanente que estão no Sigad para o RDC-Arq, para que assim seja garantida a sua preservação e acesso em longo prazo. Logicamente, poderá ocorrer a mudança do custodiador, tendo, então, uma instituição responsável pelo Sigad e outra pelo RDC-Arq, a fim de que se contemple o ciclo documental, o que não é uma condição *sine qua non*.

Ao tratar-se da cadeia ininterrupta de custódia, que até então era o referencial utilizado para os documentos em suporte analógico, devemos agora ampliar este conceito, contemplando documentos em ambiente digital. Pois, se antes a cadeia de custódia se dava do produtor ao custodiador, sem nenhuma interrupção, sendo o seu objeto o documento analógico, em papel, o qual tinha elementos e características que evidenciavam adulterações, agora ao ampliar-se este conceito de Jenkinson, devemos perceber que o documento não é mais o analógico e palpável, o qual o produtor repassa ao custodiador para a sua guarda, mas, sim, o digital, produzido e repassado ao custodiador através de ambientes digitais que apresentam complexidade e especificidade. Ou seja, um documento produzido em um ambiente digital (Sigad) e, após avaliação, é repassado deste ambiente para o ambiente permanente, que é um repositório digital, um RDC-Arq. Assim, não sofrendo rupturas na cadeia de custódia, o controle teve que ser mais efetivo, com mais controles e registros, documentações, metadados e uma garantia de inalterabilidade ao se considerar que o documento arquivístico digital é uma cadeia de bits cheia de vulnerabilidades.

O arquivo permanente digital pode ser na própria instituição produtora de documentos, logo não há mais a necessidade de ser a instituição de Arquivo, como ocorria com os documentos analógicos. Dessa forma, o RDC-Arq tem como requisito, em si mesmo, garantir a autenticidade dos documentos, e para isto, utiliza-se de artifícios como a tramitação digital, a interoperabilidade, e de um controle com trilhas de auditoria, as quais irão documentar qualquer alteração realizada. Observa-se que o RDC-Arq manterá a autenticidade dos pacotes AIP, e este ambiente será tido como uma “zona militarizada” onde não haverá possibilidade de acesso, e alteração dos documentos, para nenhuma pessoa externa ao ambiente de administração Oais.

A construção de uma cadeia de custódia ininterrupta digital requer que o documento esteja inserido no Sigad desde a produção até o seu recolhimento no arquivo permanente, o RDC-Arq, sem que haja alterações, não autorizadas ou não documentadas, em seu conteúdo. Nesse contexto, o incremento na abordagem de Jenkinson é que o produtor passa ao custodiador os documentos digitais por meio de uma interoperabilidade composta por empacotamento e metadados específicos, com plataformas próprias, do Sigad ao RDC-Arq. Os personagens são

os mesmos, produtor e custodiador, mas a forma que autentica tal linha ininterrupta é mais complexa, envolvendo inclusive agentes externos, a entidade certificadora, de auditoria, em consonância à ISO 16.363:2012. Tais requisitos irão conferir um status aos ambientes digitais, avaliando sua conformidade com modelos pré-definidos em cada região ou país, observando, assim, a efetividade da linha de custódia entre o Sigad e o RDC-Arq.

A manutenção então desta linha ininterrupta digital, desta cadeia de custódia digital, para os documentos arquivísticos, neste ambiente, pressupõe que as ferramentas digitais e os ambientes de gestão, de preservação e de acesso contemplem os requisitos, as normas, os padrões de metadados. Além disso, é preciso implementar trilhas de auditoria desde sua produção em um Sigad, incorporando metadados, até o seu recolhimento no repositório, no arquivo permanente, o que vem demonstrar que o referido documento não sofreu nenhuma adulteração e manteve a sua presunção de autenticidade, inclusive sendo auditado e certificado por instituição idônea externa.

Todo e qualquer documento digital ao ser depositado em um repositório digital, mantém a autenticidade, mesmo que sofra alterações de formato para sua preservação. Tais alterações são identificadas e, dessa forma, o repositório comprova que determinado documento ainda é autêntico através das informações registradas em metadados Premis – sigla para *Preservation Metadata: implementation strategies*; ou mesmo em outros padrões de metadados que podem ser implementados.

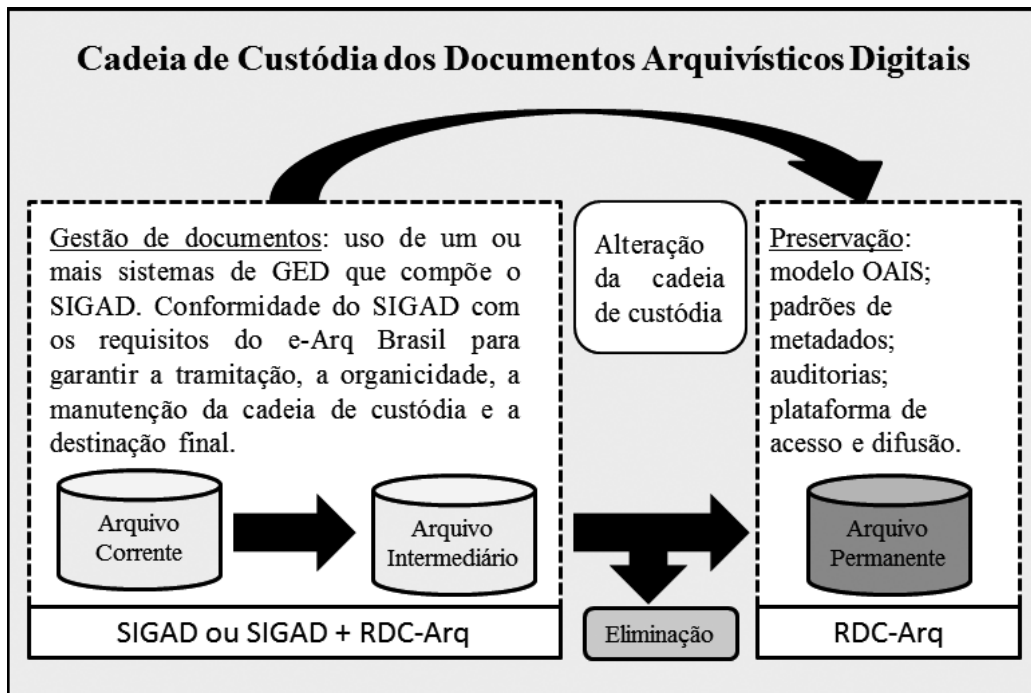
Assim, pode-se dar o acesso a um documento em uma plataforma de acesso, como, por exemplo, o ICA-AtoM (AtoM) ou outro que desempenhe a mesma função, mas jamais através do repositório digital. O repositório digital não deve permitir o acesso direto em seu ambiente de administração, e é isso que mantém a sua autenticidade, pois o documento está em uma “zona militarizada” onde não se dá nenhum tipo de acesso ao documento, senão ao ambiente de administração Oais. Em síntese, o repositório digital limita-se à função de preservar e garantir a autenticidade dos documentos em longo prazo, restringindo-se ao acesso externo. Dessa forma, membros externos ao ambiente de administração do Oais só poderão ter acesso aos documentos através da plataforma de acesso, condição que reforça a segurança deste ambiente.

A abordagem da cadeia ininterrupta de custódia aplicada ao ambiente convencional parece ser confundida com a cadeia de custódia da preservação, quando é aplicada ao meio digital. Tal fato se justifica, pois a preservação é realizada ao se trabalhar com ferramentas de tecnologia da informação, no entanto a preservação está contida dentro da cadeia de custódia ininterrupta digital. Dessa forma, o próprio sistema participará desta cadeia, visto que o documento digital será produzido e entregue ao preservador, tornando-se o novo custodiador, o qual dispõe da ferramenta de preservação: o RDC-Arq, que fará as alterações necessárias para efetuar a preservação e garantir o acesso em longo prazo.

A figura 3 ilustra as relações entre Sigad e e-ARQ, e RDC-Arq e Oais. Observa-se que o Sigad deverá contemplar princípios arquivísticos como a organicidade, além de possibilitar, por exemplo, a criação, a classificação, a tramitação e a avaliação documental. Já o RDC-Arq terá a função de preservar e garantir o acesso fidedigno em longo prazo. Para isso, a

conformidade com o modelo Oais é fundamental, da mesma forma a definição de padrões de metadados para a preservação e a realização de auditorias periódicas que comprovem a confiabilidade do ambiente de custódia.

FIGURA 3. CADEIA DE CUSTÓDIA DOS DOCUMENTOS ARQUIVÍSTICOS DIGITAIS



Fonte: elaborado pelos autores.

O modelo Oais proporciona uma série de recursos relativos à estrutura de metadados utilizados em sistemas de informação. Salienta-se que esses metadados podem registrar procedimentos técnicos de preservação e, portanto, especificar permissões de acesso para garantir a autenticidade dos materiais digitais. Os metadados ainda podem registrar as possíveis alterações na cadeia de custódia de um objeto digital, como também identificá-lo de forma única, tanto interna, quanto externamente, o que possibilita relacioná-lo ao arquivo a que pertence. Tais fatos apontam que a criação e o desenvolvimento de metadados de preservação consistem em componentes essenciais à maioria das estratégias de preservação digital (Thomaz; Soares, 2004).

Observa-se que é no ambiente de preservação (RDC-Arq) que serão realizadas as “intervenções” humanas sobre os documentos digitais. Dessa forma, o tratamento intelectual consistirá na implementação de estratégias de preservação digital, as quais são fundamentais para que se tenha uma perspectiva de acesso no futuro.

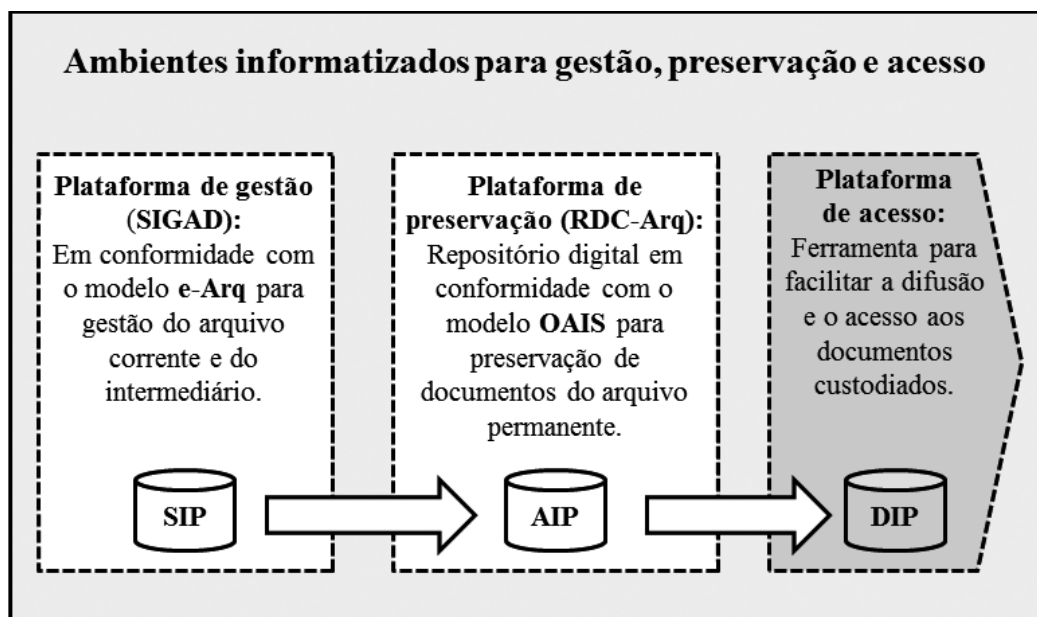
Diversos estudos recomendam a implementação de estratégias como a migração, o refreshamento, a emulação e o encapsulamento. Embora não haja uma estratégia que resolva

todos os problemas de obsolescência tecnológica, tornou-se necessário aos acervos tomar conhecimento e manter um conjunto de estratégias a serem implementadas conforme a necessidade (Ferreira, 2006; Grácio; Fadel, 2010; Hedstrom, 2001; Márdero Arellano, 2004; Rothenberg, 1999; Santos, 2005; Saramago, 2002; Thibodeau, 2002).

Além de realizar a manutenção da integridade e da autenticidade, os RDC-Arq's devem contemplar atividades de arranjo, descrição, acesso e difusão dos documentos custodiados. Considerando que esses registros são de caráter permanente, não se deverá permitir atividades típicas das fases corrente e intermediária, no caso, a avaliação.

De maneira geral, a cadeia de custódia digital consiste em uma linha ininterrupta capaz de gerenciar o ciclo de vida dos documentos arquivísticos em suas respectivas idades. Nessa linha, ressalta-se a necessidade de plataformas interoperáveis, para que assim os documentos de valor permanente contidos no Sigad (pacote SIP) sejam recolhidos ao RDC-Arq e armazenados (pacote AIP), a fim de que posteriormente possam ser difundidos e acessados (pacote DIP). Tal questão é esquematizada na figura 4.

FIGURA 4. AMBIENTES INFORMATIZADOS PARA GESTÃO, PRESERVAÇÃO E ACESSO



Fonte: elaborado pelos autores.

Assim, é reforçada a vital importância de garantir bons níveis de interoperabilidade entre o Sigad e o RDC-Arq, sendo, para isso, preciso considerar os requisitos propostos nos modelos e-ARQ e Oais, respectivamente. Logo, observa-se que a questão da interoperabilidade se estende desde as plataformas de gestão e preservação até a plataforma de acesso, comportando, desse modo, todo o ciclo de vida dos documentos arquivísticos, que é regido por uma linha de custódia ininterrupta.

CONSIDERAÇÕES FINAIS

No atual contexto prático-teórico, no qual se inserem os documentos arquivísticos digitais, existe a necessidade de se considerar a manutenção de uma cadeia de custódia digital, que será tida como uma linha ininterrupta para se gerenciar os documentos arquivísticos ao longo do seu ciclo de vida. Ao se analisar a proposta de Jenkinson, ressalta-se que seu foco está na instituição arquivística. No entanto, as complexidades e as especificidades adicionadas pelos documentos arquivísticos digitais tornam necessário que o foco esteja nos ambientes informatizados nos quais se faz a custódia desses documentos, assim como na auditoria e na certificação destes ambientes. Dessa forma, será preciso manter uma linha de custódia digital documental entre o Sigad e o RDC-Arq, considerando que qualquer ruptura irá corromper a presunção de autenticidade.

É fundamental destacar que esta linha ininterrupta da cadeia de custódia digital é composta por três ambientes ou plataformas interoperáveis, a saber, o ambiente de gestão de documentos (Sigad), o ambiente de preservação (RDC-Arq) e o ambiente de acesso, descrição arquivística e difusão (plataforma de acesso). Embora a resolução n. 43 do Conarq preconize que o RDC-Arq seja composto pelo repositório arquivístico digital confiável e pela plataforma de acesso, é preciso destacar que o modelo Oais faz uma diferenciação, mantendo os ambientes de preservação e acesso separados, conforme pode ser observado em suas entidades. Dessa forma, o repositório arquivístico está na entidade de administração do Oais, uma entidade fechada, já a plataforma de acesso está em um ambiente externo, o do consumidor. Segundo a terminologia Oais, a plataforma de acesso é o ambiente para realizar a descrição arquivística, a difusão e o acesso, enquanto que a entidade do produtor Oais corresponde ao Sigad ou ao sistema de negócio interoperado com o Sigad.

Registre-se que é preciso manter níveis de interoperabilidade entre os sistemas informatizados: Sigad, RDC-Arq e plataforma de acesso. Dessa forma, as atividades realizadas sobre os documentos custodiados não serão perdidas, visto que há necessidade de manter informações na forma de metadados, as quais são essenciais para se mensurar a sua autenticidade. Logo, o mesmo documento que se encontra no Sigad, e que posteriormente é transferido ao RDC-Arq, precisa manter seus metadados, que são fundamentais para identificar a sua organicidade e conhecer o seu “histórico” de alterações.

Os padrões de metadados podem identificar um documento e seus componentes digitais de forma única em um sistema informatizado, bem como fornecer referência ao seu código de classificação. Portanto, os metadados são capazes de registrar o histórico de migrações de formato e versão, assim como os emuladores que foram utilizados para se acessar um documento e seus respectivos componentes digitais. Além disso, os metadados são essenciais para se realizar o encapsulamento do documento junto com seus componentes. Dessa forma, a interoperabilidade entre sistemas torna-se um componente-chave para uma custódia confiável, evitando a perda de informação referente à manutenção da integridade e da autenticidade dos documentos.

Outro ponto a ser destacado é a questão da auditoria dos sistemas informatizados, pois isso irá impactar, diretamente, na mensuração da confiabilidade. Tanto os sistemas de gestão quanto os de preservação precisam ser auditados e certificados para que assim seja verificada a sua conformidade com os padrões pré-estabelecidos, a fim de se assegurar a fidedignidade dos documentos arquivísticos. Observa-se que as auditorias periódicas sucedidas de certificação, que demonstrem a conformidade com os requisitos, irão adicionar confiabilidade aos sistemas informatizados.

Por fim, este estudo demonstra que a manutenção da cadeia de custódia documental é uma prática fundamental para se manter os documentos arquivísticos digitais em um ambiente confiável. A conformidade com padrões pré-estabelecidos e a auditoria periódica dos sistemas informatizados fornecem subsídios para se desenvolver um ambiente autêntico em todo o ciclo de vida dos documentos, então, concluindo-se que ademais da investigação permanente da temática, os documentos arquivísticos digitais necessitam de uma cadeia de custódia digital arquivística desde a sua gênese, desde o seu ambiente de gestão de documentos, o Sigad, até seu recolhimento ao RDC-Arq, inclusive mantendo a autenticação referenciada nas plataformas de acesso e garantindo a descrição, a navegação multinível e a difusão arquivística.

Referências bibliográficas

CONSELHO NACIONAL DE ARQUIVOS (Conarq). Câmara Técnica de Documentos Eletrônicos. *Cenários de uso de RDC-Arq em conjunto com o Sigad*. Rio de Janeiro: Arquivo Nacional, 2015. Disponível em: <http://www.conarq.arquivonacional.gov.br/images/ctde/Orientacoes/OrientacaoC3%A7%C3%A3o_t%C3%A9cnica_RDCArq2015_pub.pdf>. Acesso em: 15 fev. 2016.

_____. Câmara Técnica de Documentos Eletrônicos. *e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos*. Rio de Janeiro: Arquivo Nacional, 2011. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/publicacoes/earq/conarq_earqbrasil_model_requisitos_2009.pdf>. Acesso em: 5 ago. 2014.

BRASIL. Lei n. 12.527, de 18 de novembro de 2011. Brasília, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 14 maio 2016.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). *Reference model for an Open Archival Information System (Oais)*. Washington: Magenta Book, jun. 2012. Disponível em: <<http://public.ccsds.org/publications/archive/650x0m2.pdf>>. Acesso em: 13 maio 2015.

DOLLAR, C. Tecnologias da informação digitalizada e pesquisa acadêmica nas ciências sociais e humanas: o papel crucial da arquivologia. *Estudos Históricos*, Rio de Janeiro, v. 7, n. 13, p. 65-80, jul. 1994. Disponível em: <<http://bibliotecadigital.fgv.br/ojs/index.php/reh/article/view/1977>>. Acesso em: 26 maio 2016.

FERREIRA, M. *Introdução à preservação digital: conceitos, estratégias e atuais consensos*. Portugal: Escola de Engenharia da Universidade do Minho, 2006. Disponível em: <<https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>>. Acesso em: 2 mar. 2016.

FLORES, D. *Cadeia de custódia digital de documentos arquivísticos: do Sigad ao RDC-Arq*. Brasília, DF: Instituto de Patrimônio Histórico e Artístico Nacional (Iphan), 2016, 122 slides, color, padrão

slides Google Drive/Docs 4x3. Material elaborado para a palestra no Iphan, 28 abr. 2016. Disponível em: <<http://documentosdigitais.blogspot.com>>. Acesso em: 28 abr. 2016.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2010.

GRÁCIO, J. C. A.; FADEL, B. Estratégias de preservação digital. In: VALENTIM, M. (org.). *Gestão, mediação e uso da informação*. São Paulo: Unesp; Cultura Acadêmica, 2010. Disponível em: <<http://books.scielo.org>>. Acesso em: 1 dez. 2014.

HEDSTROM, M. *Digital preservation: problems and prospects*. USA: University of Michigan, 2001. Disponível em: <http://www.dl.slis.tsukuba.ac.jp/DLjournal/No_20/1-hedstrom/1-hedstrom.html>. Acesso em: 10 jan. 2.

JENKINSON, H. *A manual of archive administration including the problems of war archives and archive making*. Oxford: Clarendon Press, 1922.

LUNA, S. V. de. *Planejamento de pesquisa: uma introdução*. São Paulo: Educ, 1997.

MÁRDERO ARELLANO, M. A. Preservação de documentos digitais. *Ciência da Informação*, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: <<http://revista.ibict.br/ciinf/index.php/ciinf/article/view/305>>. Acesso em: 25 jul. 2014.

ROTHENBERG, J. *Ensuring the longevity of digital information*. Santa Monica: [s.n.], 1999. Disponível em: <http://www.realtechsupport.org/UB/Aml/texts/Rothenberg_LongevityDigitalInformation_1999.pdf>. Acesso em: 21 jan. 2016.

SANTOS, V. B. dos. *Gestão de documentos eletrônicos: uma visão arquivística*. 2. ed. rev. aum. Brasília: Abarq, 2005.

SARAMAGO, M. de L. Preservação digital a longo prazo: boas práticas e estratégias. *Cadernos BAD*, Lisboa, n. 2, p. 54-68, 2002. Disponível em: <<http://www.bad.pt/publicacoes/index.php/cadernos/article/view/866>>. Acesso em: 10 fev. 2015.

THIBODEAU, K. Overview of technological approaches to digital preservation and challenges in coming years: the state of digital preservation: an international perspective. In: CLIR AND LIBRARY OF CONGRESS, 2002, Washington. *Anais eletrônicos...* Washington: Council on Library and Information Resources, 2002. Disponível em: <<http://www.clir.org/pubs/reports/pub107/thibodeau.html>>. Acesso em: 19 ago. 2015.

THOMAZ, K. P.; SOARES, A. J. A preservação digital e o modelo de referência Open Archival Information System (Oais). *DataGramaZero*, Rio de Janeiro, v. 5, n. 1, 2004. Disponível em: <http://www.dgz.org.br/fev04/F_I_art.htm>. Acesso em: 12 mar. 2015.

Recebido em 30/5/2016

Aprovado em 20/7/2016