Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo

Henrique Machado dos Santos

Graduado em Arquivologia pela Universidade Federal de Santa Maria .Membro do grupo de pesquisa CNPq-UFSM: GED/A

Daniel Flores

Doutor em Documentação pela Usal.Doutor em Metodologías y Líneas de Investigación en Biblioteconomía y Documentación - Universidad de Salamanca/España Docente Colaborador do Mestrado Profissional em Gestão de Documentos e Arquivos - PPGARQ – UNIRIO

http://dx.doi.org/10.1590/1981-5344/2341

A evolução da tecnologia da informação e a sua inserção na Arquivologia proporcionou rupturas no conceito e na concepção de documento arquivístico que se refletem nas práticas de gestão, preservação e acesso. A complexidade e a especificidade do documento arquivístico digital implica na necessidade de um tratamento diferenciado se comparado aos documentos tradicionais em suportes analógicos. Além disto, é preciso garantir a integridade e a autenticidade dos documentos digitais armazenando-os em um sistema confiável. Neste sentido, os repositórios digitais se configuram no âmbito global como a melhor alternativa para a preservação em longo prazo, entretanto, as ações para gerar confiabilidade ainda são pouco difundidas. Este artigo tem por objetivo realizar uma reflexão sobre os requisitos para desenvolver um repositório digital confiável. A metodologia utilizada consiste na revisão de materiais previamente publicados nos últimos vinte anos, a qual aborda os dados de forma qualitativa, enfatizando os estudos mais recentes. Dentre os avanços mais significativos, salienta-se a realização de auditorias para que os repositórios possam ser certificados como "confiáveis". Além disso, é reforçada a utilização de normas e recomendações, e a definição prévia de políticas de preservação digital que considerem

a confiabilidade durante todo o ciclo documental, configurando assim uma custódia confiável.

Palavras-chave: *Arquivologia; Documentos arquivísticos digitais; Repositórios digitais; Confiabilidade; Preservação Digital.*

Trusted digital repositories for digital archival documents: considerations on the preservation in long-term

The evolution of information technology and its insertion in the Archival science provided breaks in the concept and design of archival document that are reflected in practices of management, preservation and access. The complexity and specificity of the digital archival document implies the need for different treatment compared to traditional documents on analog media. In addition, we must ensure the integrity and authenticity of digital documents by storing them in a trusted system. In this sense, digital repositories are configured globally as the best alternative to preserve in long-term, however, the actions to generate trustworthy are poorly distributed. This article aims to make a reflection on the requirements for developing a trusted digital repository. The methodology used is to review of materials previously published in the last twenty years, which approaches the data qualitatively, emphasizing the most recent studies. Among the most significant advances, highlight the audits for the repositories can be certified as "trusted". Furthermore, is enhanced the use of standards and recommendations, and the prior definition of digital preservation policies that consider the trustworthy throughout the documentary cycle, thus creating a trust custody.

Keywords: *Archival science; Digital archival documents; Digital repositories; Trustworthy; Digital preservation.*

Recebido em 22.02.2015 Aceito em 07.05.2015

1 Introdução

As tecnologias da informação vêm exercendo um papel renovador, sua evolução acarretou um maior volume e variedade de dados registrados. Desta forma, paralelo ao aumento da informação registrada pela sociedade, ocorre a explosão do volume de documentos arquivísticos (DE SORDI, 2008; LOPES, L., 1997; SOUSA, 2007; 2008).

No entanto, as tecnologias para produção e armazenamento de documentos digitais estão evoluindo em um ritmo muito acelerado, logo, torna-se fundamental preservar a documentação que foi e está sendo produzida (HEMINGER; ROBERTSON, 2000). Pois a capacidade de se criar, acumular e armazenar documentos digitais excede em muito a capacidade atual para preservá-los (HEDSTROM, 1998). Desta forma, a tecnologia da informação está sendo cada vez mais discutida na Arquivologia.

> A informática está definitivamente incorporada aos arquivos, seja na gestão ou na disseminação da informação de documentos tradicionais, seja na organização e descrição de documentos em suportes isolados concretos, seja nos documentos virtuais, integrantes dos bancos de dados e dos sistemas de comunicações (BELLOTTO, 2006, p. 305).

Atualmente, há documentos arquivísticos sendo produzidos e armazenados exclusivamente em formato digital (CONSELHO NACIONAL DE ARQUIVOS -CONARQ, 2004a; 2004b; INNARELLI, 2011; INTERPARES, 2007b; THOMAZ, 2005; 2006), fato que reforça a sua relevância como registro e fonte de prova e informação (INNARELLI, 2007). Deve-se destacar que o documento arquivístico digital proporcionou vantagens como a facilidade de acesso e economia de espaço físico. Entretanto, a ausência de procedimentos adequados de segurança e de preservação criam dúvidas quanto à confiabilidade, autenticidade e acesso futuro (ROCHA; SILVA, 2007).

> Os documentos arquivísticos digitais apresentam dificuldades adicionais para presunção de autenticidade em razão de serem facilmente duplicados, distribuídos, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes (CONARQ, 2012, p. 1).

Desta forma, os documentos arquivísticos digitais necessitam de um tratamento diferenciado devido ao fato de possuírem características próprias para a comprovação de sua autenticidade, a qual é ameaçada pelos acelerados ciclos de obsolescência tecnológica (CONARQ, 2014; SOUSA, 2007). Em princípio a preservação digital deverá efetuar a manutenção da integridade e da autenticidade dos documentos arquivísticos digitais em virtude da necessidade de garantir que o

patrimônio documental mantido sob custódia é autêntico e permanecerá íntegro no decorrer do tempo. Assim será possível promover o acesso contínuo em longo prazo ao conteúdo e funcionalidade de forma fidedigna (CONARQ, 2004a; CORRÊA, 2010). A preservação de documentos digitais deve ser fundamentada no planejamento, alocação de recursos, aplicação de métodos de conservação e tecnologias necessárias para assegurar as características diplomáticas originais do documento arquivístico de modo que permaneça acessível em utilizável em longo prazo (HEDSTROM, 1998; INNARELLI, 2012). Sendo assim, as atividades de preservação digital deverão compreender uma série de políticas institucionais, responsabilidade e, é claro, a implementação de estratégias de preservação.

Com relação às estratégias de preservação digital, Santos (2005) apresenta a criação de museus tecnológicos, preservação da cadeia de bits, encapsulamento, formatos padronizados, migração e emulação. Ferreira (2006) acrescenta o refrescamento, a Pedra de Rosetta digital e define formas variáveis para a migração: migração para suportes analógicos, atualização de versões, conversão para formatos concorrentes, normalização, migração a-pedido e migração distribuída. Corrêa (2010) cita a reprodução em suportes analógicos, cópias de segurança, mídias duráveis e o Computador Virtual Universal. E Thomaz (2004) apresenta ainda, a conversão da tecnologia e a aplicação da arqueologia digital.

As estratégias de adoção de formatos padronizados, armazenamento em mídias duráveis e realização de cópias de segurança, estão mais relacionadas às políticas institucionais. A arqueologia digital será relevante caso se deseja recuperar algum documento que tenha sido corrompido ou apagado indevidamente. Estratégias como reprodução em formatos analógicos e a Pedra de Rosetta digital devem ser utilizadas como um último recurso devida a sua descaracterização do objeto digital. A criação de museus tecnológicos será viável apenas em curtos períodos de tempo devendo ser seguida de outra estratégia. O refrescamento de suporte será indispensável para qualquer acervo, entretanto deve ser auxiliado por outras estratégias. As técnicas de encapsulamento apresentam resultados satisfatórios, contudo poderão demandar maior espaço lógico para armazenamento. A emulação necessita de conhecimentos avançados e poderá causar dependência de *software* específico. Outras técnicas, como o Computador Virtual Universal apresentam alta complexidade e demandam recursos financeiros elevados. Dentre as estratégias apresentadas, a migração é a mais utilizada e vem demonstrando sua eficácia. Embora não possa ser aplicada para objetos digitas de todas as naturezas, a migração apresenta baixos custos e simplicidade de implementação.

As estratégias de preservação digital possuem suas vantagens e desvantagens no que se refere ao acesso em longo prazo, entretanto, devem-se destacar as suas vulnerabilidades com relação à presunção de autenticidade e manutenção da integridade em longo prazo. Ressalta-se

que as estratégias devem ser executadas em um ambiente que monitore todas as ações realizadas sobre os documentos e seus respectivos componentes digitais. O ambiente de armazenamento dos documentos digitais deverá ser confiável.

Neste contexto, destaca-se que além da definição de políticas de preservação e do estabelecimento de estratégias de preservação, um dos primeiros procedimentos deve ser a transferência dos documentos para um repositório digital o qual se torna fundamental para armazená-los, facilitando a implementação das respectivas políticas e estratégias de preservação (FERREIRA, 2006; LOPES, V., 2008; MÁRDERO ARELLANO, 2008). Ao repositório compete o compromisso com a preservação, o gerenciamento e o acesso contínuo em longo prazo a documentos arquivísticos digitais autênticos (CONARQ, 2014).

A escolha por abordar a preservação do documento arquivístico se justifica pelo fato deste se divergir do documento biblioteconômico em relação às motivações de sua produção e a sua custódia. O documento biblioteconômico é produzido exclusivamente visando fins culturais enquanto o documento arquivístico possui inicialmente um valor primário, por exemplo, o valor administrativo, e, após avaliação, este documento atingirá o valor cultural (SCHELLENBERG, 2006). Além disso, o documento arquivístico possui forma e suporte variados (BELLOTTO, 2006). Deste modo, as ações de preservação digital devem considerar suas especificidades com relação à integridade, autenticidade, capacidade probatória e o seu contexto de produção (MÁRDERO ARELLANO, 2008). Destaca-se que os arquivos necessitam acessar e disponibilizar documentos autênticos e utilizáveis aos usuários, devido a sua finalidade de prestar de serviços probatórios em longo prazo (SWEDEN, 2005).

Considerando as questões apresentadas, este estudo tem por objetivo, realizar uma reflexão sobre os requisitos a serem observados na implementação de repositórios digitais confiáveis, tendo como finalidade a preservação de documentos arquivísticos digitais íntegros e autênticos, para proporcionar o acesso contínuo em longo prazo. Desta forma, observam-se as principais normas, recomendações e estudos relevantes sobre preservação digital.

Para este estudo, são utilizados métodos qualitativos, com base no levantamento bibliográfico de materiais previamente publicados (SILVA; MENEZES, 2005). O critério para a escolha dos referenciais consistiu em uma análise que abrange trabalhos dos últimos vinte anos, dando ênfase aos trabalhos publicados nos últimos dez anos. Foram selecionados, artigos, livros e demais publicações institucionais e projetos relevantes. Desta forma, busca-se maior aprofundamento teórico no âmbito da preservação de documentos arquivísticos digitais.

2 Confiabilidade

Dentre os desafios apresentados pelos documentos arquivísticos digitais, podem ser destacados a garantia da produção de registros

confiáveis, a manutenção de sua autenticidade e o acesso contínuo em longo prazo (ROCHA; SILVA, 2007). No caso da autenticidade, esta está relacionada ao contexto em que o documento está inserido.

> A autenticidade de um documento está diretamente ligada ao modo, à forma e ao status de transmissão desse documento, bem como às condições de sua preservação e custódia. Isso quer dizer que o conceito de autenticidade refere-se à adoção de métodos que garantam que o documento não foi adulterado após a sua criação e que, portanto, continua sendo tão fidedigno quanto era no momento em que foi criado (RONDINELLI, 2005, p. 66-67).

A ausência de confiabilidade acaba por ofuscar os investimentos e esforços realizados para manutenção da integridade e da autenticidade, pois não há como agregar valor para um documento digital o qual não tem garantias de que não foi alterado. Logo, a implementação de um sistema confiável torna-se fundamental para a gestão e preservação de documentos arquivísticos digitais.

Para agregar confiabilidade, os documentos arquivísticos devem estar inseridos em uma cadeia de custódia ininterrupta, permanecendo desde a sua produção até a sua transferência e/ou recolhimento para o responsável por sua preservação em longo prazo (CONARQ, 2012). Caso esta cadeia de custódia for interrompida, surgirão dúvidas com relação à autenticidade dos documentos, (CONARQ, 2012; INTERPARES, 2007a) e consequentemente perde-se a sua confiabilidade.

Para implementar programas de gestão arquivística de documentos, é necessária a elaboração dos requisitos, que possibilitarão produzir e manter documentos fidedignos e autênticos. Com base nos requisitos criados é possível estabelecer os metadados que fornecerão informações sobre o contexto de produção, bem como informações sobre seu conteúdo e tramitação (CONARQ, 2004b). Desta forma, tanto a gestão de arquivo corrente e intermediário, quanto a preservação em arquivo permanente deverão ser regidas por sistemas informatizados que garantam a integridade e autenticidade dos documentos, bem como dos metadados definidos, proporcionando acesso a documentos fidedignos.

As bibliotecas, os arquivos e os museus são encarregados pela guarda do patrimônio cultural por serem instituições que adquiriram ao longo do tempo, a necessária confiança para armazenar material de tal valor. São consideradas instituições confiáveis para preservar esses itens nas melhores condições para fornecer acesso a esse material para as futuras gerações (THOMAZ, 2007). Logo, pode-se dizer que a confiança é adquirida com o passar do tempo, no caso dos documentos digitais, será necessário comprovar a eficácia do sistema informatizado em questão. A preservação digital exigirá um sistema robusto para satisfazer os

requisitos de integridade, autenticidade, atingindo assim confiabilidade desejada.

De acordo com o CONARQ (2011):

> A confiabilidade está relacionada ao momento em que o documento é produzido e à veracidade do seu conteúdo. Para tanto, há que ser dotado de completeza e ter seus procedimentos de produção bem controlados. Dificilmente pode-se assegurar a veracidade do conteúdo de um documento; ela é inferida da completeza e dos procedimentos de produção. A confiabilidade é uma questão de grau, ou seja, um documento pode ser mais ou menos confiável (CONARQ, 2011, p. 21).

Desta forma, entende-se, que não se pode tratar a confiabilidade como um *status* de "confiável" e "não confiável", e sim como uma variável que depende do contexto tecnológico onde está situado o acervo.

Percebe-se que a informação confiável é aquela a qual os usuários conferem credibilidade, embora seja uma informação que não possua veracidade absolutamente comprovada, a informação confiável é uma informação em que se acredita (DE SORDI, 2008). No caso da informação documentada, a confiabilidade dependerá da conformidade dos documentos digitais com os princípios da Arquivologia e da Diplomática, no que se refere a manutenção de sua integridade e autenticidade.

Ao se tratar de documentos arquivísticos representados em meio digital, existe a necessidade de implementar *softwares* e políticas de gestão e preservação que visem o aumento da confiabilidade do sistema como um todo. Desta forma, estima-se que com o tempo, serão atingidos os níveis de confiança desejados pelo público alvo.

3 Repositórios digitais

A complexidade e a fragilidade implícita dos documentos digitais levam ao entendimento de que a preservação digital não é e nunca será resolvida exclusivamente pela própria tecnologia (INNARELLI, 2011). A implementação de políticas de preservação digital torna-se fundamental para garantir o armazenamento e o acesso contínuo em longo prazo (MÁRDERO ARELLANO, 2008). Com isto, o planejamento torna-se determinante para garantir a longevidade dos materiais custodiados.

Preservar documentos digitais é uma atividade diferente de preservar documentos analógicos devido às complexidades e especificidades dos digitais, porém de igual relevância social, cultural, informativa e histórica. Inicialmente a preservação de documentos digitais deverá ser a definição de políticas, e a partir destas, elaborar o plano de preservação contendo as estratégias de preservação com eficácia

comprovada, e que sejam de conhecimento do acervo. Durante a elaboração do plano de preservação deve-se ter em mente as propriedades significativas dos documentos que se queiram preservar, da mesma forma, deve-se atentar para os conceitos de forma fixa e conteúdo estável.

> *Um documento digital é tido como detentor de forma fixa e conteúdo estável quando a sua apresentação na tela do computador é sempre a mesma, ainda que essa cadeia mude quando [...] seu formato é alterado [...]. Isso quer dizer que um mesmo documento digital pode ser apresentado a partir de diferentes codificações digitais (RONDINELLI, 2013, p. 245*).

Entretanto, os documentos digitais não são exclusivamente estáticos, e apresentam variações em sua forma e conteúdo. Por este motivo surge o conceito de variabilidade limitada o qual pode ser entendido como "uma variação de forma e do conteúdo do documento que não compromete seu caráter arquivístico à medida que é implementada por regras fixas, o que equivale a dizer que tal variação é intencionada pelo autor" (RONDINELLI, 2013, p. 249-250).

Inicialmente as políticas de preservação devem descrever os requisitos diplomáticos de forma fixa, conteúdo estável, variabilidade limitada. Em seguida definem-se os procedimentos para adoção de estratégias e *softwares* a serem utilizados, implementação de repositórios digitais, escolha dos formatos de arquivo recomendados para preservação e adoção dos padrões de metadados. Durante o planejamento da preservação, a tecnologia deve estar hierarquicamente abaixo das políticas institucionais, com isto, entende-se que os sistemas informatizados deverão estar em conformidade com os requisitos de preservação em longo prazo, definidos previamente, garantindo integridade, autenticidade e confiabilidade aos documentos armazenados.

Posteriormente procede-se à escolha do local onde os documentos arquivísticos digitais serão armazenados e preservados. Neste sentido, deve-se considerar a implementação de repositórios digitais, desta forma, é possível obter maior controle sobre a documentação custodiada, facilitando a adoção de padrões de metadados e a padronização dos formatos de arquivo para preservação.

O repositório digital deve ser o ambiente autêntico para a preservação em longo prazo, dispondo, por exemplo, de ferramentas para a implementação das estratégias de preservação e inserção de padrões de metadados. Neste ambiente todas as ações realizadas sobre os documentos digitais, como por exemplo, migrações, devem ser registradas, criando-se assim, um histórico de cada objeto digital armazenado, acrescentando confiabilidade aos conteúdos.

Ao implementar repositórios digitais será possível realizar estratégias de migração e refrescamento, no caso deste, copiam-se os

arquivos armazenados em uma mídia como, por exemplo, CD ou DVD, os quais posteriormente são submetidos ao repositório. Em um primeiro momento, os documentos são copiados de uma mídia externa para um computador que disponha de um repositório digital. Em seguida, solicita-se a submissão dos documentos ao repositório. Neste momento são inseridos os metadados referentes aos documentos digitais. Após a inserção de metadados, dá-se continuidade ao processo de submissão ao repositório digital. A partir deste momento os documentos estarão sob controle do repositório e poderão ser migrados de versão, convertidos para formatos concorrentes, normalizados, migrados a-pedido e migrados de forma distribuída de modo que sua autenticidade possa ser comprovada.

Com o auxílio de repositórios digitais é possível manter os formatos de arquivos sempre atualizados, desta forma, as estratégias de migração serão mais eficazes. Além disso, os repositórios facilitam a inserção de metadados, definida no próprio repositório, assim estes metadados serão preservados ao longo do tempo juntamente com os documentos digitais. Desta forma, ao realizar a migração ou o refrescamento no âmbito do repositório digital, procede-se a inserção dos metadados, assim, percebe-se que o repositório será o centro das atividades de preservação digital, por isso deverá estar em conformidade com as políticas previamente definidas.

As atividades de preservação digital poderão ser pensadas já no momento da produção dos materiais digitais, com o uso de *softwares* livres, de código aberto, formatos de arquivo sem compressão ou em conformidade com os padrões *International Organization for Standardization* (ISO). Conforme ressalta Saramago (2004), competem ao preservador as atribuições de orientar o produtor, cada repositório deve encaminhar as normas de conduta para os produtores de documentos digitais e verificar no momento da submissão se estas normas foram cumpridas (SARAMAGO, 2004). Desta forma, o produtor será o responsável pela submissão do material ao repositório, o qual deverá garantir a integridade do material processado e efetuar o seu armazenamento (FERREIRA, 2006). A partir do momento em que os documentos são submetidos, a responsabilidade pela preservação, manutenção da autenticidade e garantia de acesso em longo prazo passa a ser do repositório.

Independente da estratégia desenvolvida pelo repositório digital, o sucesso das atividades de preservação somente será atingido se forem seguidas boas práticas. Neste sentido, a criação de metadados de preservação deverá ser considerada ao longo de todo o ciclo de vida dos documentos (SARAMAGO, 2002).

Em linhas gerais, um repositório digital deve estar em conformidade com as normas e padrões estabelecidos, e trabalhar de forma colaborativa com outros serviços de preservação digital de forma a possibilitar níveis de interoperabilidade com outros repositórios digitais e sistemas informatizados para documentos arquivísticos digitais. Desta forma, é

possível solucionar suas necessidades de cópias de segurança em locais fisicamente distintos (CONARQ, 2014; MARDERO ARELLANO, 2008). De maneira geral, seguir padrões amplamente aceitos pela comunidade de preservação aumentará a confiabilidade do repositório digital, da mesma forma, reforçara as discussões e trocas de conhecimento em prol do avanço mútuo.

4 Modelo de referência Open Archival Information System (OAIS)

O modelo OAIS é um modelo de referência conceitual que especifica os requisitos para um arquivo de materiais digitais o qual tem a responsabilidade de preservar informações e disponibilizá-las para uma comunidade específica. O termo "*Open*" significa que o modelo é desenvolvido em fóruns abertos, mesmo assim, isso não quer dizer que o acesso ao repositório é irrestrito. A documentação é armazenada no OAIS porque sua necessidade de preservação é considerada de longo prazo, mesmo se o próprio modelo não for permanente. Pode-se definir longo prazo como o tempo suficiente para se preocupar com os impactos da evolução das tecnologias (CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM - CCSDS, 2002; 2012).

Considerando que os repositórios digitais para documentos arquivísticos devem seguir normas definidas previamente, o Conarq (2014) destaca que atualmente a norma mais importante da área é o OAIS. Este modelo é uma descrição de alto nível, que expõe os conteúdos os quais é capaz de suportar, bem como as funções que são necessárias para manter um repositório em conformidade consigo (HEDSTROM, 2001). Oferece uma referência sólida para os termos, conceitos e fluxos de informações que circunscrevem um repositório digital apontando os aspectos a serem considerados para estar em conformidade com o modelo de preservação. Entretanto, o modelo OAIS não prescreve implementação (SAYÃO, 2010). Logo, o OAIS não é um repositório digital e sim, um modelo conceitual que especifica como deverá funcionar um repositório digital confiável. E por esta razão, o modelo conceitual proposto poderá ser implementado em diferentes contextos tecnológicos.

Para garantir o acesso contínuo à informação em longo prazo torna-se indispensável à criação de repositórios digitais, tendo o auxílio de *softwares* com finalidade de auxiliar as atividades do repositório. No entanto, durante a implementação do repositório é necessário ter em mente o modelo de referência OAIS (LOPES, V., 2008). Além disso, deve existir em simultâneo um modelo de informação onde se encontram descritos os requisitos de metadados para a preservação em longo prazo (SARAMAGO, 2004).

A implementação de um "arquivo de materiais digitais" em concordância com os modelos de funcionalidade e estrutura da informação propostos no OAIS é pré-requisito para se estabelecer um repositório

digital confiável, garantindo a preservação em longo prazo (MÁRDERO ARELLANO, 2008). Desta forma, as instituições arquivísticas passarão a compreender com maior clareza os conceitos arquivísticos necessários para a preservação (THOMAZ, 2006).

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

A não conformidade do *software* utilizado com as normas definidas implica na busca de outro *software* que contemple todos os requisitos previstos na norma, não encontrando o *software* que contemple os requisitos exigidos, torna-se necessário o desenvolvimento deste. Da mesma forma, pode-se usar um conjunto de *softwares* para contemplar os requisitos exigidos pelas normas, mas nunca se devem adaptar as normas para manter a conformidade com os recursos dos *softwares*.

5 Repositório digital confiável para documentos arquivísticos

A dúvida crucial em relação à confiabilidade dos repositórios digitais esta exatamente em saber o que é preciso para atingir esta confiança. Além de definir as políticas institucionais, escolher as estratégias de preservação e implementar um repositório digital em conformidade com o modelo OAIS, é preciso adicionar confiabilidade as ações de preservação digital.

Um repositório digital confiável deverá atender aos procedimentos arquivísticos e aos requisitos de confiabilidade (CONARQ, 2014). Neste sentido, pode-se dizer que a confiança se desenvolve em diversos níveis para repositórios digitais confiáveis, que são no mínimo três níveis: produtores, consumidores e fornecedores. Para isso é fundamental verificar se os produtores estão enviando as informações corretas, se os consumidores estão recebendo as informações corretas, e se os fornecedores estão prestando serviços adequados (THOMAZ, 2007). A confiabilidade deve ser considerada nas medidas de segurança, desde a construção dos repositórios digitais, a fim de garantir que os materiais armazenados permanecerão autênticos em logo prazo (MÁRDERO ARELLANO, 2008). Neste sentido, a infraestrutura geral será um componente-chave apoiando a confiabilidade e a sustentabilidade do repositório digital, conquistando a confiança das comunidades-alvo (THOMAZ, 2007).

Outro aspecto a ser considerado é a interoperabilidade das fermentas de gestão e preservação, associada às políticas e ao plano de preservação são artifícios que corroboram para o desenvolvimento de um repositório arquivístico digital confiável, e será fundamental para as ações em longo prazo. Essa mesma interoperabilidade é mais um desafio para o preservador, e deverá ser considerada antes de qualquer implementação. Isto realça a necessidade de usar tecnologias livres, as quais se possam ter acesso ao seu código fonte para compreender o seu funcionamento interno e permitir o desenvolvimento de sistema interoperáveis.

Mas além de se estabelecer os parâmetros a serem seguidos é preciso uma comprovação que garanta a veracidade dos serviços que estão sendo oferecidos.

> Para as organizações que tencionam fornecer serviços de repositório digital, o desenvolvimento da desejável confiança via práticas confiáveis, comprovadas, levará algum tempo. Entretanto, tendo em vista que ações imediatas para preservar o já extenso corpo de materiais digitais precisam ser tomadas, um programa de certificação seria recomendável para fornecer uma base de confiança. A certificação especificaria os critérios a serem atingidos e empregaria mecanismos para sua avaliação e medição. [...] A certificação, periodicamente atendida ao longo de diversos anos, poderia solucionar a tensão entre a necessidade imediata de arquivos confiáveis e a necessidade de desenvolver e comprovar a confiabilidade ao longo do tempo (THOMAZ, 2007, p. 88).

A plena confiança tão esperada pelos consumidores somente será atingida com o passar dos anos, entretanto, podem-se realizar certificações periódicas que comprovem a eficácia dos serviços de preservação digital. As ações de certificação por sua vez, avaliam um determinado período de tempo, a partir deste é necessária uma nova certificação e assim consecutivamente a fim de demonstrar confiabilidade.

Dentre os fatores que corroboram para o estabelecimento de um repositório digital confiável, destacam-se os seguintes aspectos: definição de políticas institucionais; garantia de recursos financeiros em longo prazo; escolha das estratégias de preservação digital; conformidade do repositório com o modelo OAIS; custódia confiável ininterrupta dos documentos durante todo o ciclo de vida; interoperabilidade entre as tecnologias de gestão, preservação e acesso; adoção de padrões de metadados; presença de profissionais qualificados e tecnologias apropriadas para a preservação; verificação das normas e práticas recomendadas pela comunidade de preservação digital; verificação da eficácia de suas ferramentas; e divulgação dos métodos de preservação e custódia ao público alvo a fim de gerar confiança. Além destes, o desenvolvimento de manuais e recomendações no âmbito interno do repositório é fundamental para registrar os métodos testados que

corroboram ou não de forma eficaz para a preservação. Estes registros produzidos pelo próprio repositório, o qual pode ser denominado como "relatórios de atividades", ao serem compartilhados poderão impulsionar novos estudos sobre as soluções bem como sobre os problemas encontrados gerando um produto de retroalimentação, como por exemplo, um artigo que discute as práticas com repositórios digitais em uma determinada instituição.

Em linhas gerais, seguir padrões facilita o entendimento e a troca de conhecimentos entre as comunidades científicas, da mesma forma que a divulgação de suas práticas torna-se relevante para novos estudos. Considerando que o modelo OAIS é uma referência em preservação digital em nível mundial, o seu estudo torna-se fundamental na comunidade arquivística. Além disso, métodos para a auditoria e certificação dos repositórios que verifiquem a sua conformidade com o modelo OAIS, bem como o comprometimento da instituição com as práticas de preservação digital.

6 Auditoria e certificação de repositórios digitais confiáveis

O processo de auditoria consiste em verificar e avaliar as metodologias adotadas pela instituição. Desta forma, é possível verificar a conformidade do repositório digital em relação às normas e o comprometimento com as ações de preservação digital no que tange a infraestrutura física, técnica e tecnológica. Posteriormente a realização da auditoria, procede-se a análise e interpretação dos dados do levantamento, com base nestes, é possível avaliar o grau de confiabilidade do repositório digital concedendo ou não a certificação de repositório digital confiável.

Existem algumas iniciativas que propõe recomendações para realizar auditoria, dentre elas: *Trustworthy Repository Audit & Certification: Criteria and Checklist* (TRAC), *Audit And Certification of Trustworthy Digital Repositories* (ACTDR), *Catalogue of Criteria for Trusted Digital Repositories* da *Network of Expertise in long-term STORage* (NESTOR) e *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA).

6.1 TRAC

Um repositório digital confiável deve oferecer estratégias de segurança para os documentos armazenados, além disso, deverá garantir que estes documentos são fidedignos e que permanecerão seguros em longo prazo (RESEARCH LIBRARIES GROUP. ONLINE COMPUTER LIBRARY CENTER - RLG/OCLC, 2002). Desta forma, para adicionar confiabilidade aos repositórios digitais é preciso seguir rotinas de auditoria e certificação.

A definição do grau de confiabilidade dos repositórios digitais pode seguir recomendações do TRAC. Conforme o documento, estas são as principais características devem estar presentes no repositório digital para

que este seja considerado confiável. A comprovação da existência destas características, pode se dar pelas ações de certificação, que nos dias de hoje são fundamentais para os repositórios digitais.

O TRAC apresenta um conjunto de critérios usados como referência para a certificação de repositórios digitais, oferecendo ferramentas para auditoria, avaliação e certificação potencial de repositórios, além de estabelecer a documentação exigida para a auditoria. Através do TRAC pode-se esquematizar um processo de certificação, e estabelecer metodologias adequadas para determinar a base e a sustentabilidade dos repositórios digitais (SAYÃO, 2010). O TRAC tem por objetivos desenvolver critérios para identificar os repositórios digitais capazes de realizar, o armazenamento, a migração e promover o acesso aos documentos digitais forma confiável. O desafio tem sido produzir critérios de certificação e delinear um processo de certificação aplicável a uma gama de repositórios digitais (RLG/NARA, 2007). Os critérios definidos no TRAC foram base para o desenvolvimento do ACTDR que é outro documento que auxilia a auditoria e certificação de repositórios digitais.

6.2 ACTDR

Tem por objetivo definir recomendações práticas em conformidade com o modelo de referência OAIS, para fundamentar um processo de auditoria e certificação, a fim de avaliar a confiabilidade de qualquer repositório digital. É um documento destinado principalmente para os administradores que buscam adicionar confiabilidade aos repositórios digitais, bem como aos profissionais que realizam o serviço de auditoria (CCSDS, 2011). Através desta recomendação é possível avaliar o repositório digital com relação à infraestrutura organizacional, sustentabilidade financeira, gerenciamento dos objetos digitais e gestão de riscos.

Esta prática recomendada define um processo de auditoria e certificação para avaliar a confiabilidade dos repositórios digitais, é equivalente a ISO: 16363 (CCSDS, 2011).

6.3 NESTOR

Consiste em um catálogo de critérios atuais o qual é destinado principalmente a organizações de memória (arquivos, bibliotecas e museus), atuando como um manual para a elaboração, planejamento e implementação de um repositório digital confiável em longo prazo. Este catálogo é destinado a fornecer orientação a todas as instituições no âmbito da administração de arquivos, prestadores de serviços comerciais e não comerciais, e de serviços de terceiros (NESTOR, 2006).

O NESTOR CRITERIA foi publicado em dezembro de 2006 pelo *nestor Working Group Trusted Repositories – Certification*. Seu objetivo inicial era realizar a sua implementação na Alemanha, entretanto, já é discutido e padronizado internacionalmente.

6.4 DRAMBORA

É um conjunto de ferramentas para auditoria de repositórios digitais, destinado a facilitar a auditoria interna. O DRAMBORA fornece aos administradores do repositório a possibilidade de avaliar as suas qualidades, identificar os seus pontos fracos, e reconhecer seus pontos fortes (DCC/DPE, 2007).

O DRAMBORA surgiu a partir da união de esforços entre *Digital Curation Centre* (DCC) e *DigitalPreservationEurope* (DPE), formando o grupo de trabalho DCC/DPE. A estrutura do DRAMBORA consiste em apresentar métodos e ferramentas para auditoria, identificar o contexto organizacional, identificar e avaliar os riscos, definir a gestão de riscos. Além de apresentar métodos para a interpretação dos resultados da auditoria.

6.5 Considerações sobre auditoria e certificação

Em linhas gerais, entende-se que para adicionar confiabilidade a um repositório digital, este deve ser baseado no modelo OAIS e estar em conformidade com os requisitos apresentados por TRAC, ACTDR, NESTOR ou DRAMBORA.

A sincronia entre o repositório e as recomendações para auditoria e certificação proporcionará um ambiente confiável para a preservação em longo prazo. Deve-se destacar que cada recomendação possui suas características, então, haverá variações com relação ao número de critérios. Desta forma, os critérios destas recomendações vêm como um complemento ao repositório digital, assim, a sua conformidade resulta em confiabilidade: o repositório digital confiável para preservação de documentos arquivísticos.

7 Considerações finais

Este artigo realizou uma reflexão sobre questões pertinentes a preservação digital, dando ênfase à discussão dos repositórios digitais confiáveis para documentos arquivísticos. Desta forma, buscaram-se realçar questões relativas às políticas institucionais, a custódia confiável e os métodos para comprovar a confiabilidade dos repositórios digitais.

Para preservar os documentos digitais de uma instituição é preciso planejamento, ou seja, inicialmente devem ser definidas as políticas de preservação digital. Neste momento devem ser consideradas as normas, as recomendações, os padrões utilizados e outras iniciativas de preservação. Todo o planejamento inicial servirá de base para a sustentação da confiabilidade e garantia da longevidade do repositório digital.

De forma geral, o documento, a informação e o conhecimento assumem níveis de credibilidade, estes níveis variam de acordo com a confiabilidade de suas fontes. No caso da preservação de documentos arquivísticos digitais, a ausência de confiabilidade poderá resultar em

dúvidas quanto à integridade e autenticidade dos materiais custodiados. Desta forma, considerando que os documentos arquivísticos tem função probatória e informativa, a perda de sua confiabilidade implica na perda do sentido da existência destes documentos. Por estas razões, os sistemas de gestão e preservação devem oferecer mecanismos para verificação constante de sua integridade e autenticidade, o que irá gerar confiança ao público alvo.

A custódia confiável torna-se um requisito para a preservação em longo prazo, isto implica produzir, armazenar, tramitar e recolher/transferir os documentos por meio de um sistema de gestão confiável tendo como destino um sistema de preservação confiável. Neste ponto, chama-se a atenção para interoperabilidade entre estas tecnologias. Nas atividades de preservação do repositório digital, destaca-se a conformidade com o modelo OAIS como um forte atributo na busca da confiabilidade. Além disso, as ações de auditoria e certificação surgem para auxiliar na busca da confiabilidade, desta forma, as sucessivas certificações vão adicionar confiabilidade ao repositório digital.

Em linhas gerais, este artigo corrobora para o aprofundamento dos estudos sobre confiabilidade, tanto nos sistemas de preservação quanto nos sistema de gestão. Ao abordar a preservação de longo prazo em repositórios digitais confiáveis, deve-se salientar a necessidade de realizar auditorias e proceder à certificação periódica do repositório. A confiabilidade é demonstrada na medida em que as políticas de preservação digital contemplam os requisitos arquivísticos e diplomáticos.

Referências

BELLOTTO, H. L. *Arquivos permanentes:* tratamento documental. 4. Ed. Rio de Janeiro: Fundação Getúlio Vargas, 2006.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de documentos eletrônicos. *Carta para a Preservação do Patrimônio Arquivístico Digital*. Rio de Janeiro: Arquivo Nacional, 2004a. Disponível em: <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf>. Acesso em: 10 ago. 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de documentos eletrônicos. *Gestão Arquivística de Documentos Eletrônicos.* Rio de Janeiro: Arquivo Nacional, 2004b. Disponível em: <http://pt.scribd.com/doc/37174068/Gestao-Arquivistica-de-Documentos-Eletronicos-CONARQ-Por-Claudia-Rocha>. Acesso em: 9 jul. 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). 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.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de documentos eletrônicos. *Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais.* Rio de Janeiro: Arquivo Nacional, 2012. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/diretrizes_presuncao_autenticidade_publicada.pdf>. Acesso em: 20 jun. 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de documentos eletrônicos. *Diretrizes para a implementação de repositórios digitais confiáveis de documentos arquivísticos*. Rio de Janeiro: Arquivo Nacional, 2014. Disponível em: <http://www.conarq.arquivonacional.gov.br/media/publicacoes/resol_conarq_39_repositorios.pdf>. Acesso em: 13 ago. 2014.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). *Reference model for an open archival information system (OAIS)*. Blue Book. Washington, Jan. 2002. Disponível em: <http://public.ccsds.org/publications/archive/650x0b1.pdf>. Acesso em: 28 mai. 2014.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). *Audit and certification of trustworthy digital repositories (ACTDR)*. Magenta Book. Washington, Sep. 2011. Disponível em: <http://public.ccsds.org/publications/archive/652x0m1.pdf>. Acesso em: 13 nov. 2014.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). *Reference model for an open archival information system (OAIS).* Magenta Book. Washington, Jun. 2012. Disponível em: <http://public.ccsds.org/publications/archive/650x0m2.pdf>. Acesso em: 13 maio 2014.

CORRÊA, A. M. G. *Preservação digital:* autenticidade e integridade de documentos em bibliotecas digitais de teses e dissertações. 2010. 96f. Dissertação (Mestrado em Ciência da Informação) - Universidade de São Paulo, São Paulo, 2010. Disponível em: <http://www.teses.usp.br/teses/disponiveis/27/27151/tde-05112010-105831/pt-br.php>. Acesso em: 3 jul. 2014.

DE SORDI, J. O. *Administração da informação:* fundamentos e práticas para uma nova gestão do conhecimento. São Paulo: SARAIVA, 2008.

DIGITAL CURATION CENTRE. DIGITAL PRESERVATION EUROPE (DCC/DPE). *Digital repository audit method based on risk assessment (DRAMBORA).* v. 1.0, Feb 2007. Disponível em: <http://www.repositoryaudit.eu/download>. Acesso em: 13 nov. 2014.

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 ago. 2014.

HEDSTROM, M. Digital preservation: a time bomb for digital libraries. *Computer and the humanities*, Netherlands, n. 31, p. 189-202, 1998. Disponível em: <http://deepblue.lib.umich.edu/bitstream/2027.42/42573/1/10579_2004_Article_153071.pdf>. Acesso em: 01 out. 2014.

HEDSTROM, M. *Digital preservation*: problems and prospects. University of Michigan, USA, 2001. Disponível em: <http://www.dl.slis.tsukuba.ac.jp/DLjournal/No_20/1-hedstrom/1-hedstrom.html >. Acesso em: 10 jan. 2015.

HEMINGER, A. R; ROBERTSON, S. B. The Digital Rosetta Stone: a model for maintaining long-term access to static digital documents. *Communications of AIS,* v. 3, article 2, Jan. 2000. Disponível em: <http://delivery.acm.org/>. Acesso em: 24 set. 2014.

INNARELLI, H. C. *Instrumenta 2:* preservação de documentos digitais. São Paulo: ARQ-SP, 2012.

INNARELLI, H. C. Preservação digital e seus dez mandamentos. *In:* SANTOS, Vanderlei Batista (Org.). *Arquivística*: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. Distrito Federal: SENAC, 2007. p. 21-75.

INNARELLI, H. C. Preservação digital: a influência da gestão dos documentos digitais na preservação da informação e da cultura. *Revista Digital de Biblioteconomia e Ciência da Informação*, Campinas, v. 8, n. 2, p. 72-87, jan./jun. 2011. Disponível em: <http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/view/487/330>. Acesso em: 7 jul. 2014.

INTERPARES. Interpares 2 Project. *Diretrizes do Preservador*: a preservação de documentos arquivísticos digitais: diretrizes para organizações. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. 2002-2007a. Disponível em: <http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf>. Acesso em: 9 ago. 2014.

INTERPARES. Interpares 2 Project. *Diretrizes do Produtor*: a elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. TEAM Brasil. Tradução: Arquivo Nacional e Câmara dos Deputados. 2002-2007b. Disponível em: <http://www.interpares.org/ip2/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf>. Acesso em: 9 ago. 2014.

LOPES, L. C. *A gestão da informação:* as organizações, os arquivos e a informação aplicada. Rio de Janeiro: Arquivo Público do Estado do Rio de Janeiro. 1997.

LOPES, V. *Preservação Digital*. Portugal: Universidade do Minho, Guimarães, 2008. Disponível em: <http://www.vitorlopes.com/Trabalhos/Preservacao_Digital-Vitor_Lopes.pdf>. Acesso em: 28 ago. 2012.

MÁRDERO ARELLANO, M. Á. *Critérios para a preservação digital da informação científica*. 354f. Tese (Doutorado em Ciência da Informação) - Universidade Federal de Brasília, Departamento de Ciência da Informação, 2008. Disponível em: <http://bdtd.bce.unb.br/tedesimplificado/tde_busca/arquivo.php?codArquivo=4547>. Acesso em: 15 jun. 2014.

NETWORK OF EXPERTISE IN LONG-TERM STORAGE (NESTOR). Nestor Working Group on Trusted Repositories Certification. *Catalogue of Criteria for Trusted Digital Repositories*. Version 1 (draft for public comment). Frankfurt am Main: Jun 2006. Nestor c/o Deutsche Nationalbibliothek. Disponível em: <http://files.d-nb.de/nestor/materialien/nestor_mat_08-eng.pdf>. Acesso em: 13 nov. 2014.

RESEARCH LIBRARIES GROUP. ONLINE COMPUTER LIBRARY CENTER (RLG/OCLC). *Trusted digital repositories*: attributes and responsibilities. Mountain View, CA. : RLG, OCLC, 2002. Disponível em: <http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf>. Acesso em: 8 set. 2014.

RESEARCH LIBRARIES GROUP. U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (RLG/NARA). *Trustworthy repositories audit & certification.* RLG, OCLC, Feb. 2007. Disponível em: <http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf>. Acesso em: 8 set. 2014.

ROCHA, C. L.; SILVA, M. da. Padrões para garantir a preservação e o acesso aos documentos digitais. *Acervo*, Rio de Janeiro, v. 20, n. 1-2, p. 113-124, jan/dez 2007. Disponível em: <http://www.revistaacervo.an.gov.br/seer/index.php/info/article/view/142>. Acesso em: 7 set. 2014.

RONDINELLI, R. C. *Gerenciamento arquivístico de documentos eletrônicos*: uma abordagem teórica da diplomática arquivística contemporânea. 4. ed. Rio de Janeiro: Editora FGV, 2005.

RONDINELLI, R. C. *O documento arquivístico ante a realidade digital*: uma revisão conceitual necessária. Rio de janeiro: Editora FGV, 2013.

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

SARAMAGO, M. de L. Metadados para preservação digital e aplicação do modelo OAIS. *In:* CONGRESSO NACIONAL DE BIBLIOTECARIOS, ARQUIVISTAS E DOCUMENTALISTAS, 8., 2004, Estoril. *Anais...* Disponível em: <http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/640/637>. Acesso em: 4 jul. 2014.

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.

SAYÃO, L. F. Repositórios digitais confiáveis para a preservação de periódicos eletrônicos científicos. *Ponto de Acesso*, Salvador, v. 4, n. 3, p. 68-94, dez. 2010. Disponível em: <http://www.portalseer.ufba.br/index.php/revistaici/article/view/4709/3565>. Acesso em: 8 ago. 2014.

SCHELLENBERG, T. R. *Arquivos modernos*: princípios e técnicas. 6. ed. Rio de Janeiro: Editora FGV, 2006.

SILVA, E. L. da; MENEZES, E. M. *Metodologia da pesquisa e elaboração de dissertação*. 4. ed. rev. atual. Florianópolis: UFSC, 2005. Disponível em: <https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf>. Acesso em: 13 jun. 2014.

SOUSA, R. T. B. de. A classificação como função matricial do que-fazer arquivístico. *In:* SANTOS, V. B. dos. *Arquivística*: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. Brasília: SENAC, 2007. p. 79-163.

SOUSA, R. T. B. de. Em busca de um instrumental teórico-metodológico para a construção de instrumentos de classificação de documentos de arquivo. *In:* BARTALO, L.; MORENO, N. A. (Orgs.). *Gestão em arquivologia*: abordagens múltiplas. Londrina: EDUEL, 2008. p. 11-52.

SWEDEN. National Archives. *Digital preservation in archives*: overview of current research and practices. Sweden: January 2004 - February 2005. Disponível em: <http://www.ltu.se/cms_fs/1.83844!/file/Digital%20Preservation%20in%20Archives.pdf>. Acesso em: 15 fev. 2015.

THOMAZ, K. de P. *A preservação de documentos eletrônicos de caráter arquivístico*: novos desafios, velhos problemas. 2004. 389f. Tese (Doutorado em Ciência da Informação) - Escola de Ciência da Informação. Universidade Federal de Minas Gerais, 2004. Disponível em: <http://www.bibliotecadigital.ufmg.br/dspace/bitstream/handle/1843/VALA-68ZRKF/doutorado___katia_de_padua_thomaz.pdf>. Acesso em: 28 jul. 2014.

THOMAZ, K. de P. Documentos eletrônicos de caráter arquivístico: fatores condicionantes da preservação. *Perspectivas em Ciência da Informação*, Belo Horizonte, v. 10, n. 1, p. 34-53, jan./jun. 2005. Disponível em: <www.brapci.ufpr.br/download.php?dd0=13204>. Acesso em: 7 set. 2014.

THOMAZ, K. de P. Gestão e preservação de documentos eletrônicos de arquivo: revisão de literatura – parte 2. *Arquivística.net*, Rio de Janeiro, v. 2, n. 1, p. 114-131, jan./.jun. 2006. Disponível em: <www.brapci.ufpr.br/download.php?dd0=6733>. Acesso em: 7 set. 2014.

THOMAZ, K. de P. Repositórios digitais confiáveis e certificação. *Arquivística.net*, Rio de janeiro, v. 3, n. 1, p. 80-89, jan./jun. 2007. Disponível em: <http://www.brapci.inf.br/_repositorio/2010/05/pdf_fed0720dbb_0010726.pdf>. Acesso em: 7 set. 2014.