REPOSITÓRIOS PARA A PRESERVAÇÃO DE DOCUMENTOS ARQUIVÍSTICOS DIGITAIS

REPOSITORIES FOR THE PRESERVATION OF DIGITAL RECORDS

Claudia Lacombe Rocha | Mestre em Informática, pelo Núcleo de Computação Eletrônica da Universidade Federal do Rio do Janeiro; supervisora da equipe de documentos digitais e coordenadora do Programa Permanente de Preservação e Acesso a Documentos Digitais do Arquivo Nacional; presidente da Câmara Técnica de Documentos Eletrônicos do Conarq; membro do Projeto InterPARES Trust.

RESUMO

Os documentos arquivísticos digitais são uma importante fonte para as iniciativas de transparência e informação pública. Por isso precisam ser mantidos e preservados de forma a garantir sua confiabilidade, precisão, autenticidade e acessibilidade. Nesse sentido, é fundamental que sejam mantidos em repositórios digitais confiáveis, projetados de forma a cumprir com as normas e práticas arquivísticas.

Palavras-chave: documentos arquivísticos; confiabilidade; repositórios digitais confiáveis; repositórios digitais arquivísticos.

ABSTRACT

Digital records are an important source for initiatives related to transparency and access to public information. Hence, they need to be maintained and preserved so as to guarantee their reliability, accuracy, authenticity and accessibility. In this regard, it is essential that records are kept in trusted digital repositories, designed to comply with archival standards and practices.

Keywords: records; trustworthiness; trustworthy digital repositories; digital archival repositories.

RESUMEN

Los documentos archivísticos digitales son una fuente importante para las iniciativas de transparencia e información públicas. Por lo tanto, deben ser mantenidos y conservados de manera a garantir su fiabilidad, exactitud, autenticidad y accesibilidad. Es esencial que se mantengan en repositorios digitales fiables, diseñados para cumplir con las normas y prácticas archivísticas.

Palabras clave: documentos archivísticos; fiabilidad; repositorios digitales fiables; repositorios digitales archivísticos.

CONTEXTO

As iniciativas governamentais de transparência da gestão pública e de acesso à informação são estreitamente vinculadas e dependentes da gestão de documentos. É importante reconhecer que os documentos arquivísticos são a principal fonte de informação a respeito das atividades governamentais e que, para assegurar o valor da informação disponibilizada pelos governos, é necessário produzir e manter *documentos confiáveis, precisos, autênticos e acessíveis*. Assim, as autoridades arquivísticas devem desempenhar um papel-chave nas iniciativas de acesso à informação, de maneira que se possa assegurar o fornecimento de informação confiável tanto para o governo como para os cidadãos.

É igualmente importante considerar que, com o avanço do governo eletrônico e, sobretudo, com o desenvolvimento de projetos "zero papel" em diversos países, cada vez mais as atividades governamentais estão sendo registradas em formato digital. A produção de documentos digitais é crescente e diversificada, e aumentam as bases de dados que são consideradas como documentos arquivísticos.

Dessa maneira, iniciativas de "dados abertos" ou a publicação de informações do governo na internet, no contexto de transparência governamental, dependem da gestão eficiente dos documentos arquivísticos digitais. Eles precisam permanecer autênticos, acessíveis e utilizáveis. Nunca é demais lembrar que a gestão dos documentos digitais é mais complexa que a dos não digitais, uma vez que é necessário fazer frente às várias ameaças que decorrem da fragilidade inerente aos suportes digitais, da facilidade de manipulação e da rápida obsolescência tecnológica.

Surge então uma grande questão: *Como manter estes documentos?* Existe um consenso entre os especialistas na área de preservação digital de que a gestão, a preservação e a recuperação destes documentos requerem *sistemas de informação confiáveis e repositórios digitais confiáveis* (Sayão, 2010).

Com relação aos sistemas de informação voltados para a gestão de documentos arquivísticos digitais, já na década de 1990 apontava-se a necessidade de especificar requisitos para tais sistemas, com ênfase nos procedimentos de gestão documental.[1] Os primeiros documentos que surgiram com este foco foram a norma DoD 5015.2[2] (*Design criteria standard*

1 Em 1996, na primeira reunião do DLM Forum, entidade criada no âmbito da União Europeia para fomentar a cooperação no campo dos documentos eletrônicos, foi apontada a necessidade de especificar os requisitos para sistemas de gestão de documentos digitais.

2 O Departamento de Defesa dos Estados Unidos – DoD participou de um projeto de pesquisa realizado na Universidade de British Columbia (A proteção da integridade dos documentos eletrônicos: 1994-1997), com a finalidade de definir requisitos para garantir a confiabilidade e a autenticidade dos documentos arquivísticos em seus sistemas eletrônicos. Como resultado dessa parceria, foi desenvolvida a norma DoD 5015.2, que estabeleceu requisitos funcionais para a aquisição de aplicações de software de gestão de documentos. A primeira versão foi publicada em 1997 e o documento passou por diversas revisões e ampliações; foi incorporado pela administração pública federal norte-americana e se tornou um padrão de importância nacional e internacional.

for electronic records management software aplications – 5015.2 STD) e o MoReq[3] (Modelo de Requisitos para a gestão de arquivos eletrônicos). No Brasil, a Câmara Técnica de Documentos Eletrônicos (CTDE), do Conselho Nacional de Arquivos (Conarq), apresentou em 2006 a primeira versão do e-ARQ Brasil – Modelo de Requisitos para sistemas informatizados de gestão arquivística de documentos. O documento foi elaborado a partir do MoReq e da norma DoD 5015.2, sendo adaptado à prática arquivística e legislação brasileiras. O e-ARQ Brasil ressalta a importância do produtor de documentos ter uma política de gestão documental instituída e um programa de gestão de documentos estabelecido, com distribuição de responsabilidades, definição de procedimentos e elaboração dos instrumentos básicos da gestão: plano ou código de classificação de documentos e tabela de temporalidade e destinação de documentos.

Com relação aos repositórios digitais confiáveis, os primeiros documentos que tratam do tema datam também do mesmo período. Em todos fica claro que a preservação e o acesso de longo prazo aos documentos digitais não é um problema meramente tecnológico. As normas e diretrizes que orientam o desenvolvimento e a implementação de repositórios digitais confiáveis ressaltaram a importância dos aspectos organizativos, políticos e de gestão. Este artigo buscará detalhar o que foi tratado nesses documentos.

Inicialmente, irá se esclarecer a compreensão do que é um repositório digital, em seguida serão elencados os requisitos apontados nestes documentos internacionais para que um repositório seja considerado confiável, e salientadas as peculiaridades da gestão de documentos arquivísticos em um repositório. Ao final, serão indicadas algumas responsabilidades e o papel dos arquivistas e das autoridades arquivísticas neste cenário.

REPOSITÓRIOS DIGITAIS

Primeiramente, é necessário esclarecer o que se entende por repositório digital, visto que não se trata de um simples armazém de documentos. Na literatura sobre o tema, existem várias definições para repositório digital, que ressaltam seus diferentes aspectos: o sistema informatizado, os serviços que são oferecidos ou mesmo a coleção de objetos de informação. Vejamos algumas delas: "Sistema informatizado para armazenar coleções de uma biblioteca digital e distribuí-la aos usuários" (<www.cs.cornell.edu/wya/DigLib/MS1999/glossary.htm>); "Repositórios digitais são coleções de informação digital, que pode ser construída de diferentes maneiras e para diferentes propósitos" (Martins, 2008); "um conjunto de serviços que a instituição oferece aos membros de sua comunidade para a gestão e difusão da produção técnica e científica nos meios digitais" (Lynch; Lippincott, 2005).

3 Em 1996, como resultado da reunião do DLM Forum, foi criado um grupo de trabalho que elaborou um modelo de requisitos genérico, para toda a União Europeia, publicado em 2002, que ficou conhecido por MoReq. O documento define os requisitos que um sistema de gestão de documentos deve ter para garantir a gestão adequada, o acesso contínuo, e a retenção dos documentos pelo tempo necessário e a sua destinação.

O entendimento de repositório que se vai adotar aqui cumpre com todos esses aspectos. Assim, repositório digital será entendido como um ambiente tecnológico complexo para o armazenamento e a gestão de materiais digitais. Este ambiente é composto por uma solução informatizada na qual se captura, armazena, preserva e se provê acesso aos objetos de informação digitais. Um repositório digital é, então, um complexo formado por elementos de hardware (dispositivos de armazenamento), software, serviços, coleção de informação digital e metadados associados a esses objetos de informação. Todo este conjunto tem como objetivo apoiar a gestão de materiais digitais pelo tempo que seja necessário.

Um repositório, ou seja, todo esse ambiente, pode ser utilizado em diversas situações, incluindo a área de arquivos e outras áreas de gestão de informação: arquivo de documentação corrente (associado a um sistema de gestão documental), arquivo permanente, biblioteca digital, coleção de obras de arte digital, coleção de áudio e vídeo digital, curadoria de dados de pesquisa digitais etc.

REPOSITÓRIOS DIGITAIS CONFIÁVEIS

A fragilidade dos suportes digitais, os ciclos de obsolescência cada vez menores e a dificuldade de se provar a autenticidade dos documentos digitais apontam a necessidade de repositórios digitais *confiáveis*.

O que é um repositório digital confiável? É aquele capaz de manter autênticos os objetos de informação digital, de preservá-los e de dar acesso a eles pelo tempo necessário (RLG/OCLC, 2002).

Motivados por esta preocupação em se garantir a preservação e o acesso de objetos de informação autênticos, formaram-se grupos de trabalho internacionais de especialistas, que tiveram o objetivo de orientar a modelagem e a implementação de repositórios digitais, bem como de assinalar os requisitos para avaliar sua confiabilidade. A seguir, serão referidos alguns documentos importantes que resultaram dessas iniciativas.

O conceito de repositório digital confiável surgiu em um documento base, preparado por um grupo de trabalho liderado pelo Research Library Group (RLG) e o Online Computer Library Center (OCLC),[4] intitulado *Trusted Digital Repositories*: Atributes and Responsabilities (*Repositórios digitais confiáveis*: atributos e responsabilidades). Este documento propôs as bases conceituais para repositórios digitais confiáveis e estabeleceu os atributos e as responsabilidades que estes devem assumir. Também apresentou um importante debate sobre como criar novamente, em um ambiente instável como a internet, a ideia tradicional de *confiança*, que é um princípio fundamental nas instituições arquivísticas.

De acordo com esse grupo de trabalho, "um repositório digital confiável é aquele que tem como missão fornecer acesso confiável a longo prazo aos recursos digitais à sua comuni-

4 Desde junho de 2006, o RLG e o OCLC estão reunidos em uma só organização. Para obter mais informações, consulte o sítio web: <http://www.oclc.org/>.

dade designada, agora e no futuro" e deve cumprir com os seguintes atributos: cumprimento com o modelo de referência Oais; responsabilidade administrativa; viabilidade organizacional; suporte financeiro; adequação tecnológica; sistema de segurança; procedimentos transparentes para prestação de contas do próprio repositório (RLG/OCLC, 2002).

Convém evidenciar que o primeiro atributo apontado é o cumprimento com o modelo Oais, uma das normas mais importantes no que diz respeito à preservação digital e a repositórios digitais. O modelo Oais foi desenvolvido sob a coordenação do Comitê Consultivo para Sistemas de Dados Espaciais (CCSDS) da Nasa, que contou com a colaboração da comunidade científica internacional. Sua elaboração levou dez anos. Uma primeira versão foi publicada em 1999, outra em 2002 e em 2003 transformou-se na norma ISO 14721:2003.[5] O Oais é um modelo conceitual que descreve um modelo funcional e um modelo de informação para a preservação e o acesso aos materiais digitais administrados pelo repositório.

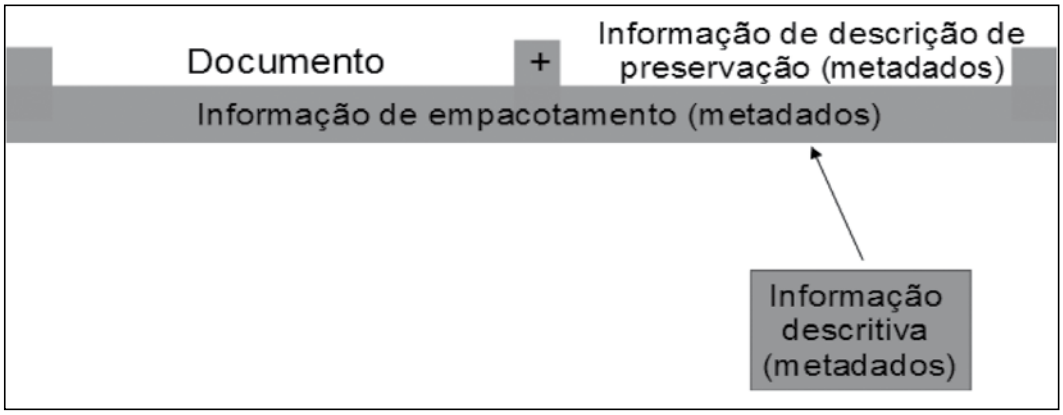
De acordo com o modelo Oais, as funcionalidades de um repositório devem estar organizadas em seis grandes grupos: a admissão (*ingest*), o armazenamento, a gestão de dados, o planejamento da preservação, a administração e o acesso. As funcionalidades de cada grupo são detalhadas no modelo funcional e podem ser acessadas por três tipos de agentes: produtores (pessoas ou sistemas que depositam os objetos digitais no repositório), consumidores (pessoas ou sistemas que interagem com o Oais para acessar os objetos digitais) e administradores (responsáveis pelo estabelecimento das políticas e pela gestão dos objetos digitais preservados). A figura 1 a seguir representa o modelo conceitual do Oais, com as funcionalidades, agentes e pacotes de informação.

Figura 1 – Modelo Oais

5 No Brasil, a norma ISO do modelo Oais foi traduzida e publicada pela Associação Brasileira de Normas Técnicas (ABNT) como NBR 15425: Modelo de referência para um sistema aberto de arquivamento de informação (Saai).

No modelo de informação é definida a formação de pacotes de informação, que atuam como um recipiente conceitual. Um pacote de informação é composto por informação de conteúdo (o documento) e informação de descrição de preservação (metadados necessários para apoiar a preservação e acesso do documento no longo prazo), que são encapsuladas e identificadas pela informação de empacotamento. Ao pacote de informação são, ainda, associadas as informações descritivas do pacote (metadados descritivos que possibilitam a localização do pacote no repositório).

Figura 2 – Pacote de informação do modelo Oais



Dando seguimento a estas iniciativas, a RLG se associou ao National Archives and Records Administration (Nara) – Arquivo Nacional dos Estados Unidos –, com o objetivo de estabelecer critérios para a certificação de repositórios confiáveis, em consonância com o relatório *Repositórios digitais confiáveis*: atributos e responsabilidades, de 2002, e com o modelo Oais. Assim, foi publicado em 2007 o documento *Trustworthy Repository Audit & Certification*: Criteria and Checklist, também conhecido pela sigla Trac, que apresenta um conjunto de critérios e um *ckecklist* para serem tomados como referência para a certificação de repositórios digitais confiáveis. Este documento serviu como base para o desenvolvimento da norma ISO 16363: 2012.

O Trac deixa claro que a gestão é a base de um repositório digital confiável. Conforme será analisado a seguir, a autenticidade dos documentos não pode ser baseada unicamente em recursos tecnológicos, pois é necessário associar as soluções tecnológicas a políticas, procedimentos e informação (na forma de metadados).

A primeira série de requisitos e critérios que são apresentados se refere à infraestrutura organizacional do repositório, ou melhor, da instituição que desempenha este papel. Já de início, é apontado que o repositório deve ter clara vocação com a preservação, a gestão e o acesso de longo prazo aos objetos de informação que lhes são confiados, que no caso dos arquivos são os documentos arquivísticos digitais. Ao longo da história, de diferentes

modos as instituições arquivísticas têm demonstrado claramente esta vocação. De acordo com Duranti, desde a antiguidade os arquivos são tidos como o local oficial de guarda e preservação dos documentos. Na Roma Antiga, o Código Justiniano definia o arquivo como o lugar público onde os documentos são depositados de maneira que se conservem incorruptos, forneçam evidencia confiável e permaneçam como memória daquilo que atestam.[6] Nas monarquias da era moderna, os prédios de arquivo situavam-se no coração das cidades e eram vistos como lugares públicos onde o registro documental das atividades era mantido e protegido. A Revolução Francesa, em 1789, inaugurou uma nova visão de arquivo, transformando-o em patrimônio da nação e acessível aos cidadãos, mas mesmo esse "novo" arquivo permaneceu como o local oficial de guarda e preservação dos documentos, que lhes dá credibilidade e atesta sua autenticidade (Duranti, 1996).

Ainda no tocante à infraestrutura, os requisitos apresentados no Trac indicam que o repositório deve contar com políticas, procedimentos e desempenho mensuráveis e auditáveis. Esta é uma maneira de demonstrar à sua comunidade de usuários que pode ser considerado um custodiador confiável.[7] O repositório deve, também, demonstrar sustentabilidade e viabilidade de longo prazo, do ponto de vista dos recursos organizacionais, financeiros e humanos. Assim, deve contar com uma equipe de profissionais qualificados e em número suficiente, ter um plano de gestão financeira transparente e ser capaz de obter recursos financeiros contínuos e estáveis, bem como ter um plano formal de sucessão, para assegurar a continuidade do serviço, no caso de deixar de funcionar ou da instituição responsável mudar de âmbito de atuação.

Também é necessário demonstrar que os sistemas cumprem com as expectativas de confiabilidade da comunidade de usuários (produtores e consumidores) e as necessidades específicas desta comunidade são atendidas pelo repositório. Essas necessidades podem estar, por exemplo, relacionadas a prazos de retenção, formas de acesso, formatos de arquivo, tamanho de arquivos e podem resultar da necessidade de satisfazer requisitos de acesso para usuários com deficiência visual ou que requeiram uma apresentação de qualidade superior.

Para finalizar a primeira série de requisitos, o repositório deve realizar o planejamento da preservação dos documentos sob sua custódia para fazer frente aos problemas colocados pela obsolescência tecnológica e fragilidade dos suportes. Este planejamento deve ser feito

---

6 Conforme o texto de Luciana Duranti (1996), "In the justinian code, which is the *summa* for all Roman law and jurisprudence, an archives is defined as *locus publicus in quo instruments deponuntur* (i.e., the public place where deeds are deposited), *quatmus incorrupta maneant* (i.e., so that they remain uncorrupted), *fidm faciant* (i.e., provide trustworthy evidence), and *perpetua rei memoria sit* (i.e., and be continuing memory of that to which they attest)".

7 O Projeto InterPARES define custodiador confiável como um preservador que pode demonstrar que não tem motivos para alterar os documentos arquivísticos preservados ou permitir que outros os alterem, e que é capaz de implementar todos os requisitos para a preservação autêntica dos documentos arquivísticos.

a partir de uma política de preservação digital, estar bem documentado, ser revisado periodicamente e cumprir com os principais padrões internacionais.

A segunda série de requisitos do Trac diz respeito ao gerenciamento dos documentos digitais no repositório. Nesse aspecto, a norma tem total conformidade com o modelo Oais, em especial com relação ao modelo de informação e aos metadados. Assim, a gestão e o armazenamento dos documentos em um repositório digital confiável devem basear-se nos pacotes de informação Oais, que encapsulam os documentos e seus metadados. De acordo com o Oais, o repositório deve tratar de três tipos de pacotes de informação: pacote de informação de submissão (*Submission Information Package – SIP*), para a entrada de documentos no repositório; pacote de informação de arquivamento (*Archival Information Package – AIP*), para o armazenamento dos documentos no repositório; pacotes de informação de disseminação (*Dissemination Information Package – DIP*), para o acesso aos documentos e seus metadados associados.

Um repositório digital confiável deve ter uma série de funções para verificar a integridade dos pacotes de informação na entrada, no armazenamento e no acesso aos documentos. Além desses controles, o repositório deve registrar, em metadados, informação descritiva e de apoio à preservação, em conformidade com as principais normas e padrões internacionais.

A última série de requisitos trata de aspectos tecnológicos. Certamente que um repositório digital deve ter uma série de soluções tecnológicas para apoiar sua confiabilidade na manutenção da autenticidade dos objetos digitais sob sua custódia e dar garantia de acesso aos mesmos no longo prazo. As tecnologias de hardware e de software devem ser apropriadas aos serviços prestados pelo repositório, e este deve contar com procedimentos para monitorar e avaliar, sempre que necessário, as mudanças de tecnologia, tendo-se o cuidado de análise da relação custo-benefício. A escolha ou definição dos softwares utilizados deve levar em conta o cumprimento das normas e convenções comumente aceitas no que diz respeito à preservação digital, contexto legal e ao âmbito do acervo custodiado. Nesse ponto, é preciso ter muita clareza no tocante às boas práticas e normas para o tratamento de arquivos, pois a escolha de software e hardware para um repositório de documentos arquivísticos precisa atendê-las. O repositório deve implementar funções que assegurem a integridade dos objetos sob sua custódia, e realizar, no mínimo, o controle do acesso de maneira segura, o monitoramento de todas ações realizadas, reparação de perdas e corrupção de dados, bem como possuir uma estratégia de *backup*. Forçosamente, deve ser capaz de implementar soluções tecnológicas para colocar em prática as estratégias de preservação digital definidas em sua política.

Conforme já assinalado, as diretrizes para repositórios digitais confiáveis determinam que é necessário satisfazer as necessidades de seus usuários e as especificidades do acervo sob sua custódia. Assim, os repositórios destinados à manutenção de documentos arquivísticos requerem requisitos adicionais para proteger as características dos documentos arquivísticos e prever procedimentos em conformidade com as normas da área de arquivo.

REPOSITÓRIOS DIGITAIS PARA DOCUMENTOS ARQUIVÍSTICOS

Documentos arquivísticos registram e apoiam as atividades de uma instituição, e servem também de evidência destas atividades. Para que seja possível creditar-lhes valor probatório, é necessário assegurar suas qualidades como documentos arquivísticos, em particular a relação orgânica e a autenticidade.

A autenticidade é a qualidade de um documento ser exatamente aquele que foi produzido, sem sofrer qualquer modificação, manipulação ou dano. Ela está relacionada com a transmissão do documento, sua manutenção e custódia ao longo do tempo. De acordo com a diplomática,[8] a autenticidade é composta de identidade e integridade, sendo a identidade entendida como o conjunto de atributos de um documento que o caracterizam como único e diferente dos demais. O documento arquivístico é único no conjunto ao qual pertence. Os documentos iguais podem existir em um ou mais grupos de documentos, mas cada um é único em seu lugar e o conjunto de suas relações com os outros documentos é sempre único. A integridade diz respeito à manutenção da forma e do conteúdo do documento ao longo do tempo.

No glossário do Projeto InterPARES,[9] relação orgânica é definida como "as relações que os documentos arquivísticos que pertencem a uma mesma agregação (dossiês, séries, fundos) têm entre si". Esta relação começa quando um documento arquivístico é, pela primeira vez, conectado a outro no curso de uma ação. Pode se expressar na ordem física dos documentos, na agregação à qual pertence e também pelo código de classificação ou número de registro do documento. Para entender melhor o conceito de relação orgânica, são expressivas as palavras de Luciana Duranti: "a relação orgânica surge principalmente quando se retém um documento arquivístico e, por tanto, ele é conectado a outro no curso de uma ação, mas é incremental, porque […] está em formação e crescimento contínuo até que a agregação à qual pertence não esteja mais propensa ao crescimento, ou seja, até que a atividade que produz esta agregação esteja encerrada" (Duranti, 1997).

A relação orgânica expressa o contexto de produção e a procedência dos documentos, que por sua vez reforçam o valor probatório dos documentos. Por isso, o acesso aos documentos arquivísticos deve ser realizado de tal maneira que seja possível recuperar uma série completa como resultado de uma busca, e que o documento seja acessado relacionado ao conjunto ao qual pertence. O conjunto expressa a atividade como um todo e funciona como um meio de autenticar cada unidade documental.

A relação orgânica e a identidade caracterizam o documento arquivístico como tal, e o distingue de outros tipos de informação. Assim, além de dar garantias da autenticidade do

8 Disciplina que tem como foco de estudo a estrutura formal, a confiabilidade e a autenticidade dos documentos. Ver Conarq (2011, p. 9).

9 O projeto InterPARES é um projeto colaborativo internacional de pesquisa sobre documentos arquivísticos digitais autênticos. Informações a respeito podem ser acessadas no sítio <www.interpares.org>.

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

CONSIDERAÇÕES E RECOMENDAÇÕES

As iniciativas de governo eletrônico e de dados abertos têm como principal fonte os documentos arquivísticos, que por sua vez devem ser mantidos de tal forma que seja possível assegurar sua autenticidade. Além disso, o aumento da produção de documentos digitais no governo e os desafios colocados para manter sua autenticidade e acesso ao longo do tempo apontam a necessidade de uma infraestrutura confiável para proteger esses documentos. Por outro lado, repositórios digitais confiáveis são meios reconhecidos internacionalmente e tecnologicamente como neutros para garantir o acesso em longo prazo aos documentos arquivísticos digitais e para proteger sua autenticidade. Logo, a manutenção dos documentos arquivísticos requer dos repositórios características singulares.

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

As autoridades arquivísticas nacionais devem definir os requisitos desses repositórios, para que tenham a capacidade de proteger as características dos documentos arquivísticos e de cumprir com as normas e melhores práticas da área de arquivos. As instituições arquivísticas públicas são responsáveis pela preservação dos documentos produzidos pelo governo e, segundo as melhores práticas internacionais, as autoridades competentes para estar à frente do desenvolvimento de repositórios digitais confiáveis.

A preservação de documentos permanentes, de valor histórico ou probatório, é a missão das instituições arquivísticas públicas, que devem estar preparadas para atuarem como repositórios digitais confiáveis destes documentos. Quanto aos documentos em fase corrente e intermediária, os arquivos devem liderar o planejamento da infraestrutura, que, para além

da definição dos requisitos para os repositórios, também implica a criação de uma arquitetura de metadados, a definição de normas para intercâmbio de dados e os meios para facilitar o acesso dos cidadãos aos repositórios.

Em vários países os arquivos nacionais e outras instituições arquivísticas públicas já contam com uma solução para atuarem como repositórios digitais confiáveis para os documentos em fase permanente, e em alguns casos recebem também documentos em fase intermediária. Alguns deles já têm atuado fortemente no desenvolvimento de uma infraestrutura de repositórios para atender aos produtores desde o início do ciclo de vida dos documentos, como os dos Estados Unidos, Reino Unido, Austrália, Nova Zelândia, Canadá, Portugal e Noruega.

Por fim, é importante o desenvolvimento de um programa de certificação para proporcionar uma base de confiança aos repositórios digitais, uma vez que estes repositórios precisam ser auditados periodicamente, para verificar sua conformidade com as normas internacionais e referendar sua confiabilidade.

Referências bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). NBR 15472: Sistemas espaciais de dados e informações – Modelo de referência para um sistema aberto de arquivamento de informação (Saai). 2007.

DURANTI, Luciana. The archival bond. *Archives and Museum Informatics*, n. 11, p. 213-218, 1997.

_____. Archives as a place. *Archives & manuscripts*, v. 24, n. 2, p. 242-255, 1996.

CONSELHO NACIONAL DE ARQUIVOS (Conarq). *e-Arq Brasil*: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. InterPARES 3 Project Terminology Database. Disponível em: <http://www.interpares.org/ip3/ip3_terminology_db.cfm>. Acesso em: 21 jun. 2013.

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. Diretrizes do Preservador – *A preservação de documentos arquivísticos digitais*: diretrizes para organizações.

INTERNATIONAL STANDARDS ORGANIZATION. ISO 14721: Reference model for an open archival information system (Oais). Geneve, 2003.

INTERNATIONAL STANDARDS ORGANIZATION. ISO 16363:2012: Space data and information transfer systems – Audit and certification of trustworthy digital repositories.

LYNCH, Clifford A.; LIPPINCOTT J. K. Institutional Repository Deployment in the United States as of Early 2005. *D-Lib Magazine*, v. 11, n. 9, Sept. 2005. Disponível em: <http://www.dlib.org/dlib/september05/lynch/09lynch.html>. Acesso em: 21 jun. 2013.

MARTINS, A.; NUNES, M.; RODRIGUES, E. Repositórios de informação e ambientes de aprendizagem: criação de espaços virtuais para a promoção da literacia e da responsabilidade social. *RBE Newsletter*, n. 3, 2008. Disponível em: <http://www.rbe.min-edu.pt/news/newsletter3/repositorios.pdf>. Acesso em: 21 jun. 2013.

RLG/NARA. *Trustworthy Repositories Audit & Certification*: Criteria and Checklist. OCLC and CRL, 2007. Disponível em: <http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf>. Acesso em: 21 jun. 2013.

RLG/OCLC. *Trustworthy digital repositories*: atributes and responsbilities. RLG, 2002. Disponível em: <https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf>. Acesso em: 21 jun. 2013.

SAYÃO, Luís Fernando et al. (org.). *Implantação e gestão de repositórios institucionais*: políticas, memória, livre acesso e preservação. Salvador: EDUFBA, 2009.

SAYÃO, Luis Fernando. *Repositórios digitais confiáveis para a preservação de documentos eletrônicos científicos*. Ponto de Acesso, 2010. Disponível em: <http://www.portalseer.ufba.br/index.php/revistaici/article/viewArticle/4709>. Acesso em: 21 jun. 2013.

THOMAZ, Katia. Repositórios digitais confiáveis e certificação. *Arquivistica.net*, v. 3, n. 1, p. 80-89, jan./jun. 2007.

Recebido em 8/6/2015
Aprovado em 26/6/2015