FUENTES
Vol. 10, N° 46 Octubre 2016: pp. 27-35. ISSN 2225-3769

Implementação de Repositórios Arquivísticos Digitais Confiáveis: recomendações e requisitos

*Ana Suely Pinho Lopes**
*Daniel Flores***

RESUMO

Este estudo tem por objetivo apontar e analisar, de uma maneira breve, os problemas referentes à preservação de documentos arquivísticos digitais, uma vez que as constantesmudanças tecnológicas vêm comprometendo cada vez mais o futuro dos acervos digitais. Diante desta perspectiva, torna-se imprescindível o uso de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq, desde que munidos de estratégias de preservação necessárias para garantir a salvaguarda dos documentos, tendo em vista que armazenam registros pessoais e institucionais como fonte de prova e informação na atualidade e para as gerações futuras. A metodologia se dá por meio de consultas a normativos e dispositivos legais, assim como realização de pesquisa bibliográfica em material publicado nos últimos anos, em busca de soluções que viabilizem o acesso contínuo e que assegure a autenticidade. Dar-se-á também, sob análise qualitativa de fundamentos teóricos a fim de identificar para o problema abordado, procedimentos arquivísticos e requisitos de um repositório digital confiável que garanta a confiabilidade desses documentos pelo tempo que se fizer necessário.

Palavras-chave: <Preservação digital> <Documento arquivístico digital> <Repositórios digitais> <Requisitos de preservação> <Estratégias de preservação>.

Implementación de Repositorios Digitales Confiables: recomendaciones y requisitos

RESUMEN

Este estudio tiene por objetivo identificar y analizar, de forma breve, los problemas relacionados con la preservación de documentos de archivo digitales, ya que los constantes cambios tecnológicos vienen comprometiendo cada vez más el futuro de los acervos digitales. Ante esta perspectiva, se torna imprescindible el uso de Repositorios Archivísticos Digitales Confiables – RDC-Arch, aprovisionarse de las estrategias de preservación necesarias para garantizar la salvaguarda de los documentos, teniendo en cuenta el almacenamiento de los registros personales e institucionales como fuente de prueba e información para las actuales y futuras generaciones. La metodología aplicada apunta a la consulta de la normativa y dispositivos legales, así como a la realización de investigación bibliográfica en materiales publicados en los últimos años, todo en busca de soluciones que viabilicen el acceso continúo y que asegure la autenticidad de estos repositorios. También se hizo un análisis cualitativo de fundamentos teóricos a fin de identificar para el problema abordado, procedimientos archivísticos y requisitos de un repositorio digital confiable que garantice la confiablidad de esos documentos por el tiempo que sea necesario.

Palabras clave: <Preservación digital> <Documento de archivo digital> <Repositorios digitales> <Requisitos de preservación> <Estrategias de preservación>.

* Mestranda; Programa de Pós-Graduação em Patrimônio Cultural; Universidade Federal de Santa Maria/UFSM.

** Doutor; Programa de Pós-Graduação em Patrimônio Cultural; Universidade Federal de Santa Maria/UFSM.

1. Introdução

Seja para registrar ou apoiar a tomada de decisões no dia a dia, servir de fonte de pesquisa ou assegurar os direitos dos cidadãos, lá estão eles, nas instituições ou organizações, os documentos arquivísticos digitais gerados como prova de atividades e para atender as demandas no dia a dia e no futuro, conforme necessidade. Para tanto, é essencial que permaneçam acessíveis e autênticos pelo tempo que se fizer necessário. A geração célere e crescente da produção de documentos arquivísticos em formato digital suscita cada vez mais que as organizações e as instituições produtoras e de guarda busquem soluções que visem ao acesso e a preservação em longo prazo. Os materiais digitais sofrem várias ameaças devido à fragilidade dos suportes e a obsolescência tecnológica, tornando seus registros vulneráveis à adulteração.Os Repositórios Arquivísticos Digitais Confiáveis – RDC-Arqse constituem em uma solução técnica, metodológica e estrategicamente adequada para este desafio(CONARQ, 2015).

O Brasil tem como iniciativa, dentre outras, a elaboração da Resolução N° 43/2015, da Câmara Técnica de Documentos Eletrônicos do Conarq–CTDE, que estabelece diretrizes para a implementação de repositórios digitais confiáveis – RDC-Arq para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR.

A Resolução Nº 43 (CONARQ, 2015), da legislação arquivística brasileira, apresenta recomendações normativas de gerenciamento para todo o ciclo de vida dos documentos, recomenda que aqueles que se encontram nas fases corrente e intermediária devem ser geridos por meio de um Sistema Informatizado de Gestão Arquivística de Documentos – SIGAD, a fim de garantir o controle do ciclo de vida, o cumprimento da destinação prevista, e a manutenção da autenticidade e da relação orgânica, características singulares desses documentos.

De acordoainda com a Resolução Nº 43 (CONARQ, 2015), a preservação dos documentos arquivísticos digitais, nas fases corrente, intermediária e permanente, deve estar associada a um repositório digital confiável. Sendo assim, os arquivos devem dispor de repositórios digitais confiáveis para a gestão, a preservação e o acesso aos documentos digitais.Assegura que,ao contrário do que muitos acreditam, nessas fases já devem existircuidados especiais, previstos em um plano de preservação digitalpara aqueles documentos destinadosa guarda por médio e longo prazo, de modo que garanta sua autenticidade e acesso.

No ato da destinação para a guarda permanente, ocorre naturalmente, alteração na cadeia de custódia, instante que a responsabilidade pela preservação dos documentos dos produtores passa à instância de guarda. Neste momento, os documentos digitais de guarda permanente são dependentes de um eficiente sistema informatizado que apoie o tratamento técnico conveniente, incluindo arranjo, descrição e acesso, de forma a assegurar a manutenção da autenticidade e da relação orgânica entre eles.É neste instante que ascende a necessidade de se conectar a preservação desses documentos a um repositório arquivístico digital confiável.

No contexto internacional, apontam-se algumas iniciativas destinadas ao desenvolvimento de repositórios arquivísticos digitais confiáveis, como solução para a garantia da autenticidade, da preservação e do acesso de longo prazo. Podemos destacar a do grupo de trabalho liderado pelo *Research Library Group* – RLG e pelo *Online Computer Library Center* – OCLC.

A preservação da informação digital torna-se uma questão complexa, uma vez que, assim como oarquivamento, envolve variáveis, compromissos de longa duração. Estanão se limita ao domínio tecnológico, abrange,ademais,questões administrativas, legais, políticas, econômico-financeiras e, sobretudo, de descrição dessa informação através de estruturas de metadados que viabilizem o gerenciamento da preservação digital e o acesso ao futuro (CONARQ, 2004).

2. Iniciativasde preservação em ambiente digital

Como forma de apresentar iniciativas de preservação em ambiente digital, define-se o repositório arquivístico digital como um ambiente autêntico capaz de garantir a preservação dos documentos digitais nele armazenados, de modo a assegurar seu acesso contínuo e manter a autenticidade.

Sabe-se que, para preservar documentos e patrimônio digital nacional, precisaremos contar com uma rede de repositórios capaz de demonstrar confiabilidade para preservar esse conteúdo (THOMAZ e SOARES, 2004).Uma rede nada mais ése não a capacidade de trabalho compartilhado, para intercambiar arquivos de dados e quiçá se amparar em algumas

instituições para preservar determinados conteúdos e outras instituições para outros tipos de conteúdos. Diante desses requisitos mínimos, começa-se a reconhecer uma nova necessidade no cenário da gestão, preservação e acesso aos documentos arquivísticos digitais.

Esse assunto foi discutido por um grupo de trabalho sobre atributos de arquivos digitais da junta RLG/OCLC[1], cujo relatório final foi publicado em 2002. De um modo geral o relatório:

* Propõe uma definição de repositório digital confiável;

* Identifica os atributos primários de um repositório digital confiável;

* Identifica as responsabilidades de um repositório compatível com o modelo de referência OAIS e,

* Articula uma estrutura para o desenvolvimento de um programa de certificação.

A partir do relatório da RLG/OCLC (2002) e novos trabalhos em continuidade, discutem-se três questões fundamentais relacionadas: confiança, modelo de referência *Open Archival Information System* (OAIS) e certificação, abordados a seguir.

2.1. Confiança

As instituições denominadas bibliotecas, arquivos e museus, são responsáveis pela guarda do patrimônio cultural pelo fato de tratarem-se de instituições que adquiriram, no decorrer do tempo, a satisfatória confiança para armazenar material de relevante valor. São consideradas instituições confiáveis para preservar esses itens nas melhores condições para fornecer acesso a esse material para as futuras gerações (THOMAZ, 2007). Entretanto, pode-se afirmar que se adquireconfiança com o passar do tempo, e, em se tratando de documentos digitais, o que vai validar essa premissa é a existência de um sistema de informação eficaz.

Entende-se que confiança se desenvolve em diversos níveis. No caso de repositórios digitais confiáveis, no mínimo três níveis são aplicáveis:

* A confiança de que os produtores estão enviando as informações corretas;

* A confiança de que os consumidores estão recebendo as informaçõe s corretas;

* A confiança de que os fornecedores estão prestando serviços adequados.

Mas como a "confiança" pode ser traduzida em um mecanismo mensurável? Como autenticamos a "confiança" que depositamos nos objetos? Porque as bibliotecas, os arquivos e os museus são responsáveis por nosso patrimônio cultural?

A resposta surge quase que naturalmente: porque essas instituições adquiriram, ao longo do tempo, a necessária confiança para armazenar esse material precioso. Essas instituições são confiáveis para fornecer acesso a esse material, com o objetivo de registrar e retratar a história, bem como fomentar o aumento do conhecimento. Elas são confiáveis para preservar esses itens nas melhores condições para futuras gerações.

Entretanto, essas instituições culturais têm sido bem sucedidas em preservar grandes quantidades de patrimônio cultural na forma de objetos físicos. Na maioria dos casos, esses objetos físicos estão disponíveis como "prova" da capacidade da instituição de recolher e preservar por longo prazo. Mas tendo em vista que a informação digital é menos tangível e muito mais mutável do que outros materiais, ademais considerando a complexidade e especificidade, confiança e credibilidade podem ser bem mais difíceis de comprovar.

Conforme citado anteriormente, o relatório da RLG/OCLC (2002) relaciona atributos e responsabilidades dos arquivos digitais confiáveis, conforme listados a seguir:

* Conformidade com o modelo de referência OAIS;
* Responsabilidade administrativa;
* Viabilidade organizacional;
* Sustentação financeira;
* Adequação tecnológica;
* Sistema de segurança;
* Responsabilidade (accountability) de procedimentos.

Ressalta-se que o modelo de referência OAISé destacado, pelo Conselho Nacional de Arquivo – CONARQ, como a norma mais importante da áreapreviamente definida a ser seguida na implementação de repositórios arquivísticos digitais e por tratar-se de uma referência internacional, optou-se pela sua descrição a seguir.

2.2. O modelo de referência OAIS

O OAIS é um modelo de referência conceitual que especifica os requisitos para um arquivo de

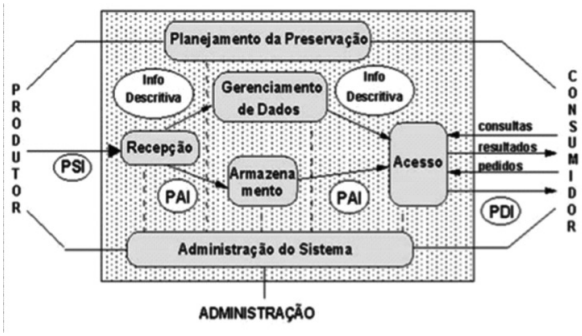
materiais digitais, o qual tem a responsabilidade de preservar informações e disponibilizá-las para uma comunidade específica.

Para compreender quando um repositório digital se encontra em conformidade com o modelo de referência OAIS, conforme o relatório da RLG/OCLC (2002), entende-se que

> '[...] Serviços' de arquivamento digitais efetivos basear-se-ão no entendimento compartilhado de todo o conjunto de partes envolvidas a respeito do que será atendido e como será atendido. [...] O modelo de referência fornece uma estrutura comum, envolvendo terminologia e conceitos, para descrição e comparação de arquiteturas e operações de arquivos digitais (RLG/OCLC WORKING GROUP ON DIGITAL ARCHIVE ATTRIBUTES, 2002.

É importante lembrar que um nível importante da confiança é a capacidade das instituições culturais em confiarem nos serviços de terceiros. Se os serviços de terceiros forem compatíveis com o modelo de referência OAIS, ou apenas preencherem um dos aspectos de um sistema compatível com este modelo, ter-se-á o início de um entendimento compartilhado e um caminho mais fácil para o relacionamento confiável.

Figura 1. Modelo funcional OAIS



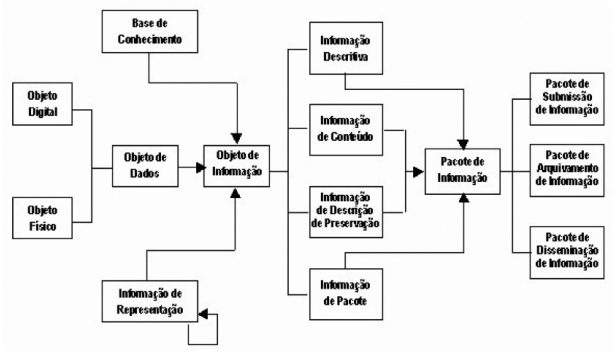
Fonte: Thomaz; Soares, 2004.

Mas enfim, o que significa estar em conformidade com o modelo de referência (OAIS)? Também conhecido por Sistema Aberto para Arquivamento de Informação (SAAI), como passamos a citá-lo de agora para frente.

Segundo o modelo de referência SAAI (ABNT, 2007), a compatibilidade é atingida quando o arquivo atende aos modelos de informação e funcional proposto. Mas, principalmente, quando cumpre um conjunto de responsabilidades, como negociar e aceitar informação adequada dos produtores de informação; obter controle suficiente da informação fornecida no nível necessário para garantir a preservação por longo prazo; determinar, por si mesmo ou em conjunto com outros parceiros, as comunidades que devem tornar comunidade alvo e, portanto, que devem ser capazes de entender a informação fornecida;por fim, garantir que a informação a ser preservada seja independentemente compreensível para uma comunidade alvo.

Em outras palavras, a comunidade alvo deve ser capaz de entender a informação sem a necessidade da assistência dos especialistas que produzem a informação; seguir políticas e procedimentos documentados que garantam que a informação seja preservada contra todas as contingências cabíveis e que possibilitem que a informação seja disseminada como cópia autêntica do original ou rastreável até o original e tornar a informação preservada disponível para a comunidade alvo (ABNT, 2007).

Figura 2: Modelode informação SAAI



Fonte: Thomaz; Soares, 2004.

Conforme mencionado anteriormente, a confiança geralmente ocorre após um longo período de tempo. Entretanto, com a preservação digital, não temos tempo a perder. Precisamos de ações emergentes. Sendo assim, qual a medida a ser adotada? Como tratar a preservação digital a curto prazo para que possamos estendê-la por longo prazo?

2.3. Certificação

Encontramos na certificação digital a solução, uma vez que se trata de uma tecnologia possível de provê os mecanismos de segurança capazes de garantir autenticidade, confiabilidade e integridade às informações eletrônicas.

> O modelo de referência SAAI não aborda diretamente a questão da certificação de arquivos. Entretanto, suscita um despertar, no que se refere no caso de quando um arquivo precisa usar outro como referência para um conjunto de serviços, sendo capaz de 'confiar' no outro arquivo. Uma forma

> de tratar essa questão de forma geral é identificar abordagens através das quais um arquivo possa estabelecer algum nível de certificação, seja por auto avaliação ou por auditoria externa (RLG/OCLC WORKING GROUP ON DIGITAL ARCHIVE ATTRIBUTES, 2002).

A certificação tornou-se um dos pilares sustentáveis para repositórios digitais confiáveis contemporâneos.

> Na dúvida, usamos a certificação como nosso mecanismo e instrumento de medida. Isso possibilita que repositórios se recuperem e caminhem, obtenham negócios, construam e comprovem boas práticas. E, ao longo do tempo, eles ganharão nossa CONFIANÇA. No passado, as práticas de certificação tendiam ao informal e implícito. Com os arquivos digitais há o desejo – talvez a necessidade – de tornar a certificação formalizada e explícita (THOMAZ e SOARES, 2004).

Um repositório digital confiável é capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário. Para tanto, deve ser capaz de estar em conformidade com os procedimentos arquivísticos e atender os requisitos de um repositório digital confiável (CONARQ, 2014).

Conforme o documento Diretrizes para a implementação de repositórios digitais confiáveis de documentos arquivísticos (CONARQ 2015), seguem algumas recomendações para a implementação de repositórios digitais de documentos arquivísticos e em seguida requisitos para um repositório digital confiável.

3. Recomendações para a implementação de repositórios digitais de documentos arquivísticos

* Responsabilidade pelo repositório

A responsabilidade pelo projeto, implantação e manutenção de um repositório digital de documentos arquivísticos deve ser compartilhada por profissionais de arquivo e de tecnologia da informação, de forma a se cumprirem os requisitos tecnológicos e os procedimentos do tratamento arquivístico.

* Tratamento arquivístico

Um repositório digital para documentos arquivísticos tem que ser capaz de organizar e recuperar os documentos, de forma a manter a relação orgânica entre eles. Nesse sentido, deve apoiar a organização hierárquica dos documentos digitais, a partir de um plano de classificação de documentos, e a descrição multinível, de acordo com a Norma Geral Internacional de Descrição Arquivística – ISAD (G) e a "Norma Brasileira de Descrição Arquivistica (NOBRADE).

Figura 3: Normageral internacional de descrição arquivística e Norma brasileira de descriçãoarquivística

Fonte: Site Arquivo Nacional

* Princípios de preservação digital

A preservação digital devegarantir o acesso em longo prazo a documentos arquivísticos autênticos, o que implica na adoção dos seguintes princípios:

- focar em documentos arquivísticos digitais autênticos;
- pressupor que a autenticidade dos documentos arquivísticos digitais está sob ameaça, principalmente no momento da transmissão no espaço (entre pessoas e sistemas) e no tempo (atualização/ substituição de *hardware* e *software* usados para armazenar, processar e comunicar os documentos);
- reconhecer que a preservação digital é um processo contínuo, que começa na concepção do documento;
- reconhecer que a autenticidade dos documentos arquivísticos digitais tem por base os procedimentos de gestão e preservação e a confiança tanto no repositório como no órgão responsável pela guarda desses documentos;
- arbitrar o que se considera como documento original, uma vez que a preservação digital implica a necessidade de conversão

de formatos e atualização de suportes; reconhecer que a elaboração de manuais e os procedimentos de preservação,,, desempenhados pelo repositório digital, apoiam a presunção de autenticidade desses documentos;

- reconhecer que o registro, em metadados, das intervenções de preservação em cada documento apoia a presunção de autenticidade desses documentos;
- reconhecer que a autenticidade dos documentos digitais deve ser avaliada e presumida no momento de sua submissão ao repositório;
- reconhecer que o repositório digital é responsável pela manutenção permanente da autenticidade dos documentos a ele submetidos; e
- distinguir claramente a autenticidade e autenticação de documentos, considerando que a primeira é a qualidade de o documento ser verdadeiro, e a segunda, uma declaração dessa qualidade, feita, em um dado momento, por uma pessoa autorizada para tal.

Ademais, um repositório deve também possuir autonomia no sentido de tanto assegurar seu funcionamento assim como dar acesso aos documentos.

*** Independência dos repositórios**

Um repositório digital deve ter independência. Isso significa que seu funcionamento e o acesso aos documentos não podem depender das aplicações que funcionam em conjunto com ele. Por exemplo, em uma aplicação para arquivos correntes e intermediários, deve ser possível acessar os documentos independentemente do SIGAD, isto é, diretamente no repositório, desde que isso seja feito de forma controlada, para não ameaçar a autenticidade dos documentos no repositório. É bom esclarecer que o acesso direto aos documentos no repositório não exclui a necessidade de um SIGAD para apoiar a gestão arquivística.

Outra característica fundamental é ter capacidade de interoperabilidade, conforme descrito a seguir.

*** Interoperabilidade**

Interoperabilidade é a capacidade de um sistema (informatizado ou não) de se comunicar de forma transparente (ou o mais próximo disso) com outro sistema (semelhante ou não). Para um sistema ser considerado interoperável, é muito importante que ele trabalhe com padrões abertos ou ontologias.

Um repositório digital deve estar em conformidade com as normas e padrões estabelecidos, de forma a possibilitar níveis de interoperabilidade com outros repositórios digitais e sistemas informatizados que tratam de documentos arquivísticos. Podem ser citados como exemplos dessas normas e padrões: o "*Open Archives Initiative Protocol for Metadata Harvesting* – OAI-PMH", para coleta de registros de metadados em repositórios digitais; o "*Metadata Encoding and Transmission Standard – METS*", para a codificação de metadados descritivos, administrativos e estruturais; o "*Encoded Archival Description* – EAD", para a codificação de metadados descritivos de documentos arquivísticos; e os "Padrões de Interoperabilidade de Governo Eletrônico – e-PING", no caso dos órgãos e entidades do governo federal.

4. Requisitos para um repositório digital confiável

Estratégias de preservação digital devem garantir que um objeto digital esteja acessível de forma utilizável ao longo do tempo. A partir dos princípios identificados no item anterior, percebe-se que manter a acessibilidade dos meios digitais é muito mais complexo, considerando suas especificidades, quando comparado ao meio analógico, no caso o papel. No caso de um relatório impresso preservado em seu formato original, todos os seus aspectos são mantidos em sua presença física: seu formato, 'layout' e conteúdo. Como no exemplo percebe-se que se torna impossível separar seus elementos por unidade, visto que estão intrinsecamente ligados. Em se tratando de objetos digitais, ao contrário, podem ser separados em partes facilmente, exigindo um esforço muito maior para a preservação do todo.

No caso de instituições e organizações que desejem implementar repositório digital confiável, precisam, como ponto de partida, observar um mínimo sequer de requisitos. Para tanto, Bullok (2001), tomando como referência o modelo de referência *Open Archival Information System* (OAIS), identificou os seguintes itens a saber:

* **Fixar os limites do objeto a ser preservado**: embora a natureza multimídia e hipertextual dosobjetos digitais seja bastante vantajosa do ponto de vista da navegação, para fins de preservação é necessário definir, claramente, quais elementos serão efetivamente mantidos.

* **Preservar a presença física**: a presença física representa o(s) arquivo(s) físico(s), i.e., a camada primitiva de suporte da informação a ser representada; refere-se, portanto, ao(s) arquivo(s) de computador, às séries de 0's e 1's que são a base para o significado de um objeto digital.

* **Preservar o conteúdo**: refere-se a manter a capacidade de acessar o conteúdo em seu nível mais baixo, como um arquivo texto em ASCII, independente do estabelecimento de variações de fontes e características de 'layout'.

* **Preservar a apresentação**: o conteúdo é apresentado visualmente através da aplicação de fontes de diferentes formatos e tamanhos, uso de espaço em branco, colunas, margens, cabeçalhos, rodapés,paginação e assim por diante. Em alguns tipos de documentos digitais (por exemplo: formatos padrão SGML e alguns formatos PDF) as especificações de apresentação ficam separadas do conteúdo.

* **Preservar a funcionalidade**: objetos digitais podem conter componentes multimídia (i.e., texto, gráficos, áudio e vídeo integrados), existir em formato hipertexto (i.e., podem desviar dinamicamente para outros pontos do próprio documento ou para outro documento), conter conteúdo dinâmico (i.e., gerado automaticamente a partir de bancos de dados) ou ter funções de navegação (i.e., barras de ferramentas, pesquisa a palavra-chave ou tabelas interativas de conteúdo).

* **Preservar a autenticidade**: é necessário confiar que o objeto acessado é exatamente aquele que se procura e que as possíveis transformações pelas quais passou, para manter sua acessibilidade, preservaram sua forma original.

* **Localizar e rastrear o objeto digital ao longo do tempo**: imediatamente após a sua criação, os objetos digitais tornam-se passíveis de serem alterados, copiados ou movimentados. Em qualquer referência ao objeto digital, é necessário localizá-lo na edição ou versão correta.

* **Preservar a proveniência**: identificar a origem de um objeto e detalhar seu histórico ajudam a confirmar sua autenticidade e integridade.

* **Preservar o contexto**: os objetos digitais são definidos por suas dependências de *hardware* e *software*, seus modos de distribuição e relacionamentos com outros objetos digitais.

E, ainda, com a finalidade de implementar um repositório arquivístico digital confiável para preservar os documentos arquivísticos digitais e proporcionar o acesso contínuo em longo prazo, há que se observar normas, recomendações para definição de requisitos adequados ao modelo recomendável. Dentre os requisitos necessários, consideram-se:

*** Infraestrutura organizacional**

O ambiente em que o repositório digital vai se estabelecer há que cumprir determinados requisitos, conforme descrito a seguir:

✓ **Governança e viabilidade organizacional**

O repositório tem como missão o compromisso com a preservação, o gerenciamento e o acesso em longo prazo dos documentos digitais. Essa missão é claramente identificada por todos os interessados no repositório e envolve: mandato legal, contexto organizacional e requisitos regulatórios. O repositório tem um plano de sucessão formal, planos de contingência e/ou acordos estabelecidos para garantir a continuidade do serviço, no caso de o repositório parar de operar ou de a instituição responsável e/ou financiadora mudar seu escopo.

✓ **Estrutura organizacional e de pessoal**

O repositório tem uma equipe dotada de qualificação e formação necessárias, e em número suficiente, para garantir todos os serviços e funcionalidades pertinentes ao repositório. Além disso, deve manter um programa de desenvolvimento profissional contínuo.

✓ **Transparência de procedimentos e arcabouço político**

O repositório deve demonstrar explicitamente seus requisitos, decisões, desenvolvimento e ações que garantem a preservação em longo prazo e o acesso a conteúdos digitais sob seus cuidados. Dessa forma, assegura aos usuários, gestores, produtores e certificadores que está cumprindo plenamente seu papel enquanto um repositório digital confiável. Para tanto, o repositório deve:

- definir a comunidade alvo e sua base de conhecimento;
- possuir políticas e definições, acessíveis publicamente, que demonstrem como os requisitos do serviço de preservação serão contemplados;
- possuir políticas, procedimentos e mecanismos de atualização, na medida em que o repositório

cresce e a tecnologia e as práticas da comunidade evoluem;

- documentar permissões legais por meio de acordos de custódia, normas de procedimentos e outros que o isentem de responsabilidade, no caso de alterações passíveis de ocorrer em estratégias de preservação digital;
- fazer o registro histórico das mudanças de procedimentos, de *software* e *hardware*;
- relacionar o registro histórico, acima referido, com as estratégias de preservação digital, e descrever os potenciais efeitos dessas mudanças sobre os documentos digitais;
- demonstrar que está sistematicamente avaliando a satisfação das expectativas dos produtores e dos usuários, e buscando atendê-las;
- estar comprometido com a definição, coleta, auditoria e fornecimento (sob demanda) de mecanismos de controle da integridade dos documentos digitais sob sua custódia;
- estar comprometido em realizar regularmente uma auto avaliação de seu funcionamento e renovar sua certificação; e
- estar comprometido em notificar as entidades certificadoras sobre as mudanças operacionais que afetarão seu ***status*** de certificação (no caso de repositórios já certificados).

✓ **Sustentabilidade financeira**

Um repositório digital confiável deve demonstrar sustentabilidade financeira. Para isso, deve ter um plano de gestão que observe os seguintes aspectos:

- demonstração da capacidade de obter recursos financeiros estáveis e contínuos para sustentá-lo, sejam por meio de prestação de serviço, parcerias, doações, verba da própria instituição, dentre outros;
- revisão e ajustes anuais;
- transparência dos procedimentos para obtenção dos recursos e auditoria dos mesmos, de acordo com o sistema jurídico no qual o repositório se insere; e
- compromisso dos ciclos de planejamento com o equilíbrio dos riscos, benefícios, investimentos e gastos.

✓ **Contratos, licenças e passivos**

Os contratos, licenças e passivos firmados pelo repositório devem ser claros e mensuráveis, delinear papéis, responsabilidades, prazos e condições; e ser facilmente acessíveis ou disponíveis aos interessados. Eles podem envolver tanto a relação entre o repositório e os produtores de documentos digitais, como a relação entre o repositório e fornecedores de serviços. Esses mesmos instrumentos devem especificar todos os direitos e obrigações do repositório sobre os documentos digitais a ele confiados, em especial no que diz respeito à propriedade intelectual e às restrições de uso.

Considerações finais

Um repositório digital confiável vai muito além de uma tecnologia desenvolvida para armazenar, dar acesso e difundir os documentos arquivísticos digitais. Um repositório digital confiávelé capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário.Para tanto, deve ser capaz de atender aos procedimentos arquivísticos e aos requisitos de um repositório digital confiável. Fica a critério de cada instituição a decisão de implementar todas as funções informacionais em apenas um sistema. Existe a opção de aderir a dois ***softwares*** livres, como por exemplo, o ICA-AtoM, como plataforma de acesso e difusão dos documentos arquivísticos digitaise o Archivematica, para preservação.O fundamental na escolha é que as ferramentas atendam as recomendações técnicas de modo que a infraestrutura, a como um todo,garanta a confiabilidade e a sustentabilidade do repositório digital,assegurando que a instituiçãoe seus usuários possam confiar que os recursos digitais serão preservados em longo prazo.

Às instituições e organizações que pretendem implementar repositório digital, o atingimento da desejável confiança, via práticas confiáveis, comprovadas, ocorrerá com a aplicaçãon o decorrer do tempo. A certificação, por sua vez, vem atender a necessidade imediata de arquivos confiáveis e a garantia de comprovar a confiabilidade ao longo do tempo.

Finalmente, é confortável saber que existem normativos e dispositivos legais nacionais que tratam de requisitos e diretrizes para garantir o tratamento adequado destes documentos, a disponibilização dos documentos arquivísticos digitais em RDCs, assim comoiniciativas de instituições internacionais que oferecem padrões como o CCSDS e ISOa serem seguidos, além do modelo de referência para um Sistema Aberto de Arquivamento de Informação – SAAI, de amplo entendimento e pronto para ser aplicado.

Nota

1 Trusted Digital Repositories: Attributes and Responsibilities. Disponível em: < http: //<www.rlg.org/longterm/repositories.pdf>.

Bibliografía

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.

BULLOCK, Alison. *Preservation of digital information*; issues and current status. April 22, 1999. Last updated on February 27, 2001. Disponível em: <http://www.nlc-bnc.ca/publications/1/p1-259-e.html>. Acesso em: 25 maio, 2016.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica dedocumentos eletrônicos. *Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente*. Rio de Janeiro: Arquivo Nacional, 2015. Disponível em:

<http://www.conarq.arquivonacional.gov.br/media/publicacoes/resol_conarq_43_repositorios.pdf>. Acesso em: 13 jan. 2016.

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/cartapreservpatrimarq

digitalconarq2004.pdf>. Acesso em: 10 fev. 2016.

Digital Curation Centre (DCC); Digital Preservation Europe (DPE). *Digital Repository Audit Method Based on Risk Assessment (DRAMBORA).28 Feb.* 2007. Disponível em: <http://www.repositoryaudit.eu/download/>. Acesso em: 23 jan. 2016.

INTERNATIONAL ORGANIZATION OF STANDARDIZATION (ISO). ISO/IEC 27001: *Information technology: Security techniques: Information security management systems: Requirements*. 2005.

NESTOR WORKING GROUP ON TRUSTED REPOSITIORIES CERTIFICATION. *Catalogue of Criteria for Trusted Digital Repositories*.Dec. 2006. Disponível em: <http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf>. Acesso em: 23 fev. 2016.

RLG/NARA TASK FORCE ON DIGITAL REPOSITORY CERTIFICATION. *Trustworthy repositories audit & certification*.Feb. 2007. Disponível em: <http://www.crl.edu/PDF/trac.pdf >. Acesso em: 13 jan. 2016.

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: 12 jan.2016.

RLG/OCLC WORKING GROUP ON DIGITAL ARCHIVE ATTRIBUTES. *Trusted digital repositories: attributes and responsibilities*. May 2002. Disponível em: <http://www.rlg.org/longterm/repositories.pdf>. Acesso em: 12 jan. 2016.

THOMAZ, K. de P. *A preservação de documentos eletrônicos de caráterarquivístico: novos desafios, velhos problemas*. 2004. 389f. Tese(Doutorado em Ciência da Informação) - Escola de Ciência da InformaçãoUniversidade 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: 05 jan. 2016.

THOMAZ, Katia P.; SOARES, Antonio José. *A preservação digital e o modelo de referência Open Archival Information System (OAIS)*.Datagramazero, v. 5, n. 1, fev. 2004. Disponível em:<http://www.dgz.org.br/fev04/F_I_art.htm>. Acesso em: 10 jan. 2016.

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: 15jan. 2016.

Recepción: 23 de febrero de 2016
Aprobación: 30 de septiembre de 2016
Publicación: Octubre de 2016