La Red Cariniana: una experiencia de preservación digital distribuida en Brasil

Cariniana Network: a Brazilian Experience With A Distributed Digital Preservation Partnerships

A Rede Cariniana: uma experiência de parcerias de preservação digital distribuída no Brasil

Miguel Ángel Márdero Arellano
Instituto Brasileiro de Informação em Ciência e Tecnologia
miguel@ibict.br

Alexandre Faria de Oliveira
Instituto Brasileiro de Informação em Ciência e Tecnologia
alexandreoliveira@ibict.br

Resumen

A nivel internacional, en el área de la arquitectura de implementación de sistemas de preservación digital, se están considerando los riesgos y las características de los repositorios digitales confiables. Las herramientas de software utilizadas pasan por la verificación de la gestión y el control de los requisitos funcionales para el establecimiento de sistemas de conservación distribuidos. La preservación de registros digitales institucionales en Brasil debe tener en cuenta todos los sistemas de gestión digital utilizados para llevar a cabo las actividades técnico-científicas de los órganos. La Red Cariniana coordinada por el Instituto Brasileño de Información en Ciencia y Tecnología puede contribuir a la especificación de políticas, requisitos técnicos, capacitación y evaluación de la gestión de la preservación digital en instituciones públicas y privadas, entre otros tipos de servicios, y así establecer las reglas de producción. de colecciones digitales para la operación de sistemas confiables de publicación, acceso y archivo a largo plazo en Brasil.

Palabras clave: preservación digital, redes de preservación digital, Cariniana, Ibict, herramientas de preservación digital..

Abstract

Internationally, in the area of digital preservation systems implementation architecture, the risks and characteristics of reliable digital repositories are being considered. The software tools being used go through the verification of the management and control of the functional requirements for the establishment of distributed preservation systems. The preservation of institutional digital records in Brazil needs to take into account all the digital management systems used to carry out the technical-scientific activities of the organs. The Cariniana Network coordinated by the Brazilian Institute of Information in Science and Technology can contribute to the specification of policies, technical requirements, training, and evaluation of digital preservation management in public and private institutions among other types of services and thus to establish the rules of production of digital collections for the operation of reliable systems of publication, access and long-term archiving in Brazil.

Keywords: digital preservation, digital preservation networks, Cariniana, Ibict, digital preservation tools.

Recibido: 09-03-2018 Aprobado: 05-06-2018

Cómo citar este artículo: Márdero Arellano, M. A.; Faria de Oliveira, A. (2018). La Red Cariniana: una experiencia de preservación digital distribuida en Brasil. *Códices, 14*(2), 9-25.

Resumo

nternacionalmente, na área da arquitetura de implementação de sistemas de preservação digital estão sendo considerados os riscos e as características dos repositórios digitais confiáveis. As ferramentas de software que estão sendo utilizadas passam pela verificação do gerenciamento e controle dos requisitos funcionais para o estabelecimento de sistemas de preservação distribuídos. A preservação dos registros digitais institucionais no Brasil precisa levar em consideração todos os sistemas digitais de gerenciamento usados na realização das atividades técnico-científicas dos órgãos. A Rede Cariniana coordenada pelo Instituto Brasileiro de Informação em Ciência e Tecnologia pode contribuir na especificação de políticas, requisitos técnicos, capacitação, e avaliação da gestão da preservação digital nas instituições públicas e privadas entre outros tipos de serviços e dessa forma estabelecer as regras de produção de acervos digitais para o funcionamento de sistemas confiáveis de publicação, acesso e arquivamento de longo prazo no Brasil.

Palavras chave: preservação digital, redes de preservação digital, Cariniana, Ibict, ferramentas de preservação digital..

I. Introdução

Na nova era digital existe o contraste entre todo mundo conectado e a garantia de que essas conexões vão a existir ao longo do tempo. A dinâmica da Web, a sua diversidade, junto com a obsolescência dos softwares e dos formatos é um campo complexo para ser tratado pela preservação digital. A preservação de esse tipo de material deve partir de princípios e normas que demarcam as estratégias adotadas para a salvaguarda das coleções digitais. Já em 1998 a Federation of Libraries Associations (IFLA) definia a gestão da preservação como não limitada ao formato, que podia ser físico ou digital e de forma geral afirmava que a preservação incluía:

> "...all the managerial and financial considerations...including storage and accommodation provisions, staffing levels, policies, techniques and methods involved in preserving library and archival material and the information contained in them" (IFLA, 1998).

Dessa forma, estava definido o princípio da gestão da preservação que afeta a forma como a preservação digital deveria ser enxergada na prática. A principal diferença está na brevidade com que as ações de preservação digital devem ser iniciadas, sendo especialmente a sua capacidade de integração o princípio que define sua área de atuação. As diferentes estratégias tecnológicas, como a reformatação a migração, a emulação e a replicação se tornam efetivas na sua conexão com novas técnicas e sistemas de preservação digital.

Instituições de pesquisa públicas e privadas estão oferecendo soluções tecnológicas comerciais e de acesso aberto, aplicando o princípio da integração entre sistema que unificam aspectos técnicos e gerenciais, deixando atrás a visão de que a preservação digital é apenas um assunto relacionado com o armazenamento, o que tem produzido um alto risco de perda da herança digital e diminuído a permanência a longo prazo de importantes acervos digitais.

São inúmeros os fatores e agentes que tipificam ameaças causadoras de danos digitais. Para prevenir, preparar, responder e recuperar repositórios digitais se faz necessário um plano de contingência ou documento que descreve as políticas e procedimentos para enfrentar os possíveis riscos (FRANK, YAKEL, 2013). As políticas de preservação digital podem ser interpretadas como planos de contingenciamento, porque elas são instrumentos documentais, orientações legais elaborados para cenários de riscos específicos e que auxiliam no planejamento da resposta, tais como, recursos necessários, tarefas e responsáveis (SILVA JUNIOR; MOTA, 2012). A Preservação digital tem haver com monitoramento permanente de risco, com a mensuração de risco e com prevenção de perdas.

Na atual gestão da informação digital os repositórios institucionais têm se tornado em ferramentas vitais e componentes chave na viabilização da preservação de acervos a longo prazo. Os repositórios para preservação de objetos digitais estão sendo apresentados como aqueles que estariam localizados em instituições confiáveis e capazes de armazenar, migrar e dar acesso a coleções digitais. Esse tipo de repositórios integra ferramentas de preservação digital, ou aquelas que sejam equivalentes nessa funcionalidade.

O risco disso não acontecer está na carência da aplicação de normas e critérios de preservação na formação de suas coleções digitais. A evidência pública do cumprimento dessa observância reside na documentação usada para gerenciar seus objetos digitais, na declaração que garante a segurança para uma organização gerenciar suas coleções em um repositório digital. Os repositórios institucionais enfrentam o desafio da formação de profissionais capacitados no tratamento de sistemas de gestão de informação digital e da integração de soluções tecnológicas auditadas e certificadas.

Neste trabalho, apresentam-se alguns exemplos de sistemas e soluções tecnológicas que estão sendo testados e que já estão sendo considerados

padrões de preservação digital pela comunidade científica, assim como também serão discutidas as propriedades mínimas de preservação digital para garantir a confiança nos repositórios digitais.

II. Fundamentos Teóricos

As iniciativas de construção e desenho de repositórios digitais, além de tornar exponencial o acesso à informação, têm permitido, no âmbito profissional, novas experiências de controle e gerenciamento de recursos eletrônicos em fluxos que compõem o ciclo informacional e possibilitado, no âmbito da comunidade usuária, o usufruto de recursos e serviços informacionais que perpassam novas formas de validação e de atribuição de autoridade à informação.

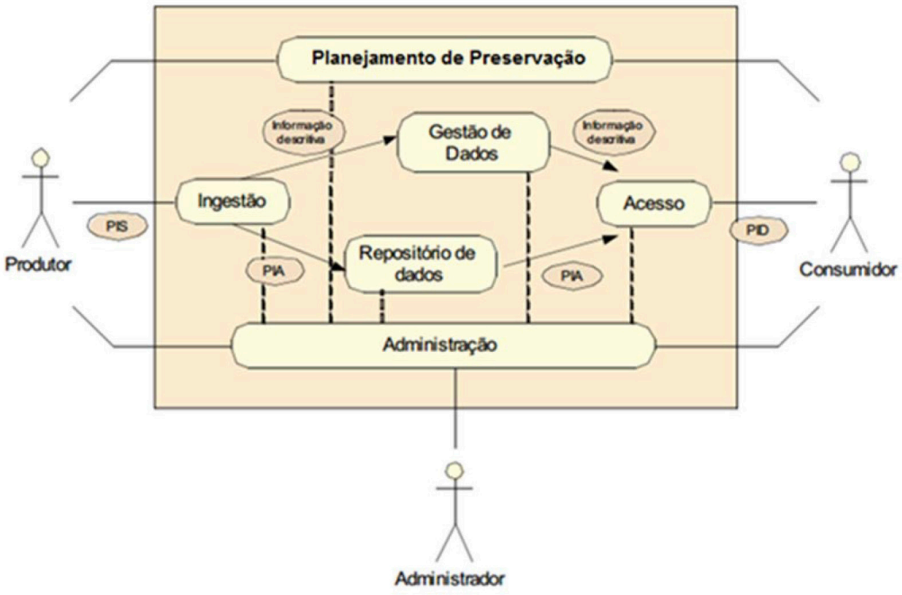
As atividades de preservação digital que permitem a garantia ao acesso contínuo à informação a longo prazo, tornam-se indispensáveis à criação de repositórios digitais confiáveis, podendo elas ser partes de diferentes softwares que ajudem no tratamento dos dados com finalidade de auxiliar as atividades de todo processo de arquivamento.

As ferramentas de preservação digital precisam observar alguns requisitos de arquitetura de software contemplados no modelo referência OAIS (Open Archival Information System). Esse modelo é uma iniciativa do Consultative Committee for Space Data Systems (CCSDS, 2012), que define os itens básicos para que ocorra o arquivamento de objetos digitais de forma que eles possam ser preservados a longo prazo em repositório de dados confiáveis (figura 1).

A adoção de utilização do modelo OAIS na construção de repositórios digitais adiciona confiança nas ações de preservação, visto que este modelo é amplamente usado nas melhores práticas já consolidadas das comunidades mundiais de preservação digital. As instituições de pesquisas devem definir as políticas que contemplem estratégias de preservação digital e utilizem ferramentas que estão em conformidade com os requisitos funcionais do modelo OAIS.

A primeira lista de atributos e responsabilidades de repositórios digitais confiáveis foi estabelecida pela Research Libraries Group (RLG) e o Online Computer Library Center (OCLC) no seu relatório publicado em 2002. Esse conjunto de atributos está influenciado pelo modelo OAIS e estabelece que

Figura 1. Modelo OAIS



essa obediência ao modelo deva ser considerada o primeiro critério a ser observado por um repositório confiável. Para esse grupo, os repositórios confiáveis devem incluir também, atributos que possam dar suporte a sistemas de segurança e aos procedimentos adequados e significativos.

O modelo Trusted Digital Repository representa a primeira forma de expressar a infra-estrutura organizacional da preservação digital. Os atributos do TDR converteram-se em padrões para a comunidade da preservação digital, pois antes deles não existia uma expressão formal do contexto organizacional da preservação digital (MÁRDERO ARELLANO, 2008). No TDR, um repositório confiável deve incluir atributos que sustentem os seguintes aspectos:

a) responsabilidade administrativa;
b) viabilidade organizacional;
c) sustentabilidade financeira;
d) adequabilidade tecnológica e procedimental;
e) sistema de segurança;
f) responsabilidade de procedimentos (certificação).

A confirmação do armazenamento de conteúdos e metadados através do processo de ingestão, até o ponto de acesso é essencial e deve estar na missão de preservação oferecendo "armazenamento para arquivamento" em termos OAIS. O repositório deve assumir a responsabilidade pela preservação a longo prazo e gerenciar essa função de forma planejada e documentada. O gestor do repositório, os depositantes e a comunidade designada precisam entender o nível de responsabilidade assumido para cada item depositado no repositório, assim como quais são os direitos legais para assumir essas responsabilidades.

Os projetos colaborativos de preservação digital estão orientados para um possível processo de auditoria para atribuir/certificar a concordância com o modelo OAIS, as primeiras ações a serem desenvolvidas nesses projetos são:

- mapear as seis entidades de um repositório que esteja em concordância com o OAIS (inserção, armazenamento arquivístico, administração, gerenciamento de dados e acesso) dentro de uma estrutura existente;
- garantir que a terminologia de um domínio específico pode ser mapeada por um equivalente OAIS.
- a infraestrutura tecnológica do repositório deve fornecer proteção das instalações e seus conteúdos, produtos, serviços e usuários.
- a equipe gestora do repositório deve analisar possíveis ameaças, avaliar riscos e criar um sistema de segurança consistente.
- descrever cenários de danos com base em ações mal-intencionadas, erro humano ou falha técnica que representem uma ameaça para o repositório e seus dados, produtos, serviços e usuários.
- medir a probabilidade e o impacto de tais cenários, decidir quais níveis de risco são aceitáveis e determinar quais medidas devem ser tomadas para combater as ameaças ao repositório e à sua Comunidade Designada.

Os repositórios devem funcionar em sistemas operacionais bem suportados e em um ou vários softwares de infraestrutura interoperável e usando tecnologias de hardware e software apropriadas às necessidades e aos serviços que fornece à sua Comunidade Designada, segundo o modelo de referência OAIS.

O modelo de rede de preservação digital colaborativa propõe que várias instituições armazenem, ofereçam acesso e criem cópias digitais atualizadas. A perspectiva DDP (Distributed Digital Preservation) propõe a criação de cópias

distribuídas em arquivos digitais em servidores geograficamente dispersos para garantir sua sobrevivência (SKINNER, 2010).

As redes de preservação digital distribuída começaram a surgir nos últimos anos, principalmente pela adoção de um software que observava os seis critérios mencionados. É o software LOCKSS (Lots of Copies Keeps Stuff Save) da Stanford University que permite a criação de Redes Privadas Locais (PLN). A maioria delas com sede na América do Norte, Europa e Ásia, onde já existem PLNs que preservam cópias de conteúdos digitais criados localmente por organizações científicas e culturais.

A Aliança LOCKSS está baseada na ideia de que se um acervo de biblioteca sofre uma perda ou destruição, outros locais no mundo oferecerão um local seguro e a oportunidade de recuperação das informações a partir de cópias autorizadas. Este modelo colaborativo suporta duas opções de armazenamento: o arquivamento controlado (CLOCKSS) e aquele que oferece acesso segundo o tipo de assinatura de acesso que a biblioteca possua aos materiais bibliográficos contratados (LOCKSS).

As bibliotecas participantes selecionam na lista de editoras no CLOCKSS ou no LOCKSS as publicações que elas desejam preservar. As editoras que solicitam que seu conteúdo seja preservado no LOCKSS devem estabelecer inicialmente um consórcio com o LOCKSS contatando uma das bibliotecas participantes e requerer a preservação. Após uma acordo, o editor publica uma declaração oficial com a autorização ("publisher manifest page") e informa a equipe LOCKSS o endereço Web. O LOCKSS informa às bibliotecas participantes que o material está disponível para preservação (NOGUEIRA, 2008).

O conteúdo digital preservado nas redes LOCKSS e CLOCKSS está formado por periódicos e coleções digitais de repositórios de acesso aberto ou privado de todas as áreas do conhecimento. Soluções de preservação digital colaborativa como a do LOCKSS são especificamente apropriadas para as revistas de acesso aberto e de pequeno porte que não possuem opções economicamente viáveis de preservação.

Observa-se que os softwares considerados como de preservação pela comunidade científica, estão voltados aos repositório repositórios institucionais (ANEXO 1). Geralmente esses repositórios não atende todos os requisitos de um repositório totalmente confiável, concentrando-se somente no acesso ao conteúdo. Os sistemas de preservação digital permitem que esse conteúdo

permaneça acessível mesmo após mudanças no software, que os metadados possam migrar de um repositório para outro, sem que haja perda de dados, incluindo também os metadados administrativos.

As redes de preservação digital são uma estratégia de salvaguarda de acervos digitais, que abrange um conjunto de computadores interligados compartilhando, softwares, arquivos e periféricos, cuja a finalidade é executar programas ou aplicações dos usuários.

III. A Preservação Digital Distribuída no Brasil

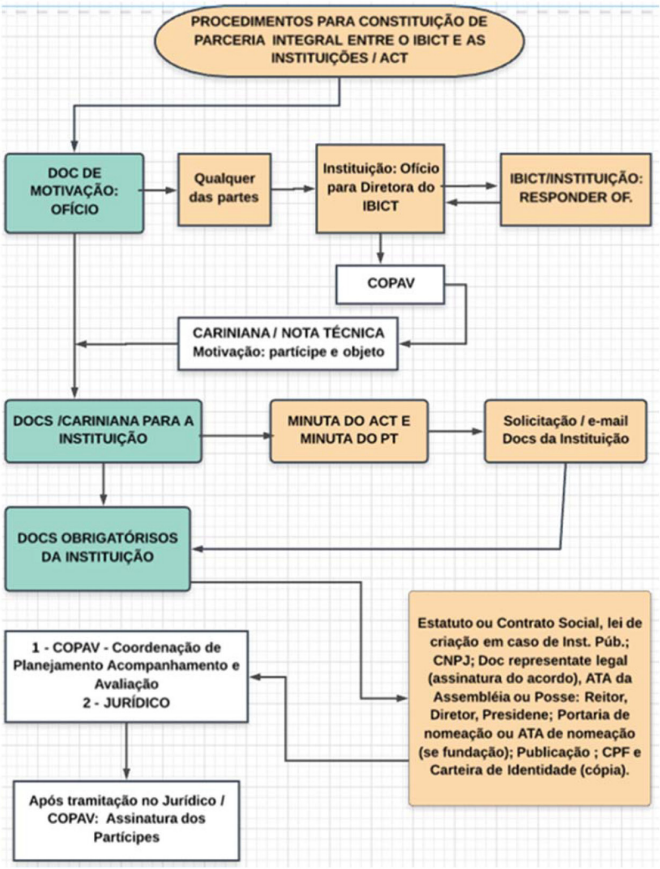
No Brasil, a rede Cariniana realiza uma ação semelhante de arquivamento de publicações de acesso aberto coordenada pelo Instituto Brasileiro de Informação em Ciência e Tecnologia - Ibict em parceria com sete instituições de ensino e pesquisa brasileiras. Essas instituições concordam em arquivar os conteúdos de acesso aberto informados pela equipe do Ibict que se encontram disponíveis para preservação na plataforma LOCKSS. A Rede iniciou esse serviço em 2012 com mais de mil periódicos brasileiros de acesso aberto que utilizam a ferramenta OJS/SEER.

Para promover esse arquivamento digital, o Ibict aderiu à Aliança LOCKSS da Stanford University, por estar em concordância com normas internacionais já testadas. Periódicos, livros, teses e dissertações eletrônicas são o alvo da primeira etapa do projeto, assim como também, a capacitação de profissionais dedicados ao registro de acervos em formato digital incorporou-se ao conjunto de primeiras ações da Rede.

Desde este enfoque, a rede Cariniana iniciou seus trabalhos num contexto tecnológico e de gestão colaborativo e distribuído, que engloba uma visão de acesso perpétuo aos documentos digitais e de aplicação de critérios de preservação digital, para a formação de redes distribuídas de compartilhamento dos registros do conhecimento humano. A Primeira Rede de Preservação digital do Brasil.

Cabe mencionar que toda a operação de preservação de periódicos eletrônicos conta também com a colaboração de iniciativas internacionais como O Public Knowledge Project (PKP) e a Stanford University Libraries. O Ibict é também, o coordenador do centro nacional do ISSN, órgão internacional especializado no registro e controle das publicações seriadas.

Fluxo do processo de parcerias na Rede Cariniana



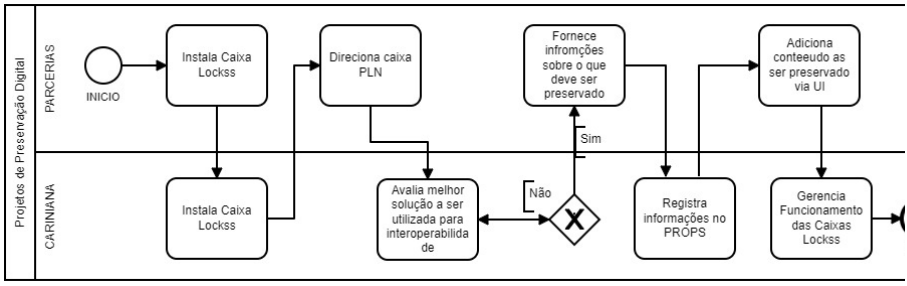
As parcerias da Cariniana são uma fonte de recursos de informação de valor para a Rede. As atuais oito instituições parceiras integrais, contando ao Ibict entre elas, compartilham os mesmos termos do acordo de colaboração, assim como o plano de atividades estabelecido para os anos 2015-2020. Coordenadas também pelo Ibict, existem parcerias institucionais via termo de adesão já estabelecidas com quatro instituições de pesquisa. Até o momento, a Rede preserva 697 periódicos científicos de 112 instituições brasileiras.

A garantia de funcionamento da Rede está descrita na sua política e nas atividades de acompanhamento e pesquisa dos seus colaboradores e equipes técnicas. A Cariniana realiza reuniões anuais e encontros presenciais bianuais

com os representantes das instituições parceira e os líderes do seu grupo de pesquisa com 10 linhas de pesquisa registrado no Diretório de Grupos de Pesquisa do CNPq. Pare estes últimos a Rede disponibiliza o primeiro repositório de dados de pesquisa preserváveis registrado na Harvard University.

A Rede Cariniana é um exemplo de rede distribuída quando é considerado o baixo custo da sua instalação e manutenção. O LOCKSS requer pouco esforço administrativo e a equipe local precisa de pouco tempo anualmente para adicionar conteúdo ao sistema. A administração local de cada uma das instalações precisa apenas de um administrador de rede e de um profissional bibliotecário. Os dois profissionais são treinados em reuniões a distância e em encontros anuais de parceiros da rede. O serviço de cursos de preservação digital da Cariniana oferece treinamento presencial em temas relacionados e a oportunidade de compartilhamento de informações.

Fluxo de preservação digital distribuída da Cariniana



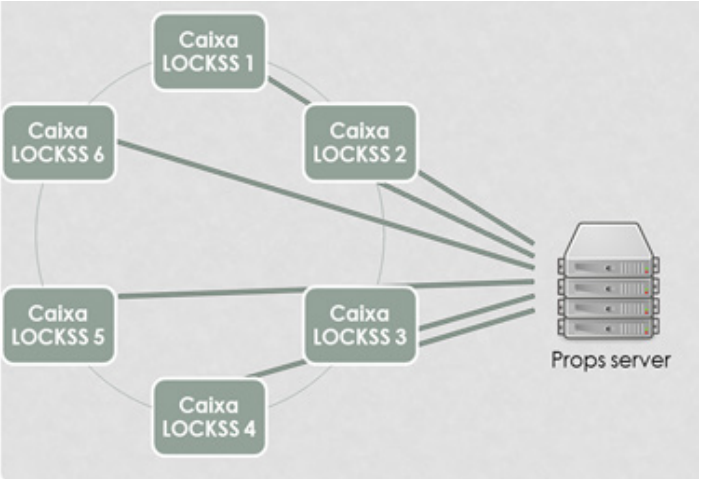
Um dos benefícios da parceria com a Aliança LOCKSS é permitir que a Rede atendesse aos requisitos funcionais do modelo de preservação OAIS e a descrição da informação do conteúdo digital em padrões de metadados de preservação digital para publicações seriadas.

O sistema LOCKSS usa um "crawler" para coletar o conteúdo de periódicos eletrônicos tal como eles foram publicados pelas revistas. No caso das revistas no OJS/SEER os editores são motivados a permitir o arquivamento digital, declarando na configuração da instalação da revista, um "manifesto" que é reconhecido pelo "crawler" como uma licença para coletar e preservar o conteúdo da publicação. Essa permissão autoriza o acesso ao conteúdo das instituições que participam da rede.

A estrutura da rede Cariniana incentiva a colaboração com o intuito de construir uma comunidade dedicada à preservação digital no futuro. É importante que cada instituição parceira esteja comprometida na manutenção de sua infraestrutura local nos próximos anos, assim como ao Ibict corresponde desenvolver as habilidades necessárias da sua equipe para continuar coordenando os serviços.

Na etapa atual, a estrutura da Rede conta com um servidor web localizado no Ibict, responsável pelo repositório de informações a serem repassadas às instituições parceiras. Esse servidor que cumpre o papel de nó central ou Props Server, não interfere na administração da Rede.

Figura 2. Estrutura de uma Rede Privada Local (PLN)



Entre as funções das nove instalações ou caixas existentes até hoje além de armazenar, preservar e corrigir danos aos conteúdos estão as de comparar continuamente o conteúdo coletado, atuar como web proxy ou cachê para acesso emergencial e controlar o acesso aos periódicos preservados (MÁRDERO ARELLANO, 2012).

A participação dos editores ficou estabelecida na autorização que eles disponibilizam do OJS, permitindo que suas publicações sejam arquivadas nas caixas LOCKSS. O termo publicado na revista registra a aprovação para que o processo ocorra. O termo já está incorporado no sistema de gerenciamento de editoração de revistas Open Journal Systems (OJS), deixando ao editor a

decisão de permitir que as caixas LOCKSS consigam identificar o endereço de IP e os conteúdos autorizados para coleta.

A Rede Cariniana chama a atenção para a importância da preservação digital distribuída, principalmente para que as instituições participantes possuam mais uma opção de arquivamento digital e que desenvolvam as habilidades necessárias para gerenciar suas próprias redes distribuídas. Uma das metas da Rede Cariniana é promover o uso de ferramentas de preservação digital no Brasil, com as quais seja possível preservar coletivamente um considerável número de publicações eletrônicas nacionais de acesso livre.

IV. Conclusões

Os estudos sobre preservação digital são fundamentais para garantir a longevidade do patrimônio registrado em dígitos binários. Há necessidade de estudos interdisciplinares que explorem o potencial das estratégias, dos sistemas informatizados e das políticas institucionais. As estratégias de preservação digital e os sistemas informatizados se implementados de forma isolada não fornecerão garantias de acesso em longo prazo. É importante definir previamente as políticas institucionais de preservação a fim de desenvolver um sistema de preservação digital sincronizado.

O método de arquivamento no modelo distribuído está direcionado para preservar a integridade das publicações eletrônicas mantendo cópias em vários servidores, conferindo periodicamente todas as cópias para verificar a congruência da informação armazenada. O objetivo é minimizar o grau de impacto que um desastre possa causar em um único arquivo digital. A base desse modelo é a colaboração entre instituições. Baseada em acordos interinstitucionais, a participação exige que os recursos técnicos sejam compartilhados e previstos em acordos (COOPER, GARCIA-MOLINA, 2001). As estratégias passam a ser combinadas e acordadas procurando garantir a segurança e prevendo as possibilidades de perda de conteúdos (SKINNER, SCHULTZ, 2010).

As instituições devem elaborar planos eficazes de preservação digital que contenham e apliquem protocolos, padrões e normas internacionais, em concordância com as políticas de cada instituição, assegurando a sua

sustentabilidade a longo prazo. O software que se está utilizando na gestão do repositório digital deve atender às normas e protocolos de preservação básicos.

A preservação digital que a Aliança LOCKSS permite não se reduz à disponibilização perpétua dos materiais armazenados, mas se estende às funções que garantem a preservação da propriedade intelectual dos documentos em qualquer formato digital. Os responsáveis pelo seu desenvolvimento adquirem e disponibilizam cópias das publicações de uma forma análoga à da biblioteca, com uma diferença: os registros não são descartados e seu acesso é salvaguardado (SCHNEIDER, 2007).

No modelo distribuído, se estabelece um compromisso entre editoras e bibliotecas, para que as instituições possam coletar, armazenar, arquivar e preservar conteúdo autorizado e salvaguardar o acesso das suas comunidades. Da mesma forma, a Aliança LOCKSS permite que as bibliotecas voltem a tomar a custódia das revistas para fins de preservação, e reforça o controle de acesso por parte dos editores, sem mudar o modelo de negócios, sejam eles restritos ou abertos.

A Aliança LOCKSS cria rede privadas locais de replicação de dados ou cópias compartilhadas de periódicos eletrônicos. Os conteúdos são validados com outras caixas LOCKSS, reparando eventuais danos, monitorando o acesso e arquivando de forma segura para qualquer recuperação por parte do editor.

A Rede Cariniana, a primeira a adotar esse modelo na América Latina, proporciona uma oportunidade para que as instituições brasileiras detentoras de coleções de documentos digitais participem de uma comunidade dedicada a garantir o acesso futuro a essas coleções. Dessa forma, o trabalho colaborativo permite a aprendizagem em um dos aspectos da gestão da informação menos atendidos nas bibliotecas e centros de informação.

Espera-se que com o tempo os benefícios da Rede Cariniana sejam evidentes, e cada vez mais instituições participem, trazendo outras perspectivas para a preservação a longo prazo de todo tipo de documento digital em território nacional.

Referências

CCSDS - CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (2012) Reference model for an Open Archival Information System (OAIS). Washington: Magenta Book. Recuperado de http://public.ccsds.org/publications/archive/650x0m2.pdf

Cooper, Brian, y GARCIA-MOLINA, Hector. (2001). Creating Trading Networks of Digital Archives. Delivered at the First ACM/IEEE Joint Conference on Digital Libraries. June 24-28. Roanoke, Virginia. Recuperado de http://dbpubs.stanford.edu:8090/pub/2001-23

Frank, Rebecca D., Yakel, Elizabeth. (2013). Disaster planning for digital repositories. Proceedings of the American Society for Information Science and Technology, 50(1), p. 1-10. Recuperado de https://goo.gl/bHVKHL

International Federation of Library Associations. (1998). Principles for the care and handling of library material. Recuperado de: http://www.ifla.org/VI/4/news/pchlm.pdf

Márdero Arellano, M. A. (2008) Critérios para a preservação digital da informação científica. 354f. Tese (Doutorado) - Universidade de Brasília, Departamento de Ciência da Informação, Brasília, 2008. Recuperado de: http://eprints.rclis.org/15412/1/Tese_Miguel_%C3%81ngel_M%C3%A1rdero_Arellano.pdf

Márdero Arellano, M. A. (2012). Cariniana: uma rede nacional de preservação digital. Ciência da Informação, v. 41, n. 1, p. 83-91. Recuperado de http://revista.ibict.br/ciinf/index.php/ciinf/article/view/2127/1794

Nogueira, André Ricardo Lopes. Preservação da Web através de replicação distribuída em larga escala. (2008), 58f. Dissertação (Mestrado em Engenharia Informática) – Universidade de Lisboa, Lisboa, PT, 2008. Recuperado de http://repositorio.ul.pt/handle/10451/3997

RLG/OCLC. (2002). Trusted digital repositories: attributes and responsibilities. Montain View, Canada: RLG-OCLC Report. Recuperado de https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

Schneider, Karen G. (2007). Lots of librarians can keep stuff safe. Library Journal, [s.l.], p. 30-31. Recuperado de http://wilsontxt.hwwilson.com/pdffull/01872/p76ee/6f6.pdf

Silva Júnior, Laerte, Mota, Valéria Gameleira da. (2012) Políticas de preservação digital no Brasil:

características e implementações. Ci. Inf., Brasília, DF, v. 41 n. 1, p.51-64, jan./abr., Recuperado de https://goo.gl/WEhvbC

Skinner. K., Schultz, M. eds. (2010). A Guide to Distributed Digital Preservation. Atlanta, GA: Enducopia Institute. 2010. Recuperado de http://www.metaarchive, org/GDDP

ANEXO 1
Ferramentas que contribuem para preservação digital

SOFTWARE	URL
ACE	https://gitlab.umiacs.umd.edu/adapt/ace
AIDA	https://aida.org.br/
ArchiveFacebook	https://github.com/machawk1/archivefacebook
Archive-it	https://archive-it.org/blog/learn-more/
Archivematica	https://www.archivematica.org/en/
ArchiveReady	http://archiveready.com/
ArchivesSpace	https://github.com/archivesspace/archivesspace
BWF MetaEdit	https://sourceforge.net/projects/bwfmetaedit/
Catalogue of Policy Elements	http://scape-project.eu/software/scape-open-source-software
CERN Advanced STORage manager (CASTOR)	http://castor.web.cern.ch/
Checker tiff	https://github.com/SLUB-digitalpreservation/checkit_tiff
Chronopolis	https://library.ucsd.edu/chronopolis/about/index.html
Cinch	https://statelibrary.ncdcr.gov/ghl/resources/digital-preservation/policies#dncr-digital-initiativesdncr-digital-initiatives

SOFTWARE	URL
Cksum Unix command	http://www.gnu.org/software/coreutils/manual/html_node/cksum-invocation.html
CMDP (Cost Model for Digital Preservation)	http://www.costmodelfordigitalpreservation.dk/
CollectiveAccess	https://collectiveaccess.org/
Collectus -- A Digital Object Collector Tool	https://guides.lib.virginia.edu/?b=s
ContextMiner	http://www.contextminer.org/about.php
DAITTS	https://daitss.fcla.edu/content/welcome-daitss-website-0
Data Vault	http://libraryblogs.is.ed.ac.uk/jiscdatavault/
DataCite	https://github.com/datacite/datacite
DataFlow	http://www.dataflow.ox.ac.uk/
Dataverse	https://github.com/IQSS/dataverse
DMPTool	https://dmptool.org/
DPBCT (Digital Preservation Business Case Toolkit)	https://projects.iq.harvard.edu/fits/home
DROID (Digital Record Object Identification)	https://github.com/digital-preservation/droid/blob/master/license.md
Dspace Direct	https://duraspace.org/dspace/about/
Duracloud	https://duraspace.org/duracloud/
File Information Tool Set (FITS)	https://github.com/harvard-lts/fits
Heritrix	https://github.com/internetarchive/heritrix3

SOFTWARE	URL
JHOVE	http://jhove.openpreservation.org/
LOCKSS	https://www.lockss.org/
Metadata Extraction Tool	http://meta-extractor.sourceforge.net/
NARA File Analyzer and Metadata Harvester	https://github.com/usnationalarchives/File-Analyzer
Carolina Digital Repository (CDR)	https://library.unc.edu/
Fixity	https://www.weareavp.com/products/fixity/