2018

MANUAL PARA AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Henrique Machado dos Santos

MANUAL PARA AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

É preciso ressaltar que a Arquivística se encontra em um momento de reformulação de suas teorias, e com a abordagem dos documentos digitais, surge à necessidade de adaptar e produzir teorias capazes de comportar os universos “analógico” e “digital”. Com este processo de reformulação teórico-prático, surgem diversas discussões e questionamentos que os arquivistas, inevitavelmente, terão de imergir e propor respostas ainda que provisórias, pois, se tratando de ciência, nada é definitivo, tudo está em constante transformação.

2018

MANUAL PARA AUDITORIA DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS

Henrique Machado dos Santos

Como citar este documento:

SANTOS, Henrique Machado. Manual para auditoria de repositórios arquivísticos digitais confiáveis. Disponível em: <furg.academia.edu/HenriqueMachadodosSantos>.

As coisas que concebemos de maneira muito clara e distinta são todas verdadeiras; há apenas alguma dificuldade em observar bem quais são aquelas que concebemos distintamente.
(René Descartes).

Para que a vida seja boa de se assistir, seu espetáculo deve ser bem interpretado: para tal, porém, são necessários bons atores.
(Friedrich Nietzsche)

Não há como prever, evitar e nem mesmo ignorar os avanços das tecnologias, só há uma certeza: tudo que é contemporâneo se tornará obsoleto, e se não for preservado, será perdido com o tempo.
(Henrique Machado dos Santos & Daniel Flores).

O avanço tecnológico mudou radicalmente os mecanismos de registro e de comunicação da informação nas instituições e, consequentemente, seus arquivos também mudaram.
(Rosely Curi Rondinelli).

SUMÁRIO

1 INTRODUÇÃO 12

2 MODELO OAIS 14

3 CADEIA DE CUSTÓDIA DOCUMENTAL 18

4 REQUISITOS DO ACTDR 20

5 CONCLUSÃO 50

6 REFERÊNCIAS 52

APRESENTAÇÃO

A implementação de um Repositório Digital Confiável requer a conformidade com requisitos do modelo *Open Archival Information System* (OAIS) – ISO 14721:2012 e que sejam devidamente auditados e certificados com o padrão *Audit and Certification of Trustworthy Digital Repositories* (ACTDR) – ISO 16363:2012. No entanto, a implementação de um Repositório "Arquivístico" Digital Confiável (RDC-Arq), além de considerar estas normas, deverá estar em conformidade com princípios e peculiaridades inatas aos documentos arquivísticos. Dentre estes princípios e peculiaridades, podem-se mencionar os princípios da proveniência, organicidade, unicidade e integridade, além de peculiaridades como a forma fixa e o conteúdo estável.

Considerando estas questões mencionadas, realizou-se uma pesquisa partindo da análise das normas OAIS e ACTDR, com objetivo de propor um instrumento que facilite a compreensão dos requisitos necessários à implementação de um RDC-Arq. Sendo assim, este manual consiste no produto de uma dissertação de mestrado, intitulada "Auditoria de repositórios arquivísticos digitais confiáveis: uma análise das normas ISO 14721 e ISO 16363"; orientada pelo professor Daniel Flores, e defendida no Programa de Pós-Graduação Profissionalizante em Patrimônio Cultural, da Universidade Federal de Santa Maria.

Desta forma, o "manual para auditoria de repositórios arquivísticos digitais" perpassa explicações gerais sobre o funcionamento de um arquivo digital em conformidade com o modelo OAIS, para preservação de documentos de caráter permanente. Ressalta a sua ligação com a gestão de documentos, assim como a necessidade de manter uma cadeia de custódia documental ininterrupta a fim de gerar confiabilidade.

Inicialmente, parte-se de uma abordagem geral do OAIS, para posteriormente, chegar a uma análise pontual dos requisitos de auditoria do ACTDR, de modo a ressaltar as necessidades de um RDC-Arq. Seu principal objetivo consiste em fornecer uma síntese dos requisitos de auditoria a fim de facilitar a compreensão dos arquivistas frente ao desafio de implementar e manter um RDC-Arq para preservação de documentos arquivísticos digitais autênticos, com garantia de acesso contínuo em longo prazo.

É preciso ressaltar que a Arquivística se encontra em um momento de reformulação de suas teorias, e com a abordagem dos documentos digitais, surge à necessidade de adaptar e produzir teorias capazes de comportar os universos "analógico" e "digital". Com este processo de reformulação teórico-prático, surgem diversas discussões e questionamentos que os arquivistas, inevitavelmente, terão de imergir e propor respostas ainda que provisórias, pois, se tratando de ciência, nada é definitivo, tudo está em constante transformação. Observa-se que a transformação não é menos intensa quanto aos documentos digitais, embora recentes, ainda não há um *corpus* teórico sedimentado, de modo que qualquer questionamento fundamentado será um divisor de opiniões potencial.

Este manual surge como um produto de reflexão acadêmica para instigar os profissionais e pesquisadores a compreenderem palavras-chave como: documento arquivístico digital, OAIS, ACTDR, cadeia de custódia, autenticidade, confiabilidade, auditoria e repositório arquivístico digital confiável. Com este manual, espera-se alavancar as discussões em torno dos RDC-Arq's, assim, como fornecer subsídios aos arquivistas que desejam compreender o processo de auditoria.

OBJETIVOS

O que este manual pretende: este manual visa orientar o processo de auditoria de RDC-Arq's, partindo da análise do OAIS e do ACTDR. Desta forma, enfatiza aspectos da Arquivística que devem ser considerados pela administração do repositório. Este manual visa aproximar o diálogo entre OAIS, ACTDR e Arquivística, isto porque, a linguagem utilizada nestas normas e a sua abrangência é tida como genérica, ou seja, destinada para repositórios digitais de diversas naturezas. Sendo assim, busca-se enfatizar os requisitos arquivísticos que estão implícitos tanto no OAIS, quanto no ACTDR. Dizem-se implícitos, pois, não há menções significativas à Arquivística, entretanto, há conceitos e princípios do OAIS que se enquadram na preservação de documentos arquivísticos digitais. Sendo assim, apresenta-se uma definição complementar capaz de resumir os requisitos que um RDC-Arq deve seguir.

O que este manual não pretende: este manual não pretende esgotar a discussão em torno da auditoria e certificação de RDC-Arq's, seu principal objetivo está centrado em promover a discussão. Da mesma forma, não pretende dispensar a leitura do OAIS e do ACTDR, pois seu princípio parte da compreensão destes e verticaliza para a visão arquivística. A leitura do OAIS é indispensável, pois será a partir de seus requisitos e orientações que o repositório será desenvolvido. Já a leitura do ACTDR é fundamental ao auditor, pois este precisa compreender os requisitos para qualquer repositório digital confiável. Sendo assim, este manual não substitui a leitura do OAIS e do ACTDR, apenas atuará de modo complementar para facilitar o diálogo com a Arquivística.

1. INTRODUÇÃO

O processo de auditoria torna-se essencial para demonstrar que um RDC-Arq está em conformidade com o modelo OAIS e que segue princípios arquivísticos. A realização de auditorias periódicas aliadas a uma certificação irá demonstrar que o RDC-Arq é confiável.

Inicialmente, é preciso estar ciente de que o processo de preservação digital começa antes da submissão dos documentos arquivísticos aos RDC-Arq. Isto reque a pré-existência de um Sistema Informatizado para Gestão Arquivística de Documentos (SIGAD), responsável pelas fases corrente e intermediária. Depois de encerrada esta fase "administrativa", os documentos devem ser recolhidos aos RDC-Arq, que será o arquivo permanente digital. E este será responsável por preservar e garantir o acesso contínuo no longo prazo.

Posteriormente, torna-se essencial compreender o modelo OAIS a fim de proceder a sua implementação em um RDC-Arq. Esta etapa deve considerar aspectos tecnológicos e políticos, de modo a abranger fluxos de informação, requisitos obrigatórios e entidades funcionais do OAIS; além de princípios fundamentais da Arquivística, como proveniência, unicidade e integridade.

Finalmente, o RDC-Arq deve ser auditado a fim de mensurar seus níveis de confiabilidade para que possa ser certificado pelo órgão competente. O processo de auditoria deve considerar o padrão ACTDR, o qual verifica a definição de políticas, a gestão de objetos digitais e os níveis de segurança dos dados armazenados. Assim, verifica-se a conformidade do RDC-Arq com o modelo OAIS para que seja mensurado o seu nível de confiabilidade.

Nesse contexto, o presente manual tem por objetivo fornecer subsídios teóricos para compreensão do modelo OAIS e do padrão ACTDR, com ênfase nos requisitos para auditoria de RDC-Arq's. Da mesma forma, busca-se esclarecer os requisitos arquivísticos que estão subentendidos no RDC-Arq, realçando sua pertinência durante o processo de auditoria.

2. MODELO OAIS

Há uma série de responsabilidades obrigatórias a serem atendidas por um repositório em conformidade com o modelo OAIS (ABNT/NBR 15472:2007; CCSDS, 2012; ISO 14721:2012). Desta forma, um RDC-Arq deverá:

- Negociar e aceitar informações adequadas junto ao produtor;
- Obter o controle das informações fornecidas para garantir a preservação em longo prazo;
- Participar da definição da comunidade designada[1], e estabelecer sua base de conhecimento para compreender as informações fornecidas;
- Garantir que a comunidade designada é capaz de compreender as informações preservadas sem necessidade de recursos especiais ou do auxílio dos produtores;
- Seguir políticas e procedimentos previamente documentados demonstrando confiabilidade na preservação da informação, além de restringir a exclusão de itens, exceto que permitido como parte de uma estratégia aprovada;
- Disponibilizar a informação preservada à comunidade designada, permitindo disseminá-la como cópia ou rastreável[2].

As responsabilidades obrigatórias são os propósitos do repositório digital, estão relacionadas a aquisição da informação digital e dos direitos para realizar a sua preservação em longo prazo. Além disso, há a definição da comunidade designada, de modo que esta seja capaz de interpretar as informações preservadas sem a necessidade de se recorrer a métodos complexos e específicos.

Em resumo, as responsabilidades irão definir o que será preservado e o seu respectivo direito para tal. Além disso, irão manter procedimentos para a

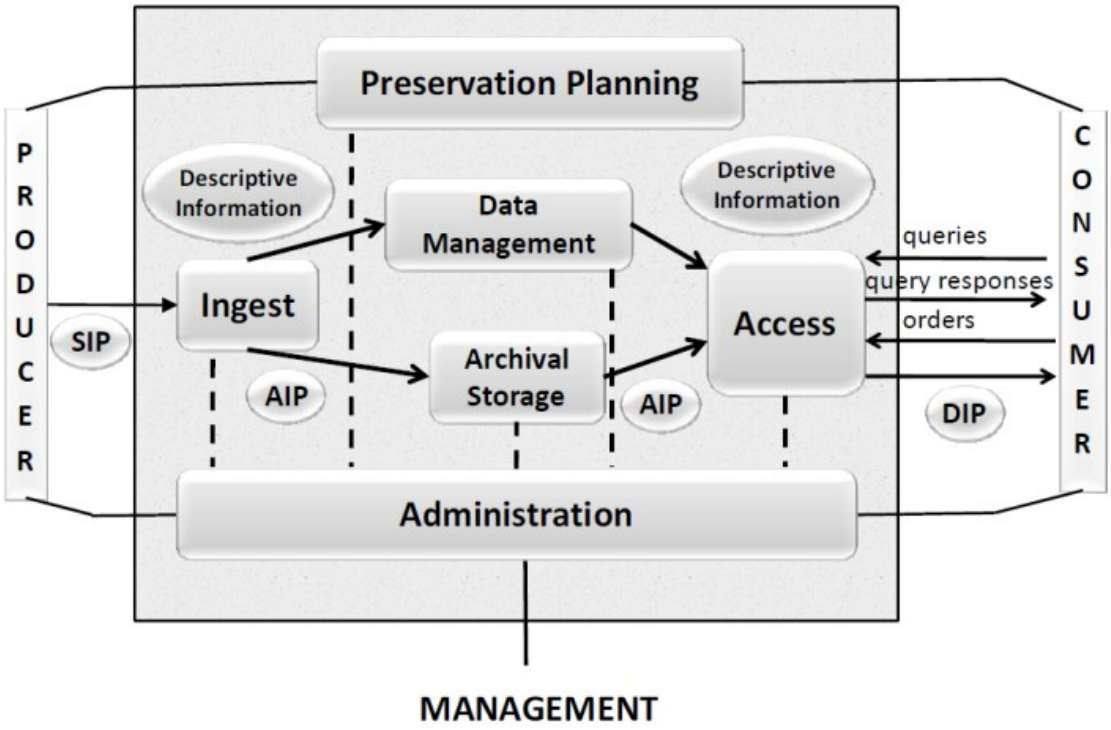
[1] Conjunto identificado de usuários potenciais capazes de entender um conjunto específico de informações. A comunidade designada pode ser composta por várias comunidades de usuários. Logo, o arquivo definirá a comunidade designada, e esta definição, poderá mudar com o tempo (CCSDS, 2012; ISO 14721:2012). No entanto, no âmbito da Arquivística, esta distinção de público não ocorre de forma rígida. O acesso à informação preservada é oferecido para quaisquer usuários que tenham interesse na informação de conteúdo. A visão arquivística da comunidade designada corresponde ao arquivo e seus usuários potenciais, ou seja, não há restrição de público. Logo, o objetivo é atender o maior número possível de usuários interessados, de modo que estes sejam capazes de interpretar corretamente as informações preservadas.

[2] Apontando para o objeto de dados originalmente submetido junto com os demais elementos que comprovam a sua autenticidade

preservação e definir quem irá usufruir deste material. Neste ponto, o modelo OAIS subentende a necessidade de assegurar a posse legal da informação digital, bem como conhecer previamente, a existência de uma comunidade potencialmente interessada na preservação e garantia de acesso ininterrupto à informação.

Com relação ao ambiente OAIS há seis entidades funcionais, que são: admissão (*ingest*), armazenamento arquivístico (*archival storage*), gestão de dados (*data management*), administração (*administration*), plano de preservação (*preservation planning*) e acesso (*access*). Neste ambiente, perpassam os pacotes de informação (*Submission Information Package* – SIP, *Archival Information Package* – AIP e *Dissemination Information Package* – DIP) nos quais são inseridas as informações descritivas (*descriptive information*) referentes às suas respectivas informação de conteúdo. A seguir, a "Figura 1 – Entidades funcionais do OAIS" apresenta uma esquematização simplificada da relação entre indivíduos, entidades funcionais e pacotes de informação.

Figura 1 – Entidades funcionais do OAIS



Fonte: (CCSDS, 2012, p. 4-1).

Há um conjunto de entidades internas e externas ao ambiente OAIS. As entidades internas são: admissão (*ingest*), armazenamento arquivístico (*archival*

storage), gestão de dados (*data management*), administração (*administration*), plano de preservação (*preservation planning*) e acesso (*access*). E as entidades externas são: produtor (*producer*), administrador (*management*) e consumidor (*consumer*).

O produtor (*producer*) se refere às pessoas ou sistemas que fornecem a informação que será preservada por meio da submissão de SIP's. O administrador (*management*) se refere àqueles que estabelecem as políticas gerais que governam o repositório pela entidade interna administração (*administrator*). Desta forma, os SIP's são transformados em AIP"s para serem arquivamentos. Já o consumidor (*consumer*) se refere às pessoas ou sistemas que interagem com os serviços oferecidos pelo OAIS para acessar a informação preservada através da entidade de acesso (*access*). Logo, para atender as demandas de acesso, o repositório irá gerar pacotes DIP, os quais são compostos por formatos de arquivos mais "leves", especiais para a disseminação via *Internet*.

Após o produtor (*producer*) submeter o SIP, a entidade de admissão (*ingest*) irá verificar a conformidade do pacote com os modelos previamente definidos nas políticas de preservação junto à entidade planejamento da preservação (*preservation planning*). Em caso de não conformidade, o pacote será rejeitado. Caso o pacote esteja de acordo com estas políticas, a entidade de administração (*administrator*) irá realizar a admissão dos conteúdos do SIP. Posterirormente, a informação descritiva (*descriptive information*) será inserida, com objetivo de registrar o histórico de custódia dos objetos digitais, relatando quaisquer aliterações realizadas juntamente com as informações adicionais utilizadas para preservação e garantia de acesso. Assim, o pacote SIP é transformado em AIP e encaminhado à entidade armazenamento arquivístico (*archival storage*).

Neste estágio, a entidade armazenamento arquivístico (*archival storage*) torna-se responsável por preservar os pocetes AIP's, enquanto a entidade gestão de dados (*data management*) irá gerenciar as informações descritivas dos objetos digitais. Assim a gestão de dados (*data management*) manterá um banco de dados atualizado sobre as informações relativas aos AIP's, corroborando com a manutenção de sua autenticidade, preservação e garantia de acesso ininterrupto no longo prazo.

A entidade de acesso (*access*) é a meio de comunicação entre o consumidor (*consumer*) e o repositório, podendo ser denominada como plataforma de acesso.

Neste ponto, ressalta-se que o consumidor (*consumer*) não tem acesso direto aos AIP's armazenados na entidade armazenamento arquivístico (*archival storage*), mas tão somente, à plataforma de acesso, comunicando-se indiretamente pela entidade de acesso (*access*). Tal procedimento é um fluxo de informação pertinente do OAIS visto que adicionam maior controle das ações e minimiza os riscos de invasão aos conteúdos preservados.

Desta forma, o consumidor solicita acesso a um determinado conteúdo e a entidade de acesso (*access*) encaminha a solicitação. O resultado da solicitação é enviado ao consumidor (*consumer*) pela entidade de acesso (*access*) por meio do pacote DIP; e segue as políticas de preservação e acesso definidas pelas entidades plano de preservação (*preservation planning*) e administração (*administrator*).

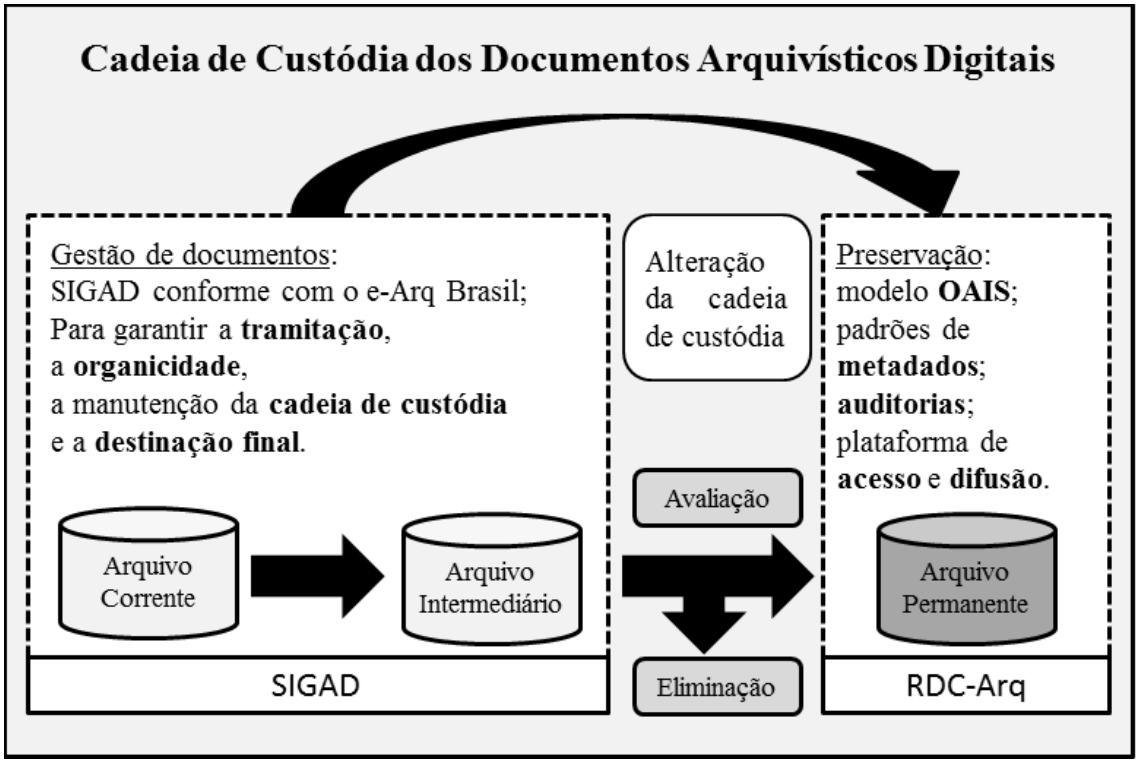
As responsabilidades do OAIS estão relacionadas às políticas de preservação digital, já o fluxo de informação, através das entidades, está relacionado ao gerenciamento dos objetos digitais admitidos, custodiados e disseminados. Tais questões são aprofundadas na ISO 14721:2012, além de definir um modelo lógico para os tipos de informações arquivadas.

Após esta breve explanação do OAIS na implementação de um RDC-Arq, procede-se a caracterização da cadeia de custódia para documentos arquivísticos em ambiente digital. Desta forma, contextualizam-se os principais componentes envolvidos no sistema de gestão de documentos, comportando desde a produção e tramitação até a preservação e acesso.

3. CADEIA DE CUSTÓDIA DOCUMENTAL

Os documentos arquivísticos em sua trajetória administrativa e histórica perpassam três fases que são: corrente, intermediária e permanente. Desta forma, têm-se dois sistemas informatizados distintos, que são o Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e o RDC-Arq, envolvidos em uma cadeia de custódia ininterrupta. Inicialmente, o SIGAD será responsável pelas fases corrente e intermediária, já o RDC-Arq será responsável pela fase permanente. A relação entre os sistemas informatizados é esquematizada na "Figura 2 – Cadeia de Custódia dos Documentos Arquivísticos Digitais".

Figura 2 – Cadeia de Custódia dos Documentos Arquivísticos Digitais



Fonte: adaptado de Flores, Rocco e Santos (2016).

As fases corrente e intermediária compõe o ambiente da gestão de documentos, enquanto a fase permanente compõe o ambiente da preservação e acesso. Assim, o SIGAD deverá considerar Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-Arq Brasil), enquanto o RDC-Arq considerar o modelo OAIS. Estes dois ambientes distintos devem ser unidos por uma cadeia de custódia ininterrupta que irá corroborar na presunção de

autenticidade e confiabilidade do sistema para gestão de documentos no seu sentido mais amplo, o organizacional.

Neste sistema, o SIGAD será responsável pela tramitação dos documentos, e deverá manter sua classificação e organicidade. Além disso, o SIGAD deve implementar rotinas de presunção de autenticidade, garantindo que não foram realizadas alterações não autorizadas e nem documentadas. Depois de encerrado o valor primário dos documentos nas fases corrente e intermediária, estes serão avaliados pelo SIGAD com base em uma tabela de temporalidade previamente definida. Desta forma, documentos sem valor secundário serão eliminados do sistema, e os documentos que possuírem um valor secundário (valor histórico, social, probatório ou informativo) serão recolhidos ao arquivo permanente.

Este é um ponto crítico no sistema para gestão de documentos, visto que os documentos armazenados em um sistema são transferidos para outro (do SIGAD para o RDC-Arq). Além disso, poderá ocorrer a mudança do custodiador (abordagem pós-custodial), ou seja, uma instituição será responsável pelas fases corrente e intermediária e, outra instituição ficará responsável pela guarda dos documentos permanentes. Esta possibilidade rompe com um dos paradigmas Arquivísticos, pois tradicionalmente, a instituição produtora era a mesma responsável pela custódia de seus documentos permanentes. Assim, o advento do documento arquivístico digital traz este pertinente questionamento: a pós-custódia.

O ambiente de preservação consiste em um local denominado arquivo permanente, no qual será implementado o repositório digital em conformidade com o modelo OAIS, além de seguir princípios arquivísticos, sendo assim, um RDC-Arq. Este será o ambiente autêntico para preservação de longo prazo, e estará isolado dos usuários externos a fim de minimizar possíveis invasões. Para isto, utiliza uma plataforma de acesso pela qual os usuários irão solicitar acesso aos materiais. Este procedimento acrescenta maiores níveis de segurança, pois, o RDC-Arq será monitorado constantemente e os usuários não terão acesso direto aos seus conteúdos, somente à plataforma de acesso.

Caso a plataforma de acesso seja invadida não ocorrerão danos contra os materiais armazenados no RDC-Arq, pois é este quem envia os dados solicitados a plataforma. A plataforma de acesso não acessa os materiais armazenados no RDC-Arq, ela solicita o envio destes materiais que lhe são solicitados pelos usuários.

4. REQUISITOS DO ACTDR

Ao abordar repositórios arquivísticos, delimita-se o horizonte de aplicação do OAIS, e consequentemente, do ACTDR. Ambos os modelos fazem menções genéricas ao "repositório digital", não entrando em especificidades da área de arquivo. Desta forma, muitos princípios arquivísticos estão subentendidos nos requisitos do OAIS e do ACTDR, sendo assim, esta seção tem por objetivo ressaltar o ponto de vista arquivístico frente aos requisitos do ACTDR.

Para realizar a análise proposta optou-se por manter os requisitos estruturados conforme o próprio documento do ACTDR, mantendo os códigos da numeração adotada por este documento para facilitar o entendimento. Desta forma, apresenta-se uma breve definição, **complementar**, para cada seção, subseção e requisitos, que estabelece um diálogo entre o ACTDR e a Arquivística.

[3] **INFRAESTRUTURA ORGANIZACIONAL**

Estas questões estão diretamente relacionadas às políticas institucionais para preservação de documentos, e delineiam o planejamento organizacional e o funcionamento legal do arquivo responsável pela custódia documental.

[3.1] GOVERNANÇA E VIABILIDADE ORGANIZACIONAL

Consiste em definir a missão do repositório e assumir o compromisso com a preservação e o acesso em longo prazo. Para isto, são definidos de forma explícita, os planos de sucessão e a política de recolhimento para custódia. Um RDC-Arq deve declarar o seu compromisso com a preservação dos documentos de tal caráter, e definir previamente quaisquer alterações na custódia, de modo a designar os requisitos a serem cumpridos por um eventual "novo custodiador".

[3.1.1] **Ter uma declaração de missão que reflete um compromisso de preservação, de retenção no longo prazo, de gestão, e de acesso à informação digital**: tal declaração pode ser facilmente realizada por uma instituição arquivística, visto que esta tem o compromisso em preservar

documentos arquivísticos. Mesmo assim, destaca-se a importância de reafirmar este compromisso, com a menção de termos como “documentos arquivísticos digitais”, “repositório arquivístico digital”, o que define claramente um compromisso em preservar os registros em ambiente informatizado.

[3.1.2] **Ter um plano estratégico de preservação definido que o aproxime de sua missão apoiando o seu cumprimento no longo prazo**: a preservação de documentos arquivísticos digitais exige uma série de recursos para garantir a sustentabilidade do arquivo no longo prazo. Logo, é preciso que estes recursos estejam previamente definidos no plano estratégico de preservação.

[3.1.2.1] **Ter um plano de sucessão, contingência e/ou acordos judiciais apropriados caso em algum momento, o repositório cesse a sua atividade ou o governo ou instituição de financiamento altere substancialmente o seu âmbito**: é essencial definir previamente os possíveis rumos dos documentos preservados em caso de alterações que gerem impacto direto no custodiador. Alterar recursos financeiros ou mesmo o responsável pela custódia documental implica em reformular o processo de preservação. Para isto, deve garantir todas as informações e permissões necessárias para que o novo custodiador consiga executar as atividades de preservação necessárias.

[3.1.2.2] **Controlar seu ambiente organizacional para determinar quando deve executar o seu plano de sucessão, contingência e/ou acordos judiciais**: o arquivo enquanto instituição deve estar ciente das influências que circundam o ambiente de preservação, analisando questões políticas e econômicas para definir a viabilidade de continuar preservando tais conteúdos. Assim, caso não seja sustentável, o RDC-Arq deve proceder à sucessão dos conteúdos, e repassar a responsabilidade pela custódia;

[3.1.3] **Ter uma política de recolhimento ou documentação que especifique o tipo de informação que irá preservar e garantir acesso**: no caso de um

RDC-Arq, os conteúdos a serem admitidos devem ser exclusivamente, documentos arquivísticos. Também será preciso identificar e distinguir os produtores, caso os documentos tenham mais de uma proveniência, e assim, registrar com precisão os procedimentos utilizados durante a aquisição. Isto irá manter a proveniência dos acervos, respeitando os princípios arquivísticos.

[3.2] ESTRUTURA ORGANIZACIONAL E DE PESSOAL

Compreende a gestão das competências de pessoal necessárias para o cumprimento das funções do repositório. Definir o organograma qual explícita a divisão de funções e responsabilidades. Além disso, incentiva o desenvolvimento pessoal, auxilia a formação continuada para desenvolver habilidades e gerar novos conhecimentos. Desta forma, a equipe do arquivo deve estar em constante atualização, visto que os documentos em ambiente digital impõem novos desafios frente ao profissional arquivista, o qual vivencia uma transição dos acervos analógicos para acervos mistos (analógicos e digitais).

[3.2.1] **Identificar e estabelecer as funções que deve executar, bem como dispor de pessoal com qualificação e experiência para tal**: os funcionários devem ser capacitados conforme surjam as demandas relacionadas à evolução das tecnologias. Este ponto é fundamental, pois as tecnologias da informação e comunicação evoluem em um ritmo cada vez mais acelerado. Tal fato tem ocasionado ciclos de obsolescência cada vez mais curtos, o que torna o processo de atualização dos funcionários tão essencial quanto à atualização tecnológica.

[3.2.1.1] **Identificar e estabelecer seus deveres**: o RDC-Arq deve estar ciente de suas atividades e demonstrar capacidade de cumpri-las, a fim de garantir a sua sustentabilidade no logo prazo.

[3.2.1.2] **Ter o número adequado de funcionários para realizar todas as funções e serviços**: no contexto de um RDC-Arq, ressalta-se a necessidade de uma equipe interdisciplinar/multidisciplinar. Assim,

profissionais de diversas áreas dialogando entre si, corroboram para o cumprimento das atividades do RDC-Arq, e com isso, eleva-se a qualidade dos serviços prestados.

[3.2.1.3] **Colocar em prática um programa de desenvolvimento profissional ativo que oferece oportunidades de desenvolvimento de competências ao pessoal**: este é um requisito de aprendizagem, pelo qual o RDC-Arq acompanha a evolução das tecnologias, dos procedimentos e da própria comunidade designada. Todo arquivo que preserva documentos em um repositório digital deve manter um plano de atualização tecnológica. Isto se faz necessário por causa da constante evolução das tecnologias aliado a necessidade de fornecer acesso aos conteúdos autênticos e inteligíveis.

[3.3] POLÍTICAS DE RESPONSABILIDADE E PRESERVAÇÃO

O repositório deve definir a comunidade designada e a base de conhecimento, além de possuir políticas para o cumprimento dos serviços, acompanhar a evolução das tecnologias e da comunidade designada, e receber o *feedback* de produtores e consumidores. Outro fator pertinente é manter ações transparentes de preservação, registro das transformações da informação e da avaliação de integridade, desta forma, é possível manter um calendário regular para certificação.

[3.3.1] **Definir a sua comunidade designada e a base de conhecimento associada, e manter essas definições de forma acessível**: no caso de um RDC-Arq, a comunidade designada assume um caráter muito abrangente e genérico, visto que os documentos preservados correspondem, por vezes, desde uma parcela significativa da sociedade até a nação como um todo.

[3.3.2] **Ter políticas de preservação para garantir que seu plano estratégico de preservação será cumprido**: as políticas irão mostrar como o RDC-Arq cumpre os requisitos do plano estratégico de preservação. Desta

forma, as políticas de preservação do arquivo devem ter claras menções ao repositório e aos documentos digitais.

[3.3.2.1] **Ter mecanismos de revisão, atualização e desenvolvimento permanente das suas políticas de preservação, os quais irão monitorar o crescimento do repositório, assim como a evolução da tecnologia e da prática da comunidade**: tais políticas devem ser compreensíveis pela equipe do RDC-Arq para auxiliar no trabalho. Logo, a revisão deve centrar-se em manter o caráter arquivístico dos documentos, de modo que as tecnologias sejam adaptadas aos princípios da Arquivística, e nunca o contrário.

[3.3.3] **Manter um histórico documentado das alterações em suas operações, procedimentos, *software* e *hardware***: a preservação de documentos arquivísticos requer o constante monitoramento e registro dos procedimentos, a fim de verificar a sua evolução, seja de tecnologia, seja de procedimentos. Isto possibilita futuras análises sobre as decisões tomadas, verificando os pontos assertivos e os equívocos.

[3.3.4] **Manter a transparência e responsabilidade em todas suas ações, além de apoiar a operação e a gestão do repositório no que tange a preservação de conteúdos digitais no longo prazo**: além dos padrões amplamente conhecidos pela comunidade de preservação digital, o RDC-Arq pode demonstrar que segue recomendações como as do Conselho Nacional de Arquivos, e realiza práticas orientadas ao projeto InterPARES, entre outros estudos pertinentes.

[3.3.5] **Definir, coletar, rastrear e fornecer adequadamente as suas medições integridade das informações**: a verificação da integridade é um procedimento essencial para RDC-Arq's, de modo que estes documentos em ambiente digital tornam-se extremamente vulneráveis, e podem ser modificados/falsificados com facilidade e sem deixar vestígios aparentes.

[3.3.6] **Comprometer-se a um calendário regular de autoavaliação e certificação externa**: um repositório arquivístico deve se submeter a auditorias periódicas para que possa ser denominado como “confiável”, tornando-se um RDC-Arq. Ressalta-se que este não é um procedimento definitivo, o qual precisa ser reafirmado por meio de nova auditoria e consequente certificação. Assim, por meio uma constante caracterização de confiança, o repositório mantém-se confiável perante a comunidade de preservação e comunidade designada.

[3.4] SUSTENTABILIDADE FINANCEIRA

Compreende a definição de processos de planejamento para curto e longo prazo, com ajustes periódicos. Assim, preconizam-se procedimentos financeiros transparentes com auditoria, além de monitorar continuamente os riscos, benefícios, investimentos e despesas, buscando solução para problemas de financiamento.

[3.4.1] **Dispor de processos de planejamento de negócios no curto e no longo prazo, para garantir a sustentabilidade ao longo do tempo**: em se tratando de um RDC-Arq, este tem o compromisso inato com a preservação e o acesso á documentos no longo prazo. Isto porque a finalidade da Arquivística consiste em preservar e garantir acesso.

[3.4.2] **Ter procedimentos financeiros transparentes, em conformidade com normas e práticas contábeis relevantes, e ser auditado por terceiros, em conformidade com os requisitos legais de seu respectivo território**: este requisito está estreitamente ligado a questões administrativas e contábeis do RDC-Arq. A transparência atua como um meio para gerar confiança na gestão financeira, não entrando em aspectos do campo teórico da Arquivística.

[3.4.3] **Comprometer-se em analisar e informar continuamente sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos)**: desta forma, o repositório irá manter o equilíbrio

adequado entre o risco e benefício, investimentos e retorno. Assim, um RDC-Arq deve manter uma estrutura próxima do ideal, de modo a considerar a relação custo/benefício. No entanto, a otimização de recursos não deve se sobrepor a necessidade de implementação de determinados requisitos necessários à preservação e garantia de acesso a documentos autênticos.

[3.5] CONTRATOS, LICENÇAS E PASSIVOS

Consiste em manter contratos ou acordos de depósito apropriados aos materiais digitais de outra organização, capazes de especificar e transferir todos os direitos de preservação necessários. Da mesma forma, permite rastrear e gerenciar os direitos de propriedade intelectual e possíveis restrições sobre o uso do conteúdo, definindo as políticas com base na legislação para conteúdos digitais com propriedade ou direitos não especificados claramente.

[3.5.1] **Manter contratos ou acordos de depósito apropriados para materiais digitais que ele gerencia, preserva e/ou fornece acesso**: o RDC-Arq deve possuir as permissões legais (autorizações, contratos e licencas) necessárias para recolher e preservar uma determinada informação, corroborando com formação da sua imagem enquanto custodiador.

[3.5.1.1] **Ter contratos de depósito que especificam a transferência de todos os direitos de preservação necessários, e que esses direitos estejam documentados**: alterar a informação digital é uma tarefa necessária para preservá-la em um RDC-Arq. Determinadas tecnologias tornam-se obsoletas, logo é necessário migrar para novos suportes e formatos de arquivo para continuar acessando os conteúdos;

[3.5.1.2] **Especificar todos os aspectos relevantes de aquisição, manutenção, acesso e retirada de conteúdos, através de acordos documentados com os depositantes e outras partes relevantes**: o RDC-Arq assume a responsabilidade da preservação, manutenção e garantia de acesso aos documentos, e paralelamente, negocia aspectos da submissão

do SIP junto aos produtores de conteúdos. Desta forma, é possível estabelecer que os conteúdos submetidos devam estar em conformidade com determinadas normas ou padrões recomendados pelo repositório.

[3.5.1.3] **Ter políticas documentadas que indiquem quando ele aceita a responsabilidade de preservação dos conteúdos de cada conjunto de objetos de dados submetidos**: este requisito formaliza a aceitação da responsabilidade pela custódia dos materiais submetidos ao RDC-Arq, e fornece documentação para as partes interessadas comprovando a transferência e as condições para que o compromisso seja firmado.

[3.5.1.4] **Ter políticas para atender as responsabilidades e os desafios relacionados às questões de propriedade/direitos**: ter políticas de preservação que mantenham a conformidade com leis e requisitos pertinentes irá minimizar as responsabilidades potenciais do RDC-Arq. Logo, o RDC-Arq terá maior controle dos documentos arquivísticos custodiados, o que corrobora para cumprir suas atividades relacionadas á preservação e garantia de acesso.

[3.5.2] **Controlar e gerenciar os direitos de propriedade intelectual e restrições à utilização do conteúdo conforme exigido pelo contrato, acordo de depósito ou licença**: isto permite que o RDC-Arq identifique quaisquer impedimentos relacionados ao processo de preservação e acesso, de modo que defina políticas para solucionar tais problemas. Assim, verificam-se restrições com relação à alteração das informações, bem como as restrições para difusão e acesso de conteúdos.

[4] GESTÃO DE OBJETOS DIGITAIS

A seção gestão de objetos digitais compreende aspectos relacionados à aquisição de conteúdo, criação do pacote de arquivamento, plano da preservação, preservação e manutenção dos AIP's, gestão da informação, e gestão de acesso.

[4.1] ADMISSÃO: AQUISIÇÃO DE CONTEÚDO

Permite identificar as propriedades significativas dos objetos digitais que serão preservadas, para isto, são associadas às informações necessárias ao pacote SIP. As fontes de proveniência dos objetos admitidos devem ser autenticadas, e devem-se executar as correções necessárias a cada SIP submetido. Além disso, é preciso obter controle físico dos objetos digitais para preservá-los, e fornecer respostas adequadas ao produtor durante o processo de submissão.

[4.1.1] **Identificar as informações de conteúdo e as propriedades da informação que serão preservadas**: o RDC-Arq define quais aspectos da informação de conteúdo são pertinentes à preservação, informando assim, aos seus colaboradores.

[4.1.1.1] **Ter procedimento(s) para identificar as propriedades da informação que serão preservadas**: o RDC-Arq estabelece os métodos e fatores utilizados para determinar os aspectos de diferentes tipos de informação de conteúdo para os quais assume a responsabilidade de preservação frente à comunidade designada. Ressalta-se que tais características são essenciais para a presunção de autenticidade, bem como para a interpretação/representação da informação de conteúdo.

[4.1.1.2] **Ter um registro das informações de conteúdo e das propriedades de informação que serão preservadas**: o RDC-Arq terá definido o que será preservado, e assim, firmar o compromisso com tais tipos de informação previamente definidas. Posterirormente, a demonstração do cumprimento deste requisito é um importante passo para demonstrar a capacidade de preservar documentos de forma confiável.

[4.1.2] **Especificar claramente, no momento do depósito, qual informação precisa ser respectivamente associada com a informação de conteúdo**: o nível de precisão destas especificações irá variar conforme as políticas de cobrança e sua relação aos produtores. Logo, o RDC-Arq deverá buscar junto

ao produtor toda a informação necessária para representar corretamente os documentos recolhidos.

[4.1.3] **Ter especificações adequadas que permitam reconhecer e analisar os SIP's**: o repositório poderá analisar o conteúdo de um determinado objeto digital e verificar se a sua estrutura lógica corresponde ao formato de arquivo que representa. Tal procedimento é pertinente, pois os formatos de arquivo podem não refletir o que realmente são. Um documento de texto pode estar equivocadamente representado em um formato de imagem, o que resulta em erro de interpretação/representação da informação de conteúdo.

[4.1.4] **Ter mecanismos para verificar adequadamente a identidade do produtor de todos os materiais**: garante que o RDC-Arq irá determinar corretamente a procedência de cada SIP recebido, mantendo um dos princípios essenciais da Arquivística, o princípio da proveniência.

[4.1.5] **Ter um processo de admissão que verifique a integralidade e precisão de cada SIP**: o RDC-Arq deve ter um rígido controle de admissão de conteúdos, de modo que os pacotes AIP reflitam as informações de conteúdos dos pacotes SIP. Isto é essencial para demonstrar que o RDC-Arq está cumprindo com seus compromissos de preservação da integridade e demais compromissos firmados frente aos produtores.

[4.1.6] **Obter controle suficiente sobre os objetos digitais para preserva-los**: o RDC-Arq necessita obter o controle dos documentos a fim de efetuar as atividades necessárias para sua preservação, assim como para prover o acesso à comunidade designada. Isto requer o controle legal e físico/lógico, de modo que isto seja suficiente para tomada de decisões relativas às suas atividades.

[4.1.7] **Fornecer ao produtor/depositante respostas apropriadas aos pontos que foram definidos durante os processos de admissão**: o RDC-Arq deverá manter o produtor informado sobre os procedimentos de admissão,

de modo que seja possível demonstrar a conformidade com as questões definidas previamente.

[4.1.8] **Ter registros contemporâneos de ações e processos de administração que são relevantes para aquisição de conteúdo**: o RDC-Arq deve registrar todos os procedimentos administrativos para manter um histórico das ações realizadas, servindo para comprovar a execução de determinado procedimento. Ressalta-se que tais procedimentos administrativos são essenciais na presunção de autenticidade, e o seu registro adiciona confiabilidade ao ambiente informatizado.

[4.2] ADMISSÃO: CRIAÇÃO DO AIP

Durante a criação do AIP define-se um identificador único de nomenclatura geral para cada AIP ou classe de informação, que demonstra a preservação de suas propriedades significativas. As transformações dos SIP's em AIP's são descritas, além de manter os identificadores únicos previamente associados. Um contexto semântico entre objetos digitais armazenados é estabelecido, e as informações de representação admitidas são registradas. Assim, devem-se documentar os processos de aquisição e gerenciamento dos metadados de preservação para as informações de conteúdo associadas, além de adquirir outros metadados necessários à preservação. O processo de criação do AIP ainda requer a verificação da compreensão da informação de conteúdo, da integridade e da precisão de cada AIP. De forma complementar, deve-se fornecer um mecanismo para auditoria da integridade dos materiais custodiados, e manter registros de metadados de processos administrativos pertinente à preservação.

[4.2.1] **Ter para cada AIP ou classe de AIP preservada, uma definição associada adequada para analisar o AIP e contemplar suas necessidades de preservação de longo prazo**: o RDC-Arq terá mais informações e assim poderá complementar as atividades de preservação.

[4.2.1.1] **Ter capacidade de identificar qual definição se aplica para qual AIP**: o RDC-Arq pode usar o método que considerar mais apropriado para associar as definições e os AIP's.

[4.2.1.2] **Ter uma definição adequada de cada AIP para sua preservação no longo prazo, permitindo identificar e analisar todos os componentes necessários dentro desse AIP**: o RDC-Arq deverá identificar e manter uma relação dos componentes necessários para preservar as propriedades significativas dos AIP's. Além disso, será necessário demonstrar, periodicamente por meio da revisão, que tais componentes satisfazem as necessidades de preservação.

[4.2.2] **Ter uma descrição de como o AIP é construído a partir SIP:** permite que o RDC-Arq demonstre que a informação de conteúdo armazenada na forma de AIP está em conformidade com aquela submetida originalmente pelo produtor na forma de SIP. Para tal, é necessário detalhar como ocorreram as transformações necessárias ao armazenamento. Esta descrição corrobora para demonstrar a autenticidade das informações de conteúdo, pois justifica as suas possíveis transformações, relacionando-as à necessidade de alterar a informação digital para melhor preservá-la. O registro destas ações também auxilia no processo de presunção de autenticidade dos documentos.

[4.2.3] **Documentar a disposição final de todos os SIP's**: o RDC-Arq deve registrar os procedimentos relativos ao tratamento dos SIP's, e assim, indicar sua localização enquanto AIP ou eliminação, em casos especiais.

[4.2.3.1] **Seguir os procedimentos documentados, caso um SIP não seja incorporado em um AIP ou descartado, deve-se justificar o motivo**: o RDC-Arq terá de registrar o motivo das exclusões de SIP's submetidos de forma equivocada, quando houver, visto que os documentos arquivísticos submetidos/recolhidos ao RDC-Arq não devem ser eliminados ou recusados de forma arbitrária. Logo, é necessário justificar a natureza do equívoco/erro

ou mesmo inconformidade dos SIP's com as normas de submissão definidas previamente pelo RDC-Arq.

[4.2.4] **Utilizar uma convenção que gera identificadores únicos para todos os AIP's**: com os identificadores únicos para cada AIP e componentes, o RDC-Arq poderá fazer verificações, inibindo duplicações.

[4.2.4.1] **Identificar cada AIP de forma exclusiva no repositório**: garante precisão no processo de busca e recuperação da informação de conteúdo

[4.2.4.1.1] **Ter identificadores exclusivos**: evita duplicações dos AIP's e otimiza a sua localização no sistema.

[4.2.4.1.2] **Ceder e manter identificadores persistentes do AIP e de seus componentes, de modo a ser exclusivo dentro do contexto do repositório**: evita a dispersão dos componentes digitais relacionados ao AIP.

[4.2.4.1.3] **Descrever todos os processos utilizados para realizar alterações em tais identificadores**: acrescenta confiabilidade ao sistema de identificadores.

[4.2.4.1.4] **Fornecer uma lista completa de todos os identificadores e fazer verificações pontuais para identificar duplicações**: permite verificar continuamente a presença de informações duplicadas no RDC-Arq, além de localizar os conteúdos com precisão, desta forma, auxilia na otimização do trabalho técnico e do armazenamento.

[4.2.4.1.5] **O sistema de identificadores deve ser adequado para comportar a demanda atual do repositório e as previsíveis necessidades futuras, tais como números de objetos**: o RDC-Arq garante a capacidade de recuperar a informação de conteúdo desejada com alto grau de precisão, o que é essencial para que comunidade

designada demonstre confiabilidade quanto á preservação. A identificação está prevista pela Norma Brasileira de Descrição Arquivística (NOBRADE) (BRASIL, 2006), em seus elementos de descrição pode-se observar que o item “1 área de identificação” possui o subitem “1.1 código de referência” o qual tem como objetivo identificar a unidade de descrição. Esta identificação[3] perpassa, obrigatoriamente, o registro do código do país (BR), o código da entidade custodiador e o código específico da unidade de descrição (BRASIL, 2006). Com a Resolução nº 28, de 17 de fevereiro de 2009, publicada pelo Conarq, a instituição terá esta identificação ao realizar o Cadastro Nacional de Entidades Custodiadoras de Acervos Arquivísticos (CODEARQ) a qual deverá ser solicitada ao Conarq. Por consequência, os acervos cadastrados terão códigos padronizados o que facilita a distinção entre as instituições cadastradas. Esta resolução também recomenda o suso da NOBRADE aos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR) (BRASIL, 2009).

[4.2.4.2] **Ter um sistema de confiável de ligação/localização para encontrar o objeto identificado exclusivamente, independentemente da sua localização física**: o RDC-Arq deve localizar o AIP e seus respectivos componentes mesmo que sejam realizadas atualizações no sistema, na mídia ou local de armazenamento. Ou seja, deve haver um monitoramento contínuo capaz de recuperar tais informações.

[4.2.5] **Ter acesso a ferramentas e recursos para fornecer informação de representação de autoridade necessária para todos os objetos digitais armazenados**: identificar os formatos de arquivo dos objetos digitais a fim de fornecer a informações de representação necessária a comunidade designada.

[4.2.5.1] **Identificar o tipo de arquivo de todos os objetos de dados submetidos**: isto permite que o RDC-Arq controle os formatos de arquivo

[3] Por exemplo, o código “BR AN Q6.LEG.COR,TEL” pertence a instituição “Arquivo Nacional do Brasil”, e corresponde a a subsérie Telegramas, nível 3,5, do fundo Floriano Peixoto, seção Governo Legal, série Correspondência (BRASIL, 2006).

em que os documentos são submetidos. Esta informação de monitoramento poderá ser útil para buscar melhores técnicas de tratamento para um determinado formato de arquivo.

[4.2.5.2] **Determinar a informação de representação necessária para tornar cada objeto de dados compreensível à comunidade designada**: o RDC-Arq deve reunir toda a informação necessária para a correta interpretação/representação dos objetos digital pela comunidade designada. Desta forma, além de cumprir as funções de preservação será necessário fornecer acesso de forma inteligível à documentação.

[4.2.5.3] **Ter acesso à informação de representação necessária**: o RDC-Arq deve buscar a informação de representação necessária junto aos produtores, desta forma, um processo de organização da informação determinará os componentes digitais que serão relacionados aos AIP's.

[4.2.5.4] **Assegurar que os requisitos da informação de representação são persistentemente associados aos objetos de dados relevantes**: o RDC-Arq terá a informação de representação suficiente para manter os objetos digitais acessíveis à comunidade designada. Para isto deverá ter acesso a ferramentas que executem tais atividades.

[4.2.6] **Ter processos documentados para aquisição de PDI, conforme os processos documentados, para sua informação de conteúdo associada**: o RDC-Arq deve assegurar a reunião de todos os componentes de PDI necessários, e manter um mecanismo padronizado para coleta destes dados.

[4.2.6.1] **Ter processos documentados para a aquisição de PDI**: o RDC-Arq definirá os procedimentos padronizados para adquirir a PDI necessária à representação da informação de conteúdo.

[4.2.6.2] **Executar processos documentados para a aquisição de PDI**: o RDC-Arq seguirá seus procedimentos de aquisição de PDI conforme definido previamente.

[4.2.6.3] **Assegurar que a PDI é persistentemente associada às informações do conteúdo relevantes**: o RDC-Arq irá registrar informações adicionais e autorizadas, capazes de corroborar com a autenticidade dos conteúdos. Este fluxo de constante associação adicionará confiabilidade aos procedimentos de aquisição de PDI.

[4.2.7] **Assegurar que as informações de conteúdo do AIP, no momento de sua criação, são compreensíveis à comunidade designada**: é essencial que o RDC-Arq crie AIP's já compreensíveis a comunidade designada. Assim, caso haja solicitações de acesso, o repositório irá dispor de toda a informação necessária que permita aos usuários interpretar corretamente a informação de conteúdo.

[4.2.7.1] **Ter um processo documentado para testar, no momento de sua criação, se a informação de conteúdo do AIP é compreensível à comunidade designada**: o RDC-Arq deve verificar logo no momento da criação do AIP, se a informação de conteúdo está acessível à comunidade designada. Assim, poderá inserir mais informações caso seja necessário para representar/interpretar as informações de conteúdo.

[4.2.7.2] **Executar um teste para cada classe de informação de conteúdo dos AIP's**: após reunir todos os componentes considerados necessários para a compreensão da informação de conteúdo pela comunidade designada é preciso executar testes para verificar cada componente do AIP.

[4.2.7.3] **Em caso de falha no teste de compreensibilidade, o repositório deve colocar as informações de conteúdo dos AIP's no nível de compreensão necessário**: caso as informações de conteúdo do AIP não sejam compreensíveis à comunidade designada, o RDC-Arq ficará

responsável por buscar informações adicionais e acrescentá-las ao pacote AIP.

[4.2.8] **Verificar a integralidade e exatidão de cada AIP no momento de sua criação**: o RDC-Arq deve manter uma descrição capaz de relacionar o AIP armazenado com o SIP submetido pelo produtor, de modo que este consiga recuperar as informações de conteúdo com integridade e precisão.

[4.2.9] **Fornecer um mecanismo independente para verificar a integridade do conjunto de conteúdos do repositório**: o RDC-Arq deverá ter um mecanismo independente para verificar a integridade do acervo, identificando cada AIP e seus componentes relacionados. Isto é relevante para garantir princípios arquivísticos como o da proveniência e da integridade dos fundos. Tal verificação auxilia para reunir toda a informação necessária para a correta interpretação/representação das informações de conteúdo pela comunidade designada.

[4.2.10] **Ter registros contemporâneos das ações e processos de administração que são relevantes à criação do AIP**: o RDC-Arq demonstra que segue uma política de criação de AIP's previamente definida. Além disso, poderá registrar ações relevantes com o uso de metadados de preservação devidamente associados a todos os componentes digitais.

[4.3] PLANEJAMENTO DA PRESERVAÇÃO

Dentre as questões relacionadas ao planejamento da preservação, ressalta-se que o repositório irá identificar e documentar as estratégias de preservação executadas. Irá notificar quando a informação de representação adquirir risco de obsolescência, alterar os planos de preservação conforme os resultados do monitoramento, e podem fornecer evidências da eficácia do planejamento de preservação.

[4.3.1] **Ter uma documentação sobre as estratégias de preservação relevantes ao acervo**: tais estratégias definidas pelo RDC-Arq em seu plano estratégico de preservação buscam solucionar riscos como a degradação dos meios de armazenamento, a obsolescência das unidades de mídia, e a obsolescência ou inadequação da informação de representação (incluindo formatos de arquivo).Desta forma, o repositório terá registrado todas as estratégias pertinentes à preservação e manutenção da autenticidade dos documentos.

[4.3.2] **Ter mecanismos para monitorar o ambiente de preservação**: através do monitoramento do ambiente de preservação o RDC-Arq poderá tomar as decisões mais adequadas para realizar a manutenção dos objetos digitais, e minimizar os efeitos da obsolescência. Assim, irá assegurar a que a comunidade designada será capaz de compreender e utilizar os materiais preservados.

> [4.3.2.1] **Ter mecanismos para monitorar e notificar quando a informação de representação está inadequada à compreensão dos dados pela comunidade designada**: o RDC-Arq deve manter mecanismos para verificar a obsolescência no que tange a base de conhecimento da comunidade designada. E desta forma, poderá atualizar ou adicionar a informação de representação necessária para garantir a correta interpretação/representação da informação de conteúdo.

[4.3.3] **Ter mecanismos para mudar o plano de preservação conforme os resultados das atividades de monitoramento**: com o monitoramento do ambiente de preservação, o RDC-Arq terá condições previstas para alterar o planejamento definido e se adequar aos imprevistos e as novas necessidades que surjam durante a execução do plano de preservação. Da mesma, forma poderá reunir informações adicionais que corroborem com a preservação e interpretação dos objetos digitais.

[4.3.3.1] **Ter mecanismos para criar, identificar ou reunir qualquer informação de representação adicional que seja necessária**: o RDC-Arq identificará a informação de representação e os formatos de arquivo potencialmente obsoletos e, por conseguinte, proceder à atualização ou adicionar maiores informações que auxiliem no processo de preservação.

[4.3.4] **Apresentar provas da eficácia das atividades de preservação**: o RDC-Arq demonstrará capacidade de preservação continuada da informação de conteúdo ao permitir auditorias (testes aleatórios) que comprovam a eficácia dos métodos, além de garantir a sua correta representação/interpretação.

[4.4] PRESERVAÇÃO DO AIP

Preservar as informações de conteúdo dos AIP's requer a implementação de estratégias de preservação documentadas por metadados adequados registrando as ações aplicadas para especificar o seu tratamento. Além disso, o RDC-Arq deve monitorar continuamente a integridade dos AIP's, e manter o registro de ações e processos administrativos pertinentes à preservação.

[4.4.1] **Ter especificações sobre a forma como os AIP's são armazenados até o nível de *bit***: o RDC-Arq poderá recuperar as informações de conteúdo do AIP devido ao conhecimento sobre os formatos, de modo que poderá extrair a informação contida no AIP em qualquer tempo.

[4.4.1.1] **Preservar as informações de conteúdo do AIP**: o RDC-Arq manterá um registro de todas as transformações realizadas sobre as informações de conteúdo recebidas. Caso sejam necessárias conversões ou informações adicionais, todos estes procedimentos estarão registrados, compondo um testemunho do histórico dos objetos digitais. Logo, este registro irá garantir a autenticidade dos conteúdos em custódia.

[4.4.1.2] **Monitorar ativamente a integridade do AIP**: O RDC-Arq manterá um processo regular de verificação da integridade para cada objeto digital admitido e adicionará informações de fixidez, as quais irão auxiliar na presunção de autenticidade, além de reparar os objetos que estão corrompidos.

[4.4.2] **Ter registros contemporâneos das ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIP's**: o RDC-Arq deverá demonstrar, através de documentação e registros de metadados, que todas as ações relevantes são realizadas. Tal procedimento agregará confiabilidade às decisões administrativas relacionadas aos AIP's.

[4.4.2.1] **Ter procedimentos definidos para todas as ações tomadas em um AIP**: o RDC-Arq deve respeitar uma variabilidade limitada, a qual é um parâmetro entre as necessidades de alterar as informações de conteúdo e de manter as propriedades significativas. Com isto, a informação de conteúdo poderá sofrer alterações desde que mantenham as propriedades significativas requeridas para manutenção da sua autenticidade. Logo, as transformações realizadas pelo repositório não devem descaracterizar os objetos digitais com relação à sua representação, para isto, deve-se considerar um conjunto de alterações aceitáveis, e registrar todas as ações de alteração.

[4.4.2.2] **Demonstrar que as medidas tomadas em um AIP estão em conformidade com as especificações dessas ações**: quaisquer ações que afetem os conteúdos armazenados no RDC-Arq devem seguir procedimentos previamente estabelecidos, além de serem registrados por metadados. Desta forma, é possível demonstrar que as ações registradas pelos metadados estão em conformidade com o que foi previamente definido como "alterações aceitáveis".

[4.5] GESTÃO DA INFORMAÇÃO

Na gestão da informação o RDC-Arq captura ou cria os metadados de descrição necessários, e os associa ao AIP, para que a comunidade designada identifique os materiais de interesse. Assim, será capaz de demonstrar que a integridade referencial é criada e mantida entre todos os AIP's e suas informações descritivas associadas.

[4.5.1] **Especificar os requisitos mínimos de informação para permitir que a comunidade designada descubra e identifique o material de interesse**: o RDC-Arq deve acrescentar informações descritivas aos objetos digitais admitidos, de modo a auxiliar no processo de busca e recuperação da informação de conteúdo desejada pela comunidade designada. Logo, ressalta-se a necessidade de definir padrões de metadados assim como um vocabulário controlado para otimizar a precisão das buscas.

[4.5.2] **Capturar ou criar informação descritiva mínima e assegurar que ela está associada ao AIP**: o RDC-Arq deverá associar a informação descritiva necessária para cada AIP, esta informação adicional não precisa, necessariamente, estar inserida no pacote de informação. No entanto, é essencial que a informação descritiva esteja relacionada com cada AIP, e poderá atuar por meio de identificadores únicos para estes. Da mesma forma, a informação descritiva poderá fornecer detalhes adicionais relacionados às responsabilidades advindas do processo de admissão de conteúdos, ressalta-se que no caso do RDC-Arq, a descrição seguira os padrões preconizados pela Arquivística.

[4.5.3] **Manter ligação bidirecional entre cada AIP e sua informação descritiva**: o RDC-Arq deve estabelecer e manter informações descritivas associadas para cada AIP. Com uma relação bidirecional, pode-se localizar a informação descritiva através do AIP, como também, pode-se localizar o AIP a partir da informação descritiva.

[4.5.3.1] **Manter associação entre o AIP e as suas informações descritivas ao longo do tempo**: o RDC-Arq deve identificar qualquer interrupção entre os dados e a informação descritiva associada, para assim, garantir que ela pode ser restaurada, e com isso, os AIP's poderão ser recuperados.

[4.6] GESTÃO DE ACESSO

Com a gestão de acesso, o repositório irá documentar e comunicar opções de acesso e entrega que estão disponíveis à comunidade designada. Todas as solicitações de acesso devem são registradas, e visam atender aos requisitos do repositório e dos produtores, além de cumprir os acordos relacionados às condições de acesso. A gestão de acesso irá definir e implementar uma política de acesso segura via sistema de gerenciamento, aos contratos de depósito. Desta forma, irá demonstrar que todas as solicitações de acesso resultam em uma resposta de aceitação ou rejeição, e assim, registrar todas as falhas de gerenciamento de acesso e analisar os casos de negação de acesso.

[4.6.1] **Cumprir políticas de acesso**: o RDC-Arq deverá demonstrar que cumpre as políticas de acesso, de modo que atende todas as solicitações da comunidade designada e mantem mecanismos de autenticação de usuários para controlar o acesso.

[4.6.1.1] **Registrar e analisar todas as falhas e anomalias de gerenciamento de acesso**: o RDC-Arq irá descobrir todas as falhas relacionadas ao acesso que afetam a sua confiabilidade. Com a identificação das anomalias e vulnerabilidades o repositório poderá concentrar esforços para solucionar estas falhas.

[4.6.2] **Seguir políticas e procedimentos que permitam a disseminação objetos de digitais os quais sejam rastreáveis aos originais, com evidência de sua autenticidade**: o RDC-Arq deverá gerar pacotes DIP's em conformidade com os AIP's dos quais são derivados. Logo, torna-se

fundamental definir procedimentos padronizados para a criação do DIP garantindo a sua fidedignidade frente ao AIP.

[4.6.2.1] **Registar e agir de acordo com relatórios de problemas sobre erros nos dados ou respostas para usuários**: O RDC-Arq deverá considerar os relatórios de erros sobre as solicitações de acesso. Sendo assim, a sua confiabilidade estará relacionada à capacidade de investigar e tomar decisões com relação a tais erros. Logo, as ações tomadas pelo repositório para solucionar problemas de acesso irão agregar confiança frente à comunidade designada.

[5] INFRAESTRUTURA E SEGURANÇA DA GESTÃO DE RISCOS

A seção de infraestrutura e segurança da gestão de riscos compreende aspectos relacionados à infraestrutura técnica do sistema, e gestão de riscos.

[5.1] GESTÃO DE RISCOS DE INFRAESTRUTURA TÉCNICA

As funções de repositório devem ser suportadas pelos principais sistemas operacionais, de modo que seja possível assegurar suporte de *hardware* e *software* adequado às funcionalidades de *backup* e suficientes aos conteúdos armazenados. Assim, é possível gerenciar as quantidades e as localizações das cópias de todos os objetos digitais, e sincronizar as cópias dos objetos digitais. Além disso, o repositório irá detectar a corrupção ou perda de *bits* por meio de mecanismos de análise de erro, e informar à administração todos estes incidentes e as medidas adotadas para reparar ou substituir os dados afetados. Os processos de atualização das mídias de armazenamento, do *hardware* e da segurança *software* devem ser definidos, e registrar a gestão de mudanças, sendo necessário um processo para testar o efeito de mudanças críticas ao sistema. Desta forma, o repositório possuirá tecnologias de *hardware* e *software* apropriadas aos serviços que presta à comunidade designada, bem como, procedimentos para monitorar e avaliar a necessidade de mudanças nas tecnologias de *hardware* e/ou *software* utilizadas.

[5.1.1] **Identificar e gerir os riscos às suas operações de preservação e os objetivos associados com a infraestrutura do sistema**: o RDC-Arq deverá preconizar uma infraestrutura confiável, para isso, irá gerir os riscos relacionados às plataformas de *hardware* e *software*, buscando minimizar a dependência do sistema. Sua infraestrutura tecnológica deve ser expansível, além de possibilitar a execução de um plano de sucessão futuro, caso seja necessário.

[5.1.1.1] **Empregar relógios de tecnologia ou outra tecnologia para sistemas de notificação de monitoramento**: o RDC-Arq deve manter um monitoramento contínuo das plataformas tecnológicas, acompanhado de avaliação para identificar potenciais vulnerabilidades nos componentes do sistema.

[5.1.1.1.1] **Ter tecnologias de *hardware* adequadas aos serviços que presta para sua comunidade designada**: o RDC-Arq deverá manter plataformas de *hardware* adequadas para os serviços que presta, e considerar o *feedback* recebido par realizar ajustes no sistema. Além disso, deve-se ressaltar que a adequação dos componentes de *hardware* irá impactar em todas as funções do repositório.

[5.1.1.1.2] **Dispor de procedimentos para monitorar e receber notificações quando forem necessárias mudanças na tecnologia de *hardware***: o RDC-Arq deverá monitorar as mudanças nas plataformas de *hardware* a fim manter uma infraestrutura capaz de realizar suas funções relativas a admissão, armazenamento e acesso. O ponto fundamental deste requisito é manter a interoperabilidade entre a plataforma de *hardware* e as funções executadas pelo repositório para desenvolvê-las conforme o esperado.

[5.1.1.1.3] **Dispor de procedimentos para avaliar quando é necessário atualizar o *hardware* atual**: o RDC-Arq deverá antecipar as atualizações

de *hardware*, ao manter um constante monitoramento do sistema, verificando meios para reduzir custos e falhas.

[5.1.1.1.4] **Ter procedimentos, compromissos e financiamentos para substituir *hardware* quando a avaliação indicar tal necessidade**: o RDC-Arq deve realizar a substituição do *hardware* logo após identificar tal necessidade. Sendo assim, deve haver o compromisso da instituição, de modo que o RDC-Arq disponha de recursos financeiros suficientes, como também poderá demonstrar que o novo *hardware* será capaz de economizar recursos no decorrer de seu uso.

[5.1.1.1.5] **Ter tecnologias de *software* apropriadas para os serviços que proporciona a sua comunidade designada**: o RDC-Arq deve manter as tecnologias de *software* apropriadas para desempenhar as funções como interfaces e ferramentas para migração. Logo, é preciso considerar, em especial, o *feedback* da comunidade designada em relação aos *softwares* utilizados para a localização e recuperação/interpretação da informação de conteúdo.

[5.1.1.1.6] **Dispor de procedimentos para monitorar e receber notificações quando alterações de *software* são necessários**: o RDC-Arq deverá ter procedimentos pré-estabelecidos para verificar erros, vulnerabilidades e buscar atualizações para os *softwares* que integram o sistema de preservação digital. Além disso, é preciso atender a mudanças solicitadas pela comunidade designada para facilitar o processo de busca, recuperação e interpretação dos conteúdos. E por fim, buscar a interoperabilidade entre as plataformas de *hardware* e *software*.

[5.1.1.1.7] **Dispor de procedimentos para avaliar a necessidade de atualização do *software* atual**: o RDC-Arq deve antecipar a necessidade de atualização de *software* ao monitorar a evolução das plataformas tecnológicas. Tal ação irá minimizar riscos, evitar custos adicionais e melhorar o desempenho do sistema. Este procedimento previamente

estabelecido fundamenta-se em evitar que os *softwares* utilizados no sistema tornem-se obsoletos e comprometam as atividades desenvolvidas no âmbito do repositório.

[5.1.1.1.8] **Ter procedimentos, definir compromissos e garantir financiamentos para substituir o *software* quando a avaliação indica tal necessidade**: o RDC-Arq deverá substituir o *software* de modo a evitar falhas e consequentes perdas de dados. Assim, deve-se demonstrar a capacidade e os recursos suficientes para incorporar novas tecnologias.

[5.1.1.2] **Ter *hardware* adequado e suporte de *software* suficiente para realização do *backup* para proteger os conteúdos do repositório e acompanhar suas funções de preservação**: o RDC-Arq deve possuir plataformas de *hardware* e *software* capazes de realizar o *backup* dos objetos digitais e dos sistemas. Com o desenvolvimento de planos de *backup* será possível retomar as funções de preservação em todas as situações que ocorrerem falhas, independente do nível (objetos digitais, mídias de armazenamento, *hardwares* ou *softwares*).

[5.1.1.3] **Ter mecanismos eficazes para detectar a corrupção ou perda de *bits***: o RDC-Arq não deve tolerar perdas de dados em seus AIP e informações relacionadas. Para isto, deverá manter mecanismos que identifiquem as possíveis perdas ou corrupção de dados e executem a restauração.

[5.1.1.3.1] **Registrar e reportar à administração, todos os incidentes de corrupção ou perda de dados, e quais medidas de reparo/substituição de dados corrompidos/perdidos, deverão ser tomadas**: o RDC-Arq deve informar à administração sobre as perdas de dados e o respectivo processo de recuperação executado. Com isto, é possível identificar as fontes de falhas e reparar as vulnerabilidades em nível de *hardware*, *software*, suportes e procedimentos.

[5.1.1.4] **Ter um processo para registrar a disponibilidade de novas atualizações de segurança com base na avaliação do risco/benefício**: o RDC-Arq deve evitar as alterações e exclusões de conteúdos não autorizadas. Além disso, deve realizar atualizações de segurança em sua infraestrutura tecnológica para minimizar os riscos.

[5.1.1.5] **Deve definir processos para a mídia de armazenamento e/ou alteração de *hardware***: é fundamental que o RDC-Arq mantenha um processo de migração para as mídias de armazenamento com base nas estimativas de vida útil e análise de conservação física. Ressalta-se que no longo prazo, há maior dificuldade em se obter suporte aos componentes de *hardware*, o que aumenta a responsabilidade do RDC-Arq em buscar alternativas.

[5.1.1.6] **Identificar e documentar os processos críticos que afetam a capacidade de cumprir as responsabilidades obrigatórias**: o RDC-Arq deve ter um controle sobre todos os processos críticos que podem afetar suas responsabilidades obrigatórias, de modo seja possível compreender a necessidade destes fluxos de informação. Assim, é possível manter uma revisão buscando a melhora contínua destes procedimentos.

[5.1.1.6.1] **Ter um processo de gestão da mudança documentado, que identifica as alterações em processos críticos, os quais afetam potencialmente a capacidade do repositório para cumprir suas responsabilidades obrigatórias**: o repositório deverá ter especificações sobre os processos aplicados ao acervo relacionados às mudanças em seus processos críticos. Desta forma, é possível compreender como as mudanças foram efetuadas no sistema, e consequentemente, aprender com as mudanças. E caso seja necessário, será possível reverter ações que comprometam as atividades do RDC-Arq.

[5.1.1.6.2] **Ter um processo para testar e avaliar o efeito das mudanças em seus processos críticos**: o RDC-Arq deve avaliar as mudanças em seus processos críticos. Isto se torna essencial, pois estes processos se referem às funções primordiais que ele executa. Assim, as alterações devem ser testadas antes de sua implementação, após implementar devem ser monitoradas e caso seja necessário devem ser revertidas.

[5.1.2] **Gerir o número e a localização das cópias de todos digitais objetos**: o RDC-Arq deve ser capaz de gerir seus *backups*, de modo que consiga localizar as cópias de segurança de todos os objetos digitais custodiados. Esta localização deverá ser descrita com elevado grau de precisão, e assim considerar a localização física, o armazenamento lógico na mídia, nos sistemas e nos subsistemas.

[5.1.2.1] **Ter mecanismos para garantir que todas as cópias dos objetos digitais são sincronizadas**: o RDC-Arq deve garantir que possui cópias sincronizadas de todos os objetos digitais, para os casos em que seja necessário executar o plano para recuperação de desastres. Isto é fundamental para garantir a proteção do acervo contra sinistros e corrupções de dados, da mesma forma, o repositório deve identificar e reparar os dados corrompidos para que estes não sejam indevidamente sincronizados na forma de cópias de *backup*.

[5.2] GESTÃO DO RISCO DE SEGURANÇA

A gestão do risco de segurança auxilia o repositório a manter uma análise sistemática em relação a dados, sistemas, pessoal, planta física e segurança. O repositório determina funções, responsabilidades e autorizações relacionadas à implementação de mudanças no sistema, além de ter um plano de preparo e recuperação de desastres.

[5.2.1] **Manter uma análise sistemática dos fatores de risco da segurança associada a dados, sistemas, pessoal e instalações físicas**: o RDC-Arq deve manter uma análise contínua dos riscos relacionados ao ambiente de preservação como um todo. Isto compreende a segurança física e lógica dos dados, e sua relação com sistemas, pessoal e instalações físicas.

[5.2.2] **Implementar controles para tratar adequadamente cada um dos riscos de segurança definidos**: o RDC-Arq deve tratar cada um dos riscos identificados, para isto, pode usar normas como a ISO/IEC 27000:2018 e a ISO/IEC 17799:2005. Da mesma forma, pode-se manter um registro de problemas relacionados a ataques para prevenir sua recorrência e revisar constantemente os planos de emergência.

[5.2.3] **Definir papéis, responsabilidades e autorizações relacionadas com a implementação de mudanças no sistema**: o RDC-Arq deve atribuir as responsabilidades e recursos para implementar mudanças no ambiente. Neste sentido, as normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir, respectivamente, na atribuição de responsabilidades e posterior certificação.

[5.2.4] **Ter uma preparação adequada para desastres e um plano de recuperação documentado, incluindo pelo menos um *backup off-site* de todas as informações preservadas, juntamente com uma cópia fora do local do plano de recuperação**: o RDC-Arq deve manter o *backup* e uma cópia do plano de recuperação em um local seguro e separado do acervo, de modo a garantir a continuidade dos serviços do repositório. As normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir para minimizar os riscos do ambiente de preservação. Além disso, o repositório deve definir claramente o seu plano de desastres, considerando todos os riscos aos quais está sujeito. Desta forma, o plano de recuperação se tornará mais eficaz, caso seja necessário executá-lo.

5. CONCLUSÃO

Este manual realizou uma complementação dos requisitos do ACTDR de modo a acrescentar uma visão arquivística aos requisitos utilizados para auditoria de repositórios digitais. Sendo assim, o ACTDR é contextualizado para ser aplicado aos RDC-Arq's, considerando que este está em conformidade com o modelo OAIS e envolvido em uma cadeia de custódia confiável.

Inicialmente, o modelo OAIS foi abordado para destacar as suas responsabilidades obrigatórias, assim como, apresentar uma breve descrição dos fluxos de informação realizados pelas entidades funcionais. Posteriormente, ao abordar a cadeia de custódia documental, destacaram-se os principais requisitos e padrões arquivísticos a serem considerados na implementação de um sistema de gestão documental.

Após relacionar o RDC-Arq frente ao modelo OAIS e a cadeia de custódia documental, prosseguiu-se com a contextualização dos requisitos do ACTDR no âmbito da Arquivística. Assim, o manual fornece uma base para que arquivistas compreendam os critérios do ACTDR, no entanto, não substitui a leitura e compreensão do OAIS e do ACTDR. Desta forma, a após a contextualização de cada critério do ACTDR tem-se uma base auxiliar para que os arquivistas dialoguem com os demais profissionais envolvidos no planejamento e implementação de um RDC-Arq.

Dessa forma, estima-se incentivar o diálogo em torno dos RDC-Arq's, visto que a literatura sobre repositórios digitais, no sentido genérico do termo, está bem avançada; ao passo que a caracterização "repositório arquivístico" ainda carece de literatura própria. Por fim, este manual consiste em uma aproximação entre RDC-Arq, OAIS, ACTDR e cadeia de custódia documental; logo, objetiva incentivar a reflexão a auxiliar nos processos de planejamento e implementação de RDC-Arq's.

6. REFERÊNCIAS

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

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. Câmara técnica de normalização da descrição arquivística. **Norma brasileira de descrição arquivística (Nobrade)**. Rio de Janeiro: Arquivo Nacional, 2006.

BRASIL. CONSELHO NACIONAL DE ARQUIVOS. **Resolução nº 28, de 17 de fevereiro de 2009**. Disponível em: <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?from_info_index=21&infoid=273&sid=46>. Acesso em: 22 abr. 2018.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). **Reference Model for an Open Archival Information System (OAIS)**. Magenta Book. Washington, Jun. 2012. Disponível em: <http://public.ccsds.org/publications/archive/650x0m2.pdf>. Acesso em: 13 mai. 2014.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. Cadeia de custódia para documentos arquivísticos digitais. **Acervo**, Rio de Janeiro, v. 29, n. 2, p. 117-132, nov. 2016. Disponível em: <http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717>. Acesso em: 09 mai. 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721:2012**. Space data and information transfer systems: Open archival information system – Reference model.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 17799:2005**. Information technology: security techniques – Code of practice for information security management.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000:2018**. Information technology: security techniques – Information security management systems: overview and vocabulary.

SOBRE O AUTOR

Henrique Machado dos Santos, bacharel em Arquivologia e mestre em Patrimônio Cultural pela Universidade Federal de Santa Maria (UFSM). Atualmente é arquivista da Universidade Federal do Rio Grande (FURG), membro dos grupos de pesquisa: Gestão Eletrônica de Documentos Arquivísticos (GED/A) e Patrimônio Documental Arquivístico (PDA). Dedica-se à pesquisa de documentos digitais desde 2012, tendo publicado mais de 25 artigos em revistas científicas no Brasil e no exterior. Os principais temas abordados são: preservação de documentos arquivísticos digitais, diplomática contemporânea e gestão do conhecimento. Dentre seus principais trabalhos destacam-se:

- Repositórios digitais confiáveis para documentos arquivísticos: ponderações sobre a preservação em longo prazo[4];
- Políticas de preservação digital para documentos arquivísticos[5];
- Preservação de documentos arquivísticos digitais: reflexões sobre o uso de padrões abertos nos acervos[6];
- As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital[7];
- Novos rumos da preservação digital: das estratégias aos sistemas informatizados[8];
- Estratégias de preservação digital para documentos arquivísticos: uma breve reflexão[9];
- Cadeia de custódia para documentos arquivísticos digitais[10];
- Os impactos da obsolescência tecnológica frente à preservação de documentos digitais[11];

[4] www.portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2341

[5] www.portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2542

[6] dx.doi.org/10.22201/iibi.24488321xe.2018.74.57905

[7] www.biblios.pitt.edu/ojs/index.php/biblios/article/view/215

[8] dx.doi.org/10.5195/biblios.2018.326

[9] www.bad.pt/publicacoes/index.php/cadernos/article/view/1225

[10] www.revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717

- Um diálogo entre arquivo, conhecimento e tecnologia[12];
- Da preservação digital ao acesso à informação: uma breve revisão[13];
- Os fundamentos da diplomática contemporânea na preservação de documentos arquivísticos digitais[14];
- O documento arquivístico digital enquanto fonte de pesquisa[15];
- O documento digital no contexto das funções arquivísticas[16];
- Documentos digitais: o desafio da preservação[17].

Contato

E-mail: henrique.hms.br@gmail.com

Academia.com: furg.academia.edu/HenriqueMachadodosSantos

Google Scholar: scholar.google.com.br/citations?user=0VLAu8sAAAAJ&hl=pt-BR

Orcid: orcid.org/0000-0002-2497-7321

Lattes: lattes.cnpq.br/2224553749651399

ResearchGate: www.researchgate.net/profile/Henrique_Santos17

Redalyc: www.redalyc.org/autor.oa?id=539

Researcherid: www.researcherid.com/rid/B-2053-2016

Scopus: www.scopus.com/authid/detail.uri?authorId=56717359300

Blog: gestaodedocumentoseinformacoes.blogspot.com.br/

[11] www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5550

[12] www.biblios.pitt.edu/ojs/index.php/biblios/article/view/231

[13] www.ojs.letras.up.pt/index.php/paginasaeb/article/view/2836

[14] www.seer.furg.br/biblos/article/view/4825

[15] www.portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2688

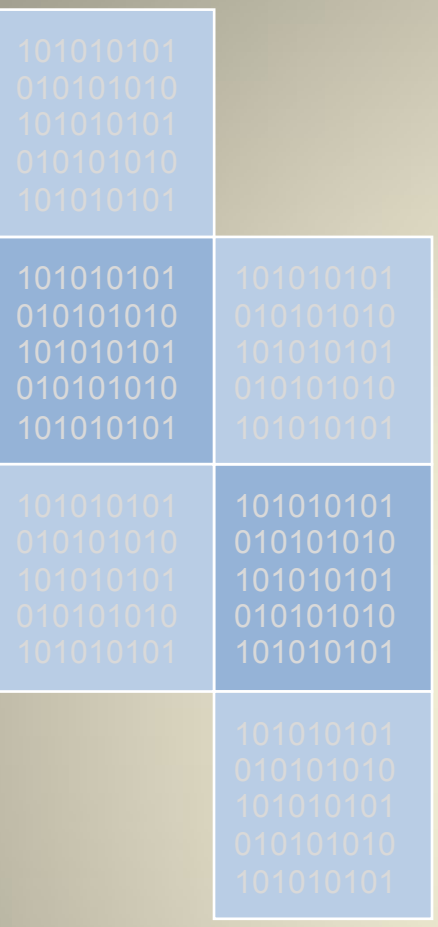
[16] www.ojs.letras.up.pt/index.php/paginasaeb/article/view/1477

[17] www.assinaturadigital.cienciahoje.org.br/revistas/reduzidas/330/?revista=330#20

Manual para Auditoria de Repositórios Arquivísticos Digitais Confiáveis

Henrique Machado dos Santos

Bacharel em Arquivologia e mestre em Patrimônio Cultural pela Universidade Federal de Santa Maria. Atualmente é arquivista da Universidade Federal do Rio Grande, membro dos grupos de pesquisa: Gestão Eletrônica de Documentos Arquivísticos e Patrimônio Documental Arquivístico. Dedica-se à pesquisa de documentos digitais desde 2012, tendo publicado mais de 25 artigos em revistas científicas no Brasil e no exterior. Os principais temas abordados são: preservação de documentos arquivísticos digitais, diplomática contemporânea e gestão do conhecimento.



O presente manual tem por objetivo fornecer subsídios teóricos para compreensão do modelo OAIS e do padrão ACTDR, com ênfase nos requisitos para auditoria de RDC-Arq's. Da mesma forma, busca-se esclarecer os requisitos arquivísticos que estão subentendidos no RDC-Arq, realçando sua pertinência durante o processo de auditoria.