Infraestrutura de segurança para gestão de riscos do Repositório Arquivístico Digital Confiável: um diálogo com a ISO 16363

Security Infrastructure for Risk Management of Trustworthy Digital Archival Repository: a dialogue with ISO 16363

Henrique Machado dos Santos

Universidade Federal do Rio Grande (FURG)
henrique.hms.br@gmail.com

Daniel Flores

Universidade Federal Fluminense (UFF)
dfloresbr@gmail.com

Resumo

Este estudo contextualiza os requisitos da infraestrutura de segurança para gestão de riscos, preconizados pela ISO 16363, no âmbito da Arquivística. São perpassadas questões como: monitoramento das plataformas de hardware/software e suportes; políticas de backup; alterações de segurança em pontos críticos do sistema; gerenciamento de riscos; e plano de recuperação para desastres. A discussão segue a lógica dedutiva, realizando uma triangulação na qual a infraestrutura de segurança da ISO 16363 é o prisma da discussão, e o Repositório Arquivístico Digital Confiável é a categoria norteadora. Dessa forma, obtém-se um artigo de revisão assistemática com temática aberta, pautada nos referenciais da preservação digital. Por fim, observa-se a necessidade estabelecer uma preservação digital sistêmica, orientada às normas e padrões amplamente aceitos pela comunidade de preservação digital.

Palavras-chave: Preservação digital; Arquivística; Repositório digital; Confiabilidade.

Abstract

This study contextualizes the requirements of security infrastructure for risk management, as recommended by ISO 16363, in the field of Archival science. Questions such as: monitoring of hardware/software platforms and supports; backup policies; security changes at critical points in the system; risk management; and recovery plan for disaster. The discussion follows deductive logic, performing a triangulation in which the security infrastructure of ISO 16363 is the prism of the discussion, and the Trusted Digital Archival Repository is the guiding category. Thus, we obtain an open-ended thematic review article, based on the references of digital preservation. Finally, there is a need to establish a systemic digital preservation, oriented to norms and standards widely accepted by the digital preservation community.

Keywords: *Digital preservation; Archival science; Digital repository; Reliability.*

1. Introdução

A evolução das Tecnologias da Informação e Comunicação (TIC) impulsionou a demanda social por documentos digitais em virtude das facilidades para criar, editar, excluir e disseminar conteúdos. Esse impacto é percebido em diversos setores, de modo a influenciar o mundo do trabalho, a pesquisa científica e os meios de comunicação.

Paralelamente a isso, surge o desafio de preservar a informação digital, visto que apresenta complexidades advindas do ambiente informático. Tal problemática tem incentivado a pesquisa no âmbito das instituições de memória (arquivos, bibliotecas, museus, centros de documentação, entre outras). Assim, ao passo que as TIC's evoluem tem-se buscado metodologias para minimizar os efeitos da obsolescência tecnológica.

Observa-se no âmbito da Arquivística/Arquivologia que a ausência de políticas de preservação aliada aos impactos da obsolescência tecnológica constitui uma ameaça para a manutenção dos princípios arquivísticos. Logo, os documentos arquivísticos em ambiente digital requerem a implementação de estratégias de preservação e sistemas informatizados para monitorar a sua autenticidade e garantir a capacidade de acessá-los no longo prazo.

Para tanto, é essencial usar de técnicas como as estratégias de migração, emulação, refrescamento e encapsulamento. Ademais, deve-se implementar um Repositório Arquivístico Digital Confiável (RDC-Arq) que será responsável pelo gerenciamento da preservação em longo prazo.

Destaca-se que o RDC-Arq deve estar em conformidade com o modelo Open Archival Information System (OAIS). O modelo OAIS é considerado o principal padrão pela comunidade de preservação e tornou-se a norma International Organization for Standardization (ISO) 14721:2012 que orienta os requisitos para um Repositório Digital Confiável (RDC). Logo, o RDC-Arq consiste em um RDC que contempla requisitos arquivísticos como, por exemplo, organicidade, proveniência, autenticidade e mantém a hierarquia dos planos de classificação/quadros de arranjo.

Além de manter a conformidade com o OAIS, cabe ao RDC-Arq realizar auditorias periódicas para demonstrá-la. Logo, surge a necessidade de auditar com o Audit And Certification of Trustworthy Digital Repositories (ACTDR) que se tornou a norma ISO 16363:2012. Essa norma possui três seções: políticas de preservação, gestão de objetos digitais e segurança da informação; de modo que analisa-se a seção de segurança da informação.

Sendo assim, este estudo tem por objetivo realizar uma análise da infraestrutura de segurança para gestão de riscos proposta pelo ACTDR. Contextualizam-se os requisitos do ACTDR no âmbito da Arquivística, considerando a implementação de um RDC-Arq em conformidade com o modelo funcional OAIS. Tal análise perpassa questões como: o monitoramento das plataformas de hardware/software e suportes; a política de backup; as alterações de segurança em pontos críticos do sistema; o gerenciamento de riscos; e o plano de recuperação para desastres.

2. Metodologia

Classifica-se este estudo como natureza aplicada, pois tem o objetivo de gerar conhecimentos para aplicação prática, conduzidos à solução de problemas específicos (Silva & Menezes, 2005). Logo, a pesquisa aplicada contribui para a ampliação do conhecimento científico, de modo a solucionar os problemas identificados e gerar novas questões que necessitam de investigação (Gil, 2010).

Parte-se do levantamento bibliográfico de materiais previamente publicados, contemplando a seleção de livros, publicações técnicas e artigos científicos. Tais artigos são recuperados por meio da Base de Dados em Ciência da Informação (BRAPCI) por meio de palavras-chave como: "preservação digital", “documentos arquivísticos digitais", "repositórios digitais confiáveis" e “segurança da informação”. Para tanto, define-se a delimitação temporal entre os anos de 2004 até 2019, e os artigos são escolhidos a partir da análise dos seus respectivos resumos.

Utiliza-se a seção de “infraestrutura de segurança para gestão de riscos” do ACTDR como prisma da discussão, logo, o RDC-Arq torna-se a categoria norteadora. A discussão dos resultados segue a lógica dedutiva, de modo que realiza uma triangulação entre o ACTDR, a infraestrutura segurança e a Arquivística (Gil, 2010; Luna, 1997; Silva & Menezes, 2005; Volpato, Barreto, Ueno, Volpato, Giaquinto & Freitas, 2013).

Dessa forma, obtém-se um artigo de revisão assistemática/narrativa que utiliza uma temática aberta, pautada nos referenciais da preservação digital. Tal abordagem permite compreender os requisitos da infraestrutura de segurança preconizados pelo ACTDR, e contextualizá-los na preservação de documentos arquivísticos digitais (Cordeiro, Oliveira, Rentería & Guimarães, 2007).

Não há pretensão de abordar exaustivamente a temática, logo, este estudo limita-se a compreensão dos pressupostos básicos da infraestrutura de segurança do ACTDR e a sua pertinência na implementação de um RDC-Arq. Assim, pretende-se proporcionar uma reflexão sobre o tema e ressaltar o ponto de vista dos autores frente à preservação de documentos arquivísticos digitais autênticos em longo prazo.

3. Gestão de riscos da infraestrutura técnica

As funções do RDC-Arq 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 a quantidade e a localização das cópias e sincronizá-las com os objetos digitais.

Ao utilizar mecanismos de análise de erro, o RDC-Arq irá detectar a corrupção ou perda de bits, 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. Além disso, é preciso registrar a gestão de mudanças, sendo necessário um processo para testar o efeito das mudanças críticas do sistema.

O êxito da preservação digital em RDC-Arq’s requer a definição de políticas e procedimentos para acompanhar a evolução das plataformas tecnológicas, dos formatos de arquivo, dos padrões de

metadados, dos suportes, das normas, da legislação vigente e das recomendações técnicas. Além disso, o RDC-Arq necessita de um plano de sucessão, a ser executado caso venha a encerrar suas atividades de preservação (Santos & Flores, 2019).

Dessa forma, o RDC-Arq possuirá tecnologias de hardware e software apropriadas aos serviços que presta à sua comunidade designada. Ademais, demonstrará maior nível de confiabilidade ao ter procedimentos para monitorar e avaliar a necessidade de mudanças nas tecnologias de hardware e/ou software utilizadas.

3.1. Atividades de preservação e infraestrutura do sistema

Um RDC-Arq deve identificar e gerir os riscos em suas operações de preservação e dos seus objetivos associados com a infraestrutura do sistema para garantir segurança e confiabilidade. Para tanto precisa dispor de inventários de infraestrutura do sistema, avaliações tecnológicas periódicas, estimativas de vida útil dos componentes do sistema, utilizar softwares amplamente suportados pela comunidade, e ser capaz de recriar arquivos de backups. O RDC-Arq deve gerir os riscos relacionados à infraestrutura de hardware, software e os procedimentos operacionais (CCSDS, 2011; ISO, 2012b).

Ademais, deve fornecer mecanismos para minimizar a dependência, mantendo-se capaz de evoluir por meio da substituição de tecnologias sem transtornos ao sistema como um todo. Nesse sentido, o RDC-Arq deve suportar novos formatos, e ser capaz de exportar sua participação para um novo custodiador no futuro; além de ter capacidade para recriar os materiais após um erro de substituição/exclusão de conteúdos (CCSDS, 2011; ISO, 2012b).

O RDC-Arq deverá preconizar uma infraestrutura confiável, para isso, precisa gerir os riscos relacionados às plataformas de hardware e software para minimizar a dependência do sistema. Sua infraestrutura tecnológica deve ser expansível e possibilitar a execução de um plano de sucessão futuro, caso seja necessário.

O plano de sucessão garante que os esforços em prol da preservação terão continuidade. Caso contrário, quaisquer interrupções dos serviços prestados pelo RDC-Arq serão suficientes para questionar a confiabilidade da custódia, e consequentemente, a autenticidade dos documentos arquivísticos (Santos & Flores, 2019).

Sendo assim, competem ao RDC-Arq ações como: monitorar hardware e software obsoletos, realizar backup, verificar corrupção de dados, realizar atualizações de segurança, atualizar hardware, software e suportes, além de identificar seus processos críticos.

3.1.1. Monitorar hardware e software obsoleto

Um RDC-Arq deve empregar sistemas de notificação para rastrear os componentes de hardware ou software que se tornam obsoletos, o que torna necessária a migração para novas infraestruturas. Tal compromisso pode ser demonstrado por meio da gestão periódica dos relatórios de avaliação da tecnologia, e consequente comparação da tecnologia existente a cada nova avaliação. Dessa forma, é possível identificar os riscos de obsolescência, e permitir a migração para novas tecnologias (CCSDS, 2011; ISO, 2012b).

Ressalta-se que documentos digitais são vulneráveis a vírus e falhas tecnológicas. Além disso, o ritmo acelerado do desenvolvimento das TIC's torna hardware e software rapidamente obsoletos, causando problemas de acesso, interpretação e perda de documentos (Interpares, 2007b).

Dessa forma, a preservação torna-se um desafio significativo à Arquivística, dada a complexidade dos documentos em ambiente digital aliada à especificidade de seu corpus teórico. Como pano de fundo da problemática, tem-se a crescente demanda da sociedade contemporânea por formatos digitais, logo, a perenidade da informação digital encontra-se em um platô.

A velocidade da produção de informações tem aumentado em ritmo constante. No entanto, sua acessibilidade diminuiu em virtude da dinâmica da indústria de computadores e dos acelerados ciclos de obsolescência tecnológica, gerando incompatibilidades em nível de hardware e software (Pinto, 2009). Nessa perspectiva, a sociedade depende cada vez mais da informação digital, e paradoxalmente, seu acesso e sua correta interpretação tem se configurado como um novo desafio à Arquivística contemporânea.

É preciso documentar a estrutura e as funções do sistema, de modo a identificar os componentes de hardware, software, periféricos e sistema operacional. Com isso, é possível identificar como os pacotes de software processam e representam a informação, como se comunicam entre si e com os usuários. Tais especificações asseguram a compreensão do contexto, pois, fornecem as informações necessárias para atualizar o sistema conforme a evolução das plataformas de hardware e software (Interpares, 2007b).

As ações necessárias à preservação e manutenção da autenticidade dos documentos arquivísticos necessita ser formalizada no âmbito organizacional. Logo, faz-se necessário desenvolver uma política de preservação digital que considere as vulnerabilidades dos documentos e proponha um conjunto de procedimentos para mitigá-las.

As políticas organizacionais, as estratégias de preservação e os sistemas informatizados são os meios para minimizar os impactos da obsolescência tecnológica. As políticas definem a priori o que será preservado, as estratégias consistem nas atividades de intervenção e os sistemas informatizados auxiliam a gerenciar todas as ações proferidas sobre a documentação, verificando inclusive, a conformidade com as políticas de preservação (Santos & Flores, 2015a).

As políticas de preservação digital buscam meios para minimizar os efeitos da obsolescência, e assim, contornar as vulnerabilidades dos documentos digitais. Para tanto, vislumbram a preservação em longo prazo, a manutenção da autenticidade e a garantia de acesso contínuo.

Os documentos digitais têm sua autenticidade ameaçada sempre que são transmitidos entre pessoas/sistemas, ou através do tempo, tendo em vista a necessidade de atualizar/substituir hardware e software necessários ao seu armazenamento, processamento e/ou comunicação. No entanto, atualizações tecnológicas regulares devem ser planejadas, pois minimizam os riscos de obsolescência, além de prevenir possíveis gastos inesperados (Interpares, 2007b).

A atualização tecnológica é necessária para que os documentos digitais continuem sendo acessados. Paradoxalmente a isso, configura-se como um intervalo de vulnerabilidade por expor os bits a possíveis manipulações que podem gerar tanto a perda da autenticidade, quanto a incompatibilidade. Logo, a

migração tecnológica torna-se um “mal necessário”, de modo que possibilita que os documentos criados em um contexto do passado possam ser corretamente interpretados por tecnologias do futuro, ainda desconhecidas. Alternativamente, pode-se minimizar a necessidade de migrações tecnológicas ao se optar pelo uso de padrões abertos nos acervos.

Ao optar por softwares oriundos de padrões abertos, o acervo minimiza o risco de perda da informação digital no momento da migração tecnológica (Innarelli, 2009). Igualmente, a plataforma de hardware ideal também deve ser livre de restrições de uso, de modo que o RDC-Arq não dependa exclusivamente de um desenvolvedor.

Dessa forma, o RDC-Arq deve ter plataformas de hardware e software adequadas à comunidade designada, e monitorá-las continuamente. Assim, é possível identificar potenciais vulnerabilidades nos componentes do sistema e substituí-los com auxílio de financiamentos previamente reservados para tal finalidade.

3.1.1.1. Plataforma de *hardware*

Dispor de tecnologias de hardware adequadas permite que o RDC-Arq preste serviços satisfatórios a sua comunidade designada. Isso facilita a admissão e a difusão por meio de interfaces apropriadas, bem como o gerenciamento dos objetos digitais, a soluções de preservação (como a migração) e a segurança do sistema. Evidencia-se o uso de hardware apropriado por meio de questões como: fornecimento de largura de banda suficiente para suportar a admissão e uso de demandas; análise sistemática do hardware e adequação do serviço conforme feedback recebido; e manutenção de inventário do hardware atual (CCSDS, 2011; ISO, 2012b).

A administração do RDC-Arq deve estar ciente de questões relacionadas ao armazenamento, gestão de dados, preservação e aos serviços que presta a sua comunidade designada; além de garantir que o hardware atual suporta a mídia em que os conteúdos são disponibilizados. Dessa forma, objetiva-se controlar as mudanças nas exigências dos serviços prestados, em especial, com relação às tecnologias de hardware e políticas de admissão ao se exigirem novas capacidades (CCSDS, 2011; ISO, 2012b).

O RDC-Arq deverá manter plataformas de hardware adequadas para os serviços que presta, e considerar o feedback recebido para realizar ajustes no sistema. Ademais, deve-se ressaltar que a adequação dos componentes de hardware irá impactar em todas as suas funções.

Ressalta-se a importância de observar o hardware como elemento essencial na preservação, caso contrário, todo o acervo digital será colocado em risco (Innarelli, 2009). É preciso considerar a viabilidade econômica, bem como, sua qualidade e durabilidade. Com isso, podem-se escolher as plataformas de hardware mais adequadas ao acervo.

Após a definição das tecnologias de hardware adequadas, o RDC-Arq deve dispor de procedimentos para monitorá-las, bem como receber notificações sobre mudanças necessárias. Isso garante que os níveis de serviço contratados são seguros e mantém conformidade com o esperado. Tais procedimentos podem ser evidenciados por meio de: auditorias sobre as taxas de erro observadas e a capacidade versus uso real; documentação das avaliações de monitoramento tecnológico; e atualizações tecnológicas dos fornecedores (CCSDS, 2011; ISO, 2012b).

Dessa forma, devem-se monitorar constantemente os componentes de hardware para verificar suas vulnerabilidades, assim como os níveis de interoperabilidade no RDC-Arq. Logo, o objetivo consiste em controlar as mudanças de hardware necessárias aos procedimentos de admissão, preservação e acesso (CCSDS, 2011; ISO, 2012b).

Compete ao RDC-Arq monitorar as mudanças nas plataformas de hardware para manter uma infraestrutura capaz de cumprir com suas funções relativas à admissão, armazenamento e acesso. O ponto fundamental consiste em manter a interoperabilidade entre a plataforma de hardware e as funções executadas pelo RDC-Arq para desenvolvê-las conforme o que foi definido previamente nas políticas de preservação.

Além de escolher o hardware apropriado e monitorá-lo, surge a necessidade do RDC-Arq dispor de procedimentos para avaliar quando será necessário atualizar tais componentes. Isso garante a capacidade de tomar decisões atempadas, quando houver informação indicando a necessidade de um novo hardware. Tal procedimento pode ser evidenciado por meio da avaliação de processos, e ao documentar a experiência da equipe em cada subsistema de tecnologia. Dessa forma, o RDC-Arq requer conhecimentos para avaliar a necessidade de substituir o hardware atual. Para tanto, necessita monitorar o desenvolvimento de sistemas que minimizem riscos/custos e melhorem o desempenho do sistema (CCSDS, 2011; ISO, 2012b).

O RDC-Arq deverá monitorar constantemente o hardware atual do sistema e assim, antecipar as atualizações, bem como verificar meios para reduzir custos e falhas. Este processo visa a melhoria contínua do RDC-Arq, respaldada nas reservas financeiras destinadas para tal. O processo de atualização do hardware é tão essencial quanto o do software, visto que as falhas podem impossibilitar o acesso aos documentos.

Destaca-se que a busca pela prestação de serviços à comunidade designada implica em monitorar, avaliar e atualizar a plataforma de hardware, a fim de evitar que se torne obsoleta. No entanto, para o êxito dessas etapas o RDC-Arq requer procedimentos, compromissos e financiamentos para substituir hardware quando houver necessidade. Isso garante a substituição de hardware em tempo hábil e evita a falha do sistema ou insuficiência de desempenho (CCSDS, 2011; ISO, 2012b).

Ressalta-se que o RDC-Arq deve ter mecanismos para avaliação de eficácia dos novos sistemas antes de sua implementação. Tal procedimento pode ser evidenciado por meio de ativos financeiros reservados para aquisição de hardware, e pela demonstração de economia de recursos com o custo amortizado pelo novo sistema. Dessa forma, o RDC-Arq demonstrará que tem capacidade e recursos financeiros suficientes para incorporar novas tecnologias; e que avalia as capacidades dos novos sistemas (CCSDS, 2011; ISO, 2012b).

Compete ao RDC-Arq substituir o hardware logo após identificar tal necessidade. Para tanto, deve dispor de recursos financeiros suficientes, como também, demonstrar que o novo hardware será capaz de economizar recursos no decorrer de seu uso. A atualização da plataforma de hardware consiste em uma necessidade motivada pelos impactos da obsolescência tecnológica, aliada à necessidade de preservar documentos autênticos e garantir o acesso à comunidade designada.

3.1.1.2. Plataforma de *software*

Dispor de tecnologias de software apropriadas contribui para que o RDC-Arq preste adequadamente os serviços oferecidos a sua comunidade designada. Isso proporciona níveis de serviços seguros, incluindo questões como: facilidade de admissão e difusão pelos depositantes e usuários; interfaces apropriadas e tecnologias como mecanismos de carregamento; gerenciamento de objetos digitais; estratégias de preservação; e segurança do sistema. Tal requisito pode ser evidenciado por meio de: sistemas de software adequados para apoiar a admissão e as demandas de uso; ao incentivar uma sistemática de feedback com relação ao software e à qualidade do serviço; e por meio da manutenção de um inventário dos softwares atuais (CCSDS, 2011; ISO, 2012b).

Dessa forma, tem-se por objetivo controlar a necessidade das mudanças nos componentes de software. Tal fato pode ocorrer devido: às necessidades da comunidade designada; as alterações nas políticas de admissão que requerem suporte para novos formatos de dados; e quando as alterações na tecnologia de software requerem novas capacidades para migração de formato. Isso pode ser conduzido por alterações nos requisitos de acesso, por mudanças nos mecanismos de entrega, e alterações no número e tamanho dos materiais arquivados que requerem software com maior escalabilidade (CCSDS, 2011; ISO, 2012b).

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 localizar e recuperar/interpretar a informação de conteúdo. Além disso, tais ferramentas tecnológicas devem ser adequadas às especificidades da Arquivística, de modo a comportar questões como: respeito aos princípios (proveniência, organicidade, unicidade, integridade e naturalidade), garantia de autenticidade, manutenção da forma fixa e do conteúdo estável.

Observa-se que o uso de softwares específicos poderá causar dependência tecnológica em relação ao suporte disponibilizado pelo fabricante. Logo, para eliminar tal dependência, deve-se garantir acesso aos documentos digitais por meio de outros softwares e por diferentes desenvolvedores. Com isso, o acesso aos documentos digitais não ficará restrito a um software específico (Innarelli, 2009).

Ao depender de softwares e formatos proprietários, incompatíveis com normas comuns, surgirá a necessidade de migrar os documentos frequentemente a fim de evitar que se tornem inacessíveis (Campos & Saramago, 2007). Portanto, deve-se considerar o uso de formatos abertos antes mesmo da produção dos documentos digitais, e com isso, escolher formatos abertos, amplamente utilizados, sem uso de técnicas de compressão e que sejam considerados padrões para preservação. Assim, tais atividades diminuem tanto os gastos com aquisição de licenças de softwares, quanto a necessidade de realizar estratégias para migração de formatos de dados (Santos & Flores, 2018).

> Preservar um acervo arquivístico demanda a implementação de mais de uma estratégia operacional. Nesta etapa, o uso de padrões abertos fará uma diferença significativa, seja na questão dos direitos autorais, ou mesmo na compreensão do funcionamento dos softwares e conhecimento da estrutura dos formatos de arquivo. A escolha de padrões abertos com licenças de uso claramente definidas simplificará o processo de preservação no que tange a utilização de plataformas de hardware e software, além de reduzir os custos com licenças (Santos & Flores, 2018, p. 44).

A adesão dos padrões abertos deve contemplar hardware, software e formatos de arquivo. Sendo assim, é preciso eliminar quaisquer dependências de desenvolvedores específicos. Quando se trabalha com padrões abertos, tem-se a liberdade de usar, aperfeiçoar e, se preciso recriar as aplicações. Logo, isso diminui questões burocráticas do RDC-Arq, bem como os seus custos relacionados a licenças e aquisições de direitos autorais.

Após definir as tecnologias de software adequadas, o RDC-Arq deverá manter procedimentos para monitorá-las e receber notificações sobre a necessidade de alterá-las. Isso garante que os serviços contratados são seguros e mantém conformidade com o esperado. Evidencia-se tal procedimento mediante: auditorias da capacidade versus o uso real; auditorias de taxas de erros observados; auditorias de desempenho relacionado aos limites da capacidade para atender aos requisitos de acesso da comunidade de usuários; e por meio de documentação das avaliações de monitoramento tecnológico, inclusive das atualizações de software dos fornecedores (CCSDS, 2011; ISO, 2012b).

Dessa forma, busca-se controlar as alterações exigidas nos serviços por parte da comunidade designada, em virtude de uma mudança correspondente na tecnologia de software, em especial, quando houver alterações nas políticas de admissão, bem como, a exigência de expandir as capacidades de preservação. Assim, o RDC-Arq deve monitorar a evolução do software e suas vulnerabilidades, bem como a interoperabilidade com o hardware (CCSDS, 2011; ISO, 2012b).

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. Ademais, precisa atender a mudanças solicitadas pela comunidade designada para otimizar o processo de busca, recuperação e interpretação das informações; bem como, buscar a interoperabilidade entre as plataformas de hardware e software.

Além de definir o software adequado e monitorá-lo continuamente, o RDC-Arq deve dispor de procedimentos para avaliar, antecipadamente, a necessidade de atualizá-lo. Isso pode ser evidenciado por meio de procedimentos que comprovem a experiência da equipe em cada tecnologia do subsistema. Portanto, o RDC-Arq coletará informações de monitoramento, de modo que deverá ter procedimentos estabelecidos e conhecimentos para avaliar esses dados e tomar decisões sobre a necessidade de um novo software. O monitoramento da tecnologia minimizará riscos e custos, além de melhorar o desempenho do sistema. A avaliação do software deve identificar quando o risco de usar a nova tecnologia supera o benefício esperado, e quando a nova tecnologia é suficientemente sedimentada para minimizar o risco (CCSDS, 2011; ISO, 2012b).

Dessa forma, cabe ao RDC-Arq monitorar a evolução das plataformas tecnológicas e antecipar a atualização de software quando necessário. Tal ação irá minimizar riscos de obsolescência tecnológica, evitar custos adicionais e melhorar o desempenho do sistema. Esse procedimento, previamente estabelecido, fundamenta-se em evitar que os softwares utilizados se tornem os documentos inacessíveis, comprometam sua autenticidade e demais atividades de preservação desenvolvidas.

Compete ao RDC-Arq manter o software adequado, e assim, monitorá-lo e avaliá-lo continuamente para evitar que se torne obsoleto. Logo, é fundamental que existam recursos suficientes para as eventuais atualizações. Para tanto, o RDC-Arq deve manter procedimentos, compromissos e financiamentos para substituir o software quando a avaliação indica tal necessidade. Isso garante que

a substituição do software seja realizada em tempo hábil para evitar falhas do sistema ou insuficiência de desempenho (CCSDS, 2011; ISO, 2012b).

Ressalta-se que o RDC-Arq deve ter mecanismos para avaliar a eficácia dos novos sistemas antes de serem implementados. Tal procedimento pode ser evidenciado por: uma declaração de compromisso em fornecer os níveis de serviço esperados no contrato; demonstração de ativos financeiros reservados para aquisição de software; e pela demonstração de economia de recursos através do custo amortizado pelo novo sistema. Dessa forma, demonstram-se as capacidades financeiras e operacionais para incorporar novas tecnologias ao sistema (CCSDS, 2011; ISO, 2012b).

O RDC-Arq deverá substituir o software potencialmente obsoleto para evitar falhas e consequentes perdas de dados. Com isso, surge a necessidade de demonstrar a capacidade e os recursos suficientes para incorporar novas tecnologias, de modo a garantir a preservação de documentos autênticos e aperfeiçoar os serviços prestados à comunidade designada.

3.1.2. Sistema de *backup*

O RDC-Arq deve realizar backup dos documentos e das informações custodiadas. Para tanto, necessita de plataformas de hardware adequadas, bem como, de suporte ao software, suficiente para cumprir as funções de preservação e acesso contínuo em longo prazo. Tal procedimento pode ser evidenciado por: documentação comprovando a realização do backup; inventário de backups; validação de backups concluídos; plano para recuperação de desastres; testes de backups; contratos de suporte de hardware e software para backup; preservação dos metadados do sistema; controles de acesso; localização de cópias; trilhas de auditoria; e verificação em checksum (CCSDS, 2011; ISO, 2012b).

Dessa forma, demonstra-se a adequação dos processos, do hardware e do software aos sistemas de backup, bem como, toda a gama das funções de admissão, preservação e disseminação, necessárias ao RDC-Arq. Logo, mecanismos simples de backup devem preservar o conteúdo dos documentos e os metadados gerados pelas funções de preservação. Portanto, compete ao RDC-Arq desenvolver planos de backup para garantir a continuidade de suas ações em todas as situações de falha do sistema (CCSDS, 2011; ISO, 2012b).

O backup consiste em uma cópia dos dados que é criada e mantida para, se necessário, recuperar dados excluídos ou corrompidos (Somasundaram & Shrivastava, 2011). As técnicas de backup por si só, não garantem a preservação em longo prazo, apenas asseguram a capacidade de se recuperar documentos, metadados e sistemas em caso de falhas eventuais. Sendo assim, deve ser compreendido como um procedimento de apoio, e não como a finalidade do processo de preservação digital.

A sequência de mudanças organizacionais pode afetar a longevidade dos documentos digitais. Há o aumento da possibilidade de perder documentos digitais dada a sua fragilidade frente aos documentos tradicionais. Tal risco é contornado ao duplicar os documentos de forma descontrolada, entretanto, este descontrole dificulta a identificação da última versão atualizada (Interpares, 2007a).

As organizações requerem uma cultura em prol dos arquivos para otimizar os fluxos de informação. Para isso, torna-se necessário inserir o arquivo como um subsistema do sistema maior, a organização. Deste modo, as decisões que influenciam a segurança e a gestão de documentos/informações devem

ser consideradas pelos administradores em seu plano estratégico e tático, não se limitando ao operacional.

Observa-se que o ambiente para replicação do backup requer o mesmo nível de segurança dos documentos originais. Pode-se considerar ainda, conforme a realidade organizacional, o armazenamento dos backups em câmaras/cofres de segurança anti-chamas e climatizados (Innarelli, 2009). Essa câmara de segurança consiste em um local considerado de segurança máxima, com estrutura independente do acervo que é construída com materiais à prova de fogo (Camargo & Bellotto, 2012).

Ademais, diversas metodologias de backup podem ser efetuadas, dentre elas: o backup completo, que contempla todos os documentos; o backup incremental, que se limita aos documentos que foram modificados; e a cópia do ciclo, que abrange um backup completo e sucessivos backups incrementais para um determinado período de tempo (por exemplo: uma semana), posteriormente, faz-se novo backup completo do período e prosseguem-se backups incrementais do novo ciclo (Casanovas, 2008).

Com as técnicas de backup é possível elevar o nível de segurança do RDC-Arq, tal precaução faz-se necessária dada a vulnerabilidade dos documentos digitais. O backup assegura a capacidade de retomar as atividades de preservação sem que ocorram perdas de informação significativas. Para tanto, deve-se implementar a rotina de backup mais adequada para cada contexto organizacional.

Definir uma política de backup é essencial para a preservação de documentos digitais, pois garante a restauração completa do acervo e dos sistemas informatizados. Sendo assim, o backup é uma técnica obrigatória nas áreas de informática, de modo que consiste em um dos pilares da segurança e da confiabilidade da informação (Innarelli, 2009).

Um RDC-Arq requer plataformas de hardware e software capazes de realizar o backup dos documentos digitais, dos metadados 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 (documentos digitais, suporte, plataforma de hardware ou software). As técnicas de backup elevam a segurança dos documentos custodiados, e são um pré-requisito para as ações de preservação digital.

3.1.3. Verificar corrupção de dados

A eficácia das ações de preservação digital requer mecanismos para detectar a corrupção ou perda dos bits. Isso assegura a integridade do Pacote de Informação para Arquivamento (Archival Information Package – AIP) e dos metadados, conforme as políticas definidas pelo RDC-Arq. Tal procedimento pode ser evidenciado por: documentação que especifica os mecanismos de detecção de erro nos bits e correções utilizadas; análises de riscos; relatórios de erros; e análise periódica da integridade dos conteúdos do RDC-Arq (CCSDS, 2011; ISO, 2012b).

Dessa forma, o objetivo consiste em tratar, em sua essência, as causas das perdas de dados. Logo, qualquer dado perdido deve ser recuperado pelo procedimento de backup. As falhas sistemáticas não devem ser acumuladas, isso garante um nível tolerável de perda de dados definido nas políticas (o qual pode ser restaurado com o backup). Para tal, podem-se usar mecanismos como assinaturas digitais e

checksums a fim de detectar as perdas de bits e auxiliar na validação da integridade (CCSDS, 2011; ISO, 2012b).

O RDC-Arq não deve tolerar perdas de dados em seus AIP's e informações relacionadas. Portanto, é fundamental dispor de mecanismos que identifiquem as possíveis perdas ou corrupção de dados e executem a restauração. A integridade dos dados é um preceito básico na preservação digital, de modo que assegura a longevidade dos bits. Com isso, pode-se avançar para o estágio seguinte, que é o tratamento dos bits vislumbrando a garantia de acesso inteligível à comunidade designada.

Ressalta-se que a informação desprovida de integridade é aquela que foi adulterada, que se encontra diferente da qual foi originalmente produzida, tramitada ou arquivada. Isso pode acontecer por razões intencionais ou acidentais, logo, é fundamental observar que independentemente da natureza, a quebra da integridade ocorre em virtude das falhas nos procedimentos de segurança da informação. Além disso, os membros da própria organização também podem adulterar as informações (De Sordi, 2008).

A integridade da informação dos AIP's deve ser controlada por meio de procedimentos de segurança de informação. Neste ponto, destaca-se a necessidade de monitoramento por meio de trilhas de auditoria que identifiquem as alterações e tenham capacidade para desfazê-las.

Além de detectar possíveis erros relacionados a corrupção ou perda de dados, compete ao RDC-Arq registrá-los e reportá-los à administração. E orientar quais medidas de reparo/substituição de dados corrompidos/perdidos, devem ser tomadas. Isso garante que a administração do RDC-Arq está informada sobre incidentes e ações de recuperação, fato que permite a identificação das fontes de corrupção ou perda de dados (CCSDS, 2011; ISO, 2012b).

Tal procedimento pode ser evidenciado por: procedimentos de notificação de incidentes aos administradores; registros de metadados de preservação; relatórios de erros; rastreamento das fontes de incidentes; e ações corretivas tomadas para eliminar as fontes de incidentes. Dessa forma, com mecanismos eficazes é possível detectar a corrupção dos bits. Além do registro e reparação dos danos à integridade, deve-se comunicar os incidentes à administração, para possibilitar revisões dos sistemas de software e hardware, ou políticas e procedimentos para minimizar tais vulnerabilidades (CCSDS, 2011; ISO, 2012b).

Observa-se que o RDC-Arq deve registrar todos os incidentes e reportá-los à administração para que possa tomar providências. Logo, os procedimentos de segurança da informação precisam ser definidos na política de preservação para que haja uma sistemática de identificação, registro, comunicação e solução dos problemas.

É elementar a adoção de ferramentas que protejam e garantam a manutenção dos documentos digitais. Com isso, será possível prever os danos e reduzir os riscos dos efeitos naturais (preservação prospectiva) ou reparar/restaurar os documentos danificados (preservação retrospectiva) (Márdero Arellano, 2004).

Logo, o RDC-Arq deve informar à administração sobre as perdas de dados e o respectivo processo de recuperação executado; além dos riscos potenciais. Com isso, será possível identificar as origens das falhas e reparar as vulnerabilidades em nível de hardware, software, suportes e procedimentos.

3.1.4. Atualizações de segurança

Além de manter plataformas de hardware e software adequadas, surge a necessidade do RDC-Arq registrar a disponibilidade de novas atualizações de segurança, com base na avaliação do risco/benefício. Isso protege a integridade dos objetos armazenados, e evita alterações ou exclusões não autorizadas. Tal requisito pode ser evidenciado por meio do registro de riscos, evidência de processos de atualização, e documentação relacionada à atualizações instaladas. As decisões para aplicar atualizações de segurança são resultado da avaliação do risco/benefício. Cada atualização de segurança, automática ou manual, considerada necessária, deve ser documentada após ser concluída. Ressalta-se que as atualizações de segurança não se limitam ao nível de software (CCSDS, 2011; ISO, 2012b).

As atualizações de segurança em um RDC-Arq devem comportar as plataformas de hardware e software, os suportes, os manuais de procedimentos e o treinamento/capacitação dos colaboradores. Ou seja, deve-se olhar para toda e qualquer vulnerabilidade em potencial, e mitigá-la, vislumbrando a manutenção de um ambiente favorável à preservação de longo prazo.

Destaca-se que os riscos e ameaças não se limitam por fronteiras geográficas, linguísticas, políticas ou outras. Conforme a informação digital se expande, especialmente via Internet, há um aumento progressivo das ameaças e dos ataques à segurança da informação digital. Consequentemente, isso promove o crescimento das estratégias de segurança da informação (Pereira, 2005).

Para impedir a dissolução dos princípios arquivísticos é preciso que a elaboração dos softwares conte com a participação de arquivistas. Assim, evita-se que se percam os vínculos da documentação com os princípios da proveniência e da organicidade. Durante o desenvolvimento dos softwares podem ser levantadas questões relativas à padronização internacional dos procedimentos arquivísticos. Assim, o uso de softwares adequados para os documentos de arquivo, facilita os processos de tomada de decisão, bem como, evita que a memória documental da sociedade seja perdida, corroborando assim, com a pesquisa histórica (Bellotto, 2006).

Cabe ao RDC-Arq evitar as alterações e exclusões de conteúdos não autorizadas. Além disso, deve realizar atualizações de segurança em sua infraestrutura tecnológica para minimizar os riscos. Para tanto, é preciso considerar a segurança em todo o ciclo de vida dos documentos, e manter assim, uma cadeia de custódia ininterrupta que garanta a manutenção da autenticidade desde a produção até a preservação e o acesso.

3.1.5. Atualização de hardware e mídias de armazenamento

É elementar que o RDC-Arq defina processos para atualizar as mídias de armazenamento e o hardware. Isso assegura que os dados não serão perdidos quando houver falha em ambos os meios de comunicação, ou quando o suporte ao hardware não puder mais ser usado para acessar os dados. Tal procedimento pode ser evidenciado por: documentação dos processos de migração; políticas relacionadas ao suporte (manutenção e substituição) de hardware; e documentação de ciclos de vida de suporte esperados do fabricante de hardware (CCSDS, 2011; ISO, 2012b).

Portanto, o RDC-Arq deve ter estimativas da velocidade de acesso e a quantidade de informações para cada tipo de mídia de armazenamento. Da mesma forma, deverá ter estimativas de vida útil confiável

das mídias de armazenamento, e estimar o tempo necessário para a migração ou refrescamento. Além disso, deve-se considerar a obsolescência em todos os componentes de hardware dentro do sistema como potenciais eventos para proceder à migração (CCSDS, 2011; ISO, 2012b).

A migração de suporte é uma alternativa para garantir que os documentos digitais não sejam perdidos fisicamente, o que acarreta em sua perda definitiva. Logo, pode se optar por dois caminhos: migrar os documentos de uma mídia obsoleta para uma atual; ou migrar os documentos de uma mídia que apresenta sinais de deterioração para uma mídia da mesma natureza, porém nova.

Os suportes de informação necessitam de cuidados para prolongar a sua vida útil. Assim, surge a necessidade de manter temperatura e umidade constantes, pois as alterações podem afetar definitivamente sua estrutura (Jesus & Kafure, 2010). Além da questão da temperatura e da umidade há outras variáveis que têm influência direta sobre a durabilidade e a confiabilidade das mídias, dentre elas, o tempo de uso, a qualidade do material, os campos magnéticos, a manipulação e a poluição do local (Innarelli, 2012).

Tão logo, observa-se a importância de estabelecer uma tabela de confiabilidade para determinar o tempo de uso das mídias. Isso auxiliará no gerenciamento de riscos a fim de evitar a perda de documentos digitais, visto que essa tabela fornece informações sobre quando substituir uma mídia antes que sua confiabilidade seja comprometida. A confiabilidade dos suportes é primordial, pois, a perda de documentos digitais é invisível e de difícil identificação (Innarelli, 2009).

Portanto, compete ao RDC-Arq manter um processo de migração das mídias de armazenamento com base no monitoramento e avaliação das estimativas de vida útil e 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 para não depender de tecnologias específicas.

3.1.6. Processos críticos indispensáveis

Compete ao RDC-Arq identificar e documentar os processos críticos que afetam sua capacidade de cumprir as responsabilidades obrigatórias, além de examinar e testar quaisquer alterações aos processos. Tal procedimento pode ser evidenciado pela matriz de rastreabilidade entre os processos e os requisitos obrigatórios. Dentre estes processos críticos, incluem-se o gerenciamento de dados, o acesso, o armazenamento arquivístico, a admissão, e os demais processos de segurança. Já a rastreabilidade torna possível compreender os processos necessários para atender cada uma das responsabilidades obrigatórias preconizadas pelo OAIS (CCSDS, 2011; ISO, 2012b).

Conforme o modelo OAIS, um RDC tem responsabilidades obrigatórias, dentre elas: negociar e aceitar informações junto ao produtor; obter o controle das informações e possibilitar sua preservação em longo prazo; definir a comunidade designada bem como sua respectiva base de conhecimento; garantir que a comunidade designada seja capaz de compreender as informações preservadas sem a necessidade de recursos especiais ou auxílio dos produtores; seguir políticas e procedimentos para assegurar que as informações são preservadas de forma confiável; disponibilizar as informações à comunidade designada com garantia de autenticidade (ABNT/NBR, 2007; CCSDS, 2012; ISO, 2012a).

O RDC-Arq deve controlar todos os processos críticos que podem afetar suas responsabilidades obrigatórias, de modo que seja possível compreender as necessidades destes fluxos de informação. Assim, é possível manter uma revisão em busca da melhoria contínua destes procedimentos entendidos como essenciais.

Ressalta-se a pertinência de um estudo sobre a confiabilidade, entendida como fundamental para determinar o risco de falha, a vida útil, a durabilidade, o desempenho, a necessidade de manutenção e as condições ideais de operação. Tal afirmação se estende ao sistema de arquivos como um todo (Innarelli, 2009). As plataformas de hardware e software, os suportes de informação, os formatos de arquivo e os procedimentos adotados pelo RDC-Arq devem ser confiáveis. Para tanto, é preciso definir rotinas de avaliação do sistema de arquivos nas políticas de preservação.

Além de identificar os processos críticos, é essencial ao RDC-Arq ter um processo de gestão da mudança documentado, que identifique as alterações que afetam potencialmente a capacidade de cumprir suas responsabilidades obrigatórias. Com isso é possível especificar os processos atuais e os processos aplicados anteriormente ao acervo. Tal procedimento pode ser evidenciado pela documentação sobre a avaliação do risco associado ao processo de alteração, e sobre a análise do impacto esperado no processo de mudança (CCSDS, 2011; ISO, 2012b).

Dentre estes processos de mudança, incluem-se o gerenciamento de dados, o acesso, o armazenamento arquivístico, a admissão, e os demais processos de segurança. Logo, devem-se saber, essencialmente, quais e quando as mudanças foram realizadas. Já a rastreabilidade torna possível compreender como são efetuadas as alterações no sistema. Com esse registro é possível reverter alterações ou pelo menos documentá-las (CCSDS, 2011; ISO, 2012b).

O RDC-Arq deverá ter especificações sobre os processos aplicados ao acervo relacionados às mudanças em seus processos críticos. Dessa forma, é possível compreender como as mudanças foram efetuadas no sistema, e consequentemente, usá-las como meio de aprendizado. Caso seja necessário, será possível reverter ações que comprometam as atividades do RDC-Arq.

Em caráter complementar a gestão de processos críticos, o RDC-Arq deve manter um processo para testar e avaliar os efeitos de tais mudanças. Isso contribui para proteger a integridade dos processos críticos a fim atender aos requisitos obrigatórios do OAIS. Tal procedimento pode ser evidenciado por: documentação dos procedimentos de teste; documentação que comprove alterações realizadas com base nos testes anteriores; e análise do impacto de uma mudança de processo (CCSDS, 2011; ISO, 2012b).

Dessa forma, as alterações críticas nos sistemas devem ser testadas previamente e separadamente. Após as alterações, os sistemas devem ser monitorados para identificar possível comportamento inesperado e inaceitável. Caso tal comportamento seja descoberto, as mudanças devem ser revertidas. Tal procedimento consiste em executar testes de todo o sistema ou em unidades (CCSDS, 2011; ISO, 2012b).

Cabe ao RDC-Arq avaliar as mudanças em seus processos críticos relacionados às funções primordiais que executa, em especial, as responsabilidades obrigatórias a cumprir. Assim, as alterações em pontos críticos (admissão, armazenamento, gestão de dados, acesso e segurança) devem ser testadas antes de sua implementação, após implementar, devem ser monitoradas e caso seja necessário, revertidas.

3.2. Gerenciamento de cópias dos objetos digitais

Cabe ao RDC-Arq gerir o número e a localização das cópias de todos os objetos digitais, para que possa fornecer cópias autênticas. Tal procedimento pode ser evidenciado por: testes de recuperação aleatória; validação da existência de objeto para cada local registado; validação de um local registrado para cada objeto no sistema de armazenamento; e verificação da informação de proveniência e fixidez. Dessa forma, o RDC-Arq pode ter políticas de preservação específicas para diferentes classes de objetos, motivadas pelo seu produtor, tipo de informação custodiada, ou valor (CCSDS, 2011; ISO, 2012b).

Igualmente, pode manter quantidades diferentes de cópias para cada classe, assim como requisitos de identificação adicionais, caso seja necessário usar as cópias alternativas para substituição. Ademais, deverá indicar a localização dos objetos com precisão, seja no nível físico, na mídia de armazenamento, no sistema ou em um subsistema. As informações de proveniência devem estar atualizadas a fim de controlar a cadeia de custódia e garantir que o RDC-Arq fornece cópias autênticas de seus objetos (CCSDS, 2011; ISO, 2012b).

Portanto, o RDC-Arq deve gerir seus backups, de modo que consiga localizar as cópias de segurança de todos os objetos digitais custodiados. É essencial que essa localização seja descrita com elevado grau de precisão, considerando a localização física e o armazenamento lógico, seja na mídia, nos sistemas ou nos subsistemas.

3.2.1. Sincronização de cópias

Ao implementar uma rotina de backup, o RDC-Arq precisa de mecanismos para garantir que todas as cópias dos objetos digitais estão sincronizadas. Isso assegura que as cópias múltiplas de um objeto digital permanecem idênticas, em tempo aceitável conforme estabelecido pelo RDC-Arq; e que uma cópia pode ser utilizada para substituir a versão do objeto corrompido (CCSDS, 2011; ISO, 2012b).

Tal procedimento pode ser evidenciado por: fluxos de trabalho de sincronização; análise do tempo que o sistema requer para sincronizar as cópias; e procedimentos documentados sobre os processos de sincronização. O plano para recuperação de desastres deve abordar o que fazer se um desastre e uma atualização coincidirem. Os mecanismos para sincronizar as cópias devem ser capazes de detectar a corrupção dos bits, bem como, verificar a fixidez antes de realizar a sincronização (CCSDS, 2011; ISO, 2012b).

Dessa forma, o RDC-Arq poderá recuperar-se de eventuais desastres, sendo capaz de restaurar os sistemas e a documentação. Com uma sistemática de backup adequada é possível manter cópias autênticas, as quais podem substituir os originais em caso de perda ou corrupção de dados.

Compete a política de contingência abordar os riscos iminentes à documentação digital, e assim, definir a periodicidade para realizar as réplicas, o nível de segurança e a método de recuperação caso ocorra algum problema inesperado (Innarelli, 2009). Ressalta-se a importância de que o backup contemple o sistema abrangente: o sistema operacional, os aplicativos e os documentos digitais. Logo, o sistema abrangente deve ser tão seguro quanto a última versão do backup, de modo que possa ser

recuperado de forma ágil. As cópias de segurança antigas devem ser adequadamente eliminadas, conforme definido das políticas de preservação (Interpares, 2007b).

Sendo assim, o RDC-Arq deve possuir cópias sincronizadas de todos os objetos digitais caso seja necessário executar o plano para recuperação de desastres. Isso garante a proteção do acervo contra sinistros e corrupções de dados, da mesma forma, é preciso identificar e reparar os dados corrompidos para que estes não sejam indevidamente sincronizados na forma de cópias de backup, ocasionando um grave erro no sistema.

Ademais, é preciso definir uma política de controle de backup, a fim de gerir a quantidade adequada de cópias de segurança, e assim, eliminar sistematicamente as versões antigas. Com isso, otimiza-se o armazenamento lógico, minimizam-se os custos relacionados, bem como, reduz-se o "lixo digital".

4. Gestão do risco de segurança

A gestão do risco de segurança auxilia o RDC-Arq a manter uma análise sistemática em relação a dados, sistemas, pessoal, planta física e segurança. Dessa forma, é possível determinar funções, responsabilidades e autorizações relacionadas à implementação de mudanças no sistema, além de ter um plano para preparo e recuperação de desastres.

Há de se ressaltar que perdas significativas têm ocorrido devido aos desastres naturais em grande escala, ataques cibernéticos, incêndios, dentre outros. Logo, percebe-se a vulnerabilidade de arquivos, bibliotecas e demais custodiadores da informação. Para minimizar tais riscos, tem-se implementado estratégias colaborativas para desenvolver novos modelos orientados a preservação digital, e assim, salvaguardar a informação em longo prazo (Souza, Oliveira, D'avila & Chaves, 2012).

4.1. Fatores de risco da segurança

Cabe ao RDC-Arq manter evidências da análise sistemática dos seus fatores de risco da segurança associada a dados, sistemas, pessoal e instalações físicas. Isso garante um serviço ininterrupto à comunidade designada, de modo que torna possível avaliar os riscos regularmente e manter a segurança adequada, conforme os níveis de serviços contratados (CCSDS, 2011; ISO, 2012b).

Neste sentido, é preciso definir sistemas de proteção contra incêndios, detecção de inundações, meios para avaliar a equipe, os procedimentos de gestão, os recursos, bem como a prestação de serviços. O treinamento interno e a avaliação externa devem ser realizados para mensurar a qualidade dos serviços e sua pertinência em relação a comunidade atendida. Já a realização periódica de auditorias financeiras, devem averiguar questões éticas, as práticas jurídicas e a manutenção de recursos operacionais necessários, incluindo a perda de receita. Outra questão pertinente é o direito de propriedade intelectual, o qual deve ser revisado constantemente (CCSDS, 2011; ISO, 2012b).

O RDC-Arq pode utilizar normas como a ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Com isso, é possível elevar os níveis de segurança da informação da organização como um todo.

Esta norma consiste em um padrão aplicável a todos os tipos e tamanhos de organizações, de modo que fornece um modelo para configuração e operação de um sistema de gerenciamento. Tal modelo incorpora características que os especialistas definiram em consenso, como, o estado da arte internacional. Dessa forma, as organizações podem desenvolver e implementar uma estrutura para gerenciar a segurança de seus ativos informacionais, incluindo informações financeiras, propriedade intelectual, detalhes dos funcionários, e ainda, informações confiadas a eles por clientes ou terceiros (ISO/IEC, 2018).

Além disso, é pertinente ter consciência das principais ameaças que circundam o ambiente de preservação. Logo, a avaliação de riscos pode ser realizada com o auxílio de ferramentas como o Digital Repository Audit Method Based On Risk Assessment (DRAMBORA), que permite a organização realizar um autodiagnostico das ações proferidas em torno do RDC-Arq.

O padrão DRAMBORA consiste em uma ferramenta de auditoria interna para repositórios digitais. Logo, fornece aos administradores de repositórios um meio de avaliar a capacidade, identificar vulnerabilidades, e reconhecer os pontos fortes. Posteriormente, é possível mensurar os riscos para definir e implementar medidas para mitigá-los. Além de riscos tecnológicos há também riscos no ambiente organizacional, por vezes ligados às pessoas e com fatores externos. Dessa forma, tanto o repositório, quanto a organização como um todo, podem se beneficiar das técnicas de análise e gestão de riscos para apoiar a administração geral e as ações de preservação digital (DCC/DCP, 2007).

Compete ao RDC-Arq manter uma análise contínua dos riscos relacionados tanto ao ambiente de preservação, quanto ao ambiente organizacional como um todo. Da mesma forma, a análise de riscos deve compreender a segurança física e lógica dos dados, bem como, a sua relação com os sistemas, as pessoas e as instalações. Normas como a ISO/IEC 27000:2018 podem elevar a segurança do ambiente organizacional, e padrões pertinentes à preservação, como o DRAMBORA, permitem identificar e mensurar o nível dos riscos que cercam a organização, e consequentemente, o RDC-Arq.

4.2. Controles para tratar riscos de segurança

Compete ao RDC-Arq implementar controles para tratar adequadamente cada um dos riscos de segurança identificados para satisfazer as necessidades de segurança. Tal procedimento pode ser evidenciado por: um sistema de listas de controle; análises de riscos; e por controles de detecção e avaliação permanente dos riscos (CCSDS, 2011; ISO, 2012b).

Para tanto, pode-se utilizar a já citada ISO/IEC 27000:2018, bem como a ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management. Isso contribui para o gerenciamento das ações de segurança da informação, o que corrobora para elevar os níveis de confiabilidade do RDC-Arq.

Observa-se que a ISO/IEC 17799:2005 estabelece as diretrizes e os princípios gerais para orientar a implementação, manutenção e melhora dos controles para gerenciamento de segurança da informação da organização. Seus objetivos e controles devem ser implementados para atender aos requisitos identificados por uma avaliação de risco. Assim, destina-se a ser uma base comum de orientações práticas para o desenvolvimento de padrões de segurança organizacionais, bem como,

práticas efetivas ao gerenciamento de segurança para ajudar a criar confiança nas atividades interorganizacionais (ISO/IEC, 2005).

Com isso, é possível demonstrar que tem-se melhorado os requisitos de segurança. Logo, o RDC-Arq também poderá armazenar informações sobre ataques à sua segurança, descrevendo os procedimentos tomados para possíveis ações futuras, e para evitar ocorrências semelhantes. Outra questão pertinente é a realização periódica de testes, atualizações e revisões dos planos de emergência (CCSDS, 2011; ISO, 2012b).

Dessa forma, o RDC-Arq poderá tratar cada um dos riscos identificados, logo, a combinação entre as normas ISO/IEC 27000:2018 e a ISO/IEC 17799:2005 corrobora para reforçar a segurança da informação, inclusive em âmbito organizacional. Ademais, pode-se manter um registro dos problemas relacionados a ataques para prevenir sua recorrência e revisar constantemente os planos de emergência.

4.3. Atribuições para alterar o sistema

É preciso que o RDC-Arq defina papéis, responsabilidades e autorizações relacionadas com a implementação de mudanças no sistema. Isso assegura que os indivíduos têm a autoridade e recursos adequados para implementar alterações, além de especificar quais indivíduos serão responsáveis pela implementação de determinada mudança. Tal procedimento pode ser evidenciado por: uso da norma ISO/IEC 27000:2018; organogramas; documentação relativa a autorizações do sistema; e certificação pela norma ISO/IEC 17799:2005. Dessa forma, as autorizações justificadas devem definir as permissões dos indivíduos, dentre elas, adicionar usuários, alterar metadados e/ou acessar trilhas de auditoria (CCSDS, 2011; ISO, 2012b).

Há de se destacar que somente os indivíduos autorizados devem ter acesso as configurações globais dos sistemas. Portanto, surge a necessidade de se definir grupos de usuários com diferentes permissões de acesso para modificar as propriedades do RDC-Arq e demais sistemas organizacionais.

A segurança da informação de um RDC-Arq pode ser observada com relação a autenticidade e ao armazenamento confiável. A autenticidade é a garantia de que a informação está intacta e que não dúvidas quanto a sua manipulação indevida. Neste sentido, o uso de contas de usuário, a definição das propriedades de acesso, a implementação de trilhas de auditoria constituem um mecanismo que registra e identifica as alterações proferidas. Além disso, é essencial que o RDC-Arq seja capaz de restaurar versões anteriores caso ocorram alterações não autorizadas (Santos & Flores, 2015b).

Com relação a confiabilidade do armazenamento, reitera-se a necessidade de backup do sistema abrangente, garantindo inclusive, a recuperação de todas as informações relacionadas aos documentos digitais custodiados. Assim, os documentos devem ser restaurados de modo a manter sua relação orgânica e seus metadados, sem que ocorram manipulações nos dados (Santos & Flores, 2015b).

Sendo assim, 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, para tal atribuição e posterior certificação. Observa-se uma convergência entre

autenticidade e segurança, na qual mantém um backup para eventual restauração, caso o original sofra manipulações não autorizadas. Portanto, tanto o RDC-Arq quanto os demais sistemas de informação organizacionais devem manter elevados níveis de segurança, especialmente em relação aos direitos de acesso e configurações globais.

4.4. Fatores de risco da segurança

Compete ao RDC-Arq preparar-se adequadamente para desastres e manter um plano de recuperação documentado, que inclua, pelo menos, um backup off-site, ou seja, realizado em local geograficamente separado do acervo para manter uma cópia de todas as informações preservadas, juntamente com o plano de recuperação. Isso garante que as capacidades de backup e restauração são suficientes para preservação contínua, bem como para acesso aos sistemas e aos documentos, com interrupção limitada dos serviços (CCSDS, 2011; ISO, 2012b).

Tal requisito pode ser evidenciado por: conformidade com a norma ISO/IEC 27000:2018; planos de recuperação de desastres; comprovante de existência de uma cópia de backup off-site de todas as informações; plano de continuidade dos serviços; documentação definindo as atividades; avaliações geológicas, geográficas ou meteorológicas sobre o local; e certificação da norma ISO/IEC 17799:2005. O nível de detalhamento do plano de desastre e os riscos específicos contemplados precisam ser adequados aos riscos que se sujeita (CCSDS, 2011; ISO, 2012b).

A segurança da informação digital não se limita ao controle por meio de sistemas informatizados, senhas e perfis de usuários com níveis de acesso/restrição. Igualmente, o plano de recuperação para desastres deve considerar as diversas variáveis as quais o RDC-Arq está sujeito. Tal visão comporta desde ataques cibernéticos, perpassando furtos, falhas nas plataformas de hardware/software, incêndios, inundações, entre outros possíveis.

A segurança dos sistemas deve considerar os aspectos físicos e lógicos, logo, torna-se pertinente manter testes regulares realizados por auditores externos à organização. Assim é possível verificar os níveis de segurança no que tange a testes de invasão, restauração de backups, verificar o estado de conservação das estruturas, simular acidentes, testar antivírus e firewalls (Pereira, 2005).

Destaca-se a pertinência de um RDC-Arq manter-se off-site, visto que tal técnica minimiza as invasões ao acervo custodiado. Sendo assim, disponibilizam-se as cópias dos AIP's via plataforma de acesso por meio do Pacote de Informação para Disseminação (Dissemination Information Package – DIP), o qual é estruturado em formatos de fácil acesso à comunidade designada. Tal estratégia protege os AIP's originais, eleva os níveis de confiabilidade do RDC-Arq na busca pela preservação de documentos autênticos em longo prazo. Da mesma forma, pode-se definir uma rotina de backup off-site, para assegurar sua confiabilidade.

Para caso de desastre ou falhas na segurança da informação do RDC-Arq, é ideal que os sistemas informatizados, os documentos e seus respectivos metadados sejam restaurados por meio do backup. Caso contrário a presunção de autenticidade dos documentos arquivísticos digitais será contestada (Santos & Flores, 2015b).

Sendo assim, o RDC-Arq deve manter o backup e uma cópia do plano de recuperação em um local seguro, separado do acervo, para garantir a continuidade dos serviços. As normas ISO/IEC 27000:2018 e ISO/IEC 17799:2005 podem contribuir para minimizar os riscos do ambiente de preservação, e inclusive, do ambiente organizacional como um todo. Ademais, o RDC-Arq deve definir claramente o seu plano de recuperação para desastres, considerando todos os riscos aos quais está sujeito. Assim, esse plano se tornará mais eficaz, caso seja necessário executá-lo.

5. Considerações finais

Este estudo realizou uma análise da infraestrutura de segurança para gestão de riscos proposta pelo ACTDR, perpassando assim, questões como: monitoramento das plataformas de hardware, software e suportes; sincronização de backup; controle de riscos; e plano de recuperação para desastres. Para tanto, buscou-se contextualizar tais requisitos no âmbito da Arquivística, tendo em vista a implementação de RDC-Arq's que seguem o modelo funcional OAIS.

A auditoria proposta para a infraestrutura de segurança e gestão de riscos contém os requisitos que vislumbram a segurança da informação tanto para o RDC-Arq, quanto para o âmbito organizacional. Essa proteção é definida para documentos digitais e sistemas informatizados, ou seja, avalia riscos da infraestrutura e da segurança da informação.

Ao monitorar a infraestrutura de hardware/software, bem como os suportes, o RDC-Arq irá minimizar as vulnerabilidades identificadas. Deste modo, a adoção da migração de suporte periódica, das plataformas livres e dos formatos abertos irá minimizar os riscos de obsolescência tecnológica, e consequente perda da informação. Destaca-se que os padrões abertos são o caminho para o RDC-Arq preservar documentos arquivísticos digitais em longo prazo sem depender de tecnologias ou fabricantes específicos. Da mesma forma, a constante migração de suporte será entendida como um pré-requisito para qualquer RDC-Arq.

Manter uma rotina de backup dos documentos digitais e dos sistemas informatizados possibilita a retomada ágil das ações de preservação digital do exato ponto no qual foram interrompidas. Tal procedimento agrega confiabilidade ao RDC-Arq, visto que tanto o sistema, quanto os AIP's serão restaurados em seu estado atual, juntamente com os metadados, que conferem autenticidade à documentação. Ressalta-se que o ambiente para armazenamento do backup deve possuir segurança igual ou superior ao da documentação original.

Ademais, a pertinência do backup também pode ser evidenciada nos casos de corrupção de dados. Logo, surge a necessidade de manter um sistema de verificação da integridade, bem como uma trilha de auditoria para identificar todas as alterações proferidas sobre os documentos e as configurações do RDC-Arq. Ao identificar a corrupção de dados, pode-se utilizar a versão atualizada do backup para restaurar o documento.

Com as atualizações de segurança é possível elevar os níveis de confiabilidade do RDC-Arq e minimizar as vulnerabilidades na infraestrutura, seja com relação às tecnologias utilizadas ou à capacitação das pessoas. Igualmente, deve-se atentar para os processos críticos, os quais têm impacto direto nas alterações relacionadas com: admissão, armazenamento arquivístico, gerenciamento de dados, acesso e demais processos de segurança da informação. Portanto, devem-se avaliar tais impactos a fim de

comprovar a eficácia das atualizações, de modo que o RDC-Arq possa cumprir com as responsabilidades obrigatórias preconizadas pelo modelo OAIS.

Além das plataformas e dos suportes de informação, deve-se atentar para a segurança das configurações globais dos sistemas. A autenticidade dos documentos digitais também dependerá das propriedades de acesso que cada grupo de usuários possuir, visto que deverá haver um responsável pela administração do RDC-Arq, com direitos de acesso superiores aos demais colaboradores da organização. Dessa forma, um sistema confiável deve limitar as alterações permitidas pelos indivíduos, para assegurar a autenticidade dos documentos custodiados.

Observa-se a necessidade do RDC-Arq ter um gerenciamento dos riscos aos quais está sujeito, para identificar e mensurar as suas vulnerabilidades, e posteriormente, implementar mecanismos de segurança para mitigá-las. Para tanto, pode-se utilizar o DRAMBORA, de modo a realizar auditorias interna a fim de comprovar os níveis de segurança. Paralelamente a isso, as normas ISO/IEC 17799:2005 e ISO/IEC 27000:2018 contribuem para melhoria da segurança da informação organizacional como um todo.

Cabe ao RDC-Arq ter um plano para recuperação de desastres, com cópia documentada em local separado da documentação original. Esse plano garante a continuidade dos serviços de preservação digital, visto que descreve como proceder a restauração dos backups de sistemas e de documentos digitais.

Por fim, ressalta-se que os constantes avanços do conhecimento em preservação digital despertam a atenção para o uso de normas e padrões. Logo, as ações para preservar documentos digitais autênticos em longo prazo devem ser respaldadas em uma abordagem sistêmica, que considera normas e padrões como, por exemplo: a ISO 14721:2012, a ISO 16363:2012, a ISO/IEC 17799:2005, a ISO/IEC 27000:2018 e o DRAMBORA. Sendo assim, o presente estudo contribui para expandir o conhecimento em relação a segurança da informação nos RDC-Arq’s em conformidade com o OAIS, bem como desperta a necessidade de se desenvolver uma “preservação digital sistêmica”. Ademais, os conhecimentos referentes aos “documentos arquivísticos digitais” podem ser generalizados para os demais tipos de informação digital, desde que sejam respeitadas as suas especificidades.

Referências Bibliográficas

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

BELLOTTO, H. L. (2006). Arquivos permanentes: tratamento documental. (4a ed.). Rio de Janeiro: FGV.

CAMARGO, A. M. A., & BELLOTTO, H. L. (2012). Dicionário de terminologia arquivística. (3a ed.). São Paulo: ARQ-SP.

CAMPOS, F. M. G., & SARAMAGO, M. L. (2007). Preservação digital de longo prazo em instituições patrimoniais: reutilização e adaptação de metadados. In: Actas dos Congressos Nacionais de Bibliotecários, Arquivistas e Documentalistas, 9(1), pp. 1-7, Lisboa. Disponível em: http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/540/330

CASANOVAS, I. (2008). Gestión de archivos electrónicos. Buenos Aires: Alfagrama.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). (2011). Audit and Certification of Trustworthy Digital Repositories. Magenta Book. Washington: CCSDS. Disponível em: http://public.ccsds.org/publications/archive/652x0m1.pdf

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM (CCSDS). (2012). Reference Model for an Open Archival Information System. Magenta Book. Washington: CCSDS. Disponível em: https://public.ccsds.org/pubs/650x0m2.pdf

CORDEIRO, A. M., OLIVEIRA, G. M., RENTERÍA, J. M., & GUIMARÃES, C. A. (2007). Revisão sistemática: uma revisão narrativa. Rev. Col. Bras. Cir., 34(6), pp. 428-431, Rio de Janeiro. Disponível em: http://dx.doi.org/10.1590/S0100-69912007000600012

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

DIGITAL CURATION CENTRE, & DIGITAL PRESERVATION EUROPE (DCC/DPE). (2007). Digital Repository Audit Method Based on Risk Assessment. Disponível em: http://wiki.statsbiblioteket.dk/drambora/DRAMBORAStart?action=AttachFile&do=get&target=DRAMBORA_guide.pdf

GIL, A. C. (2010). Como elaborar projetos de pesquisa. (5a ed.). São Paulo: Atlas.

INNARELLI, H. C. (2009). Preservação digital e seus dez mandamentos. In SANTOS, V. B. (ed.). Arquivística: temas contemporâneos, classificação, preservação digital, gestão do conhecimento. (3a ed.). Distrito Federal: SENAC, pp. 21-75.

INNARELLI, H. C. (2012). Instrumenta 2: Preservação de Documentos Digitais. São Paulo: ARQ-SP.

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

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). (2012a). ISO 14721:2012. Space data and information transfer systems: open archival information system – Reference model. Genebra: ISO.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). (2012b) ISO 16363:2012. Space data and information transfer systems: audit and certification of trustworthy digital. Genebra: ISO.

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

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS (INTERPARES). (2007a). A preservação de documentos arquivísticos digitais: diretrizes para organizações. Disponível em: http://www.interpares.org/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf

INTERNATIONAL RESEARCH ON PERMANENT AUTHENTIC RECORDS IN ELECTRONIC SYSTEMS. (INTERPARES). (2007b). A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. Disponível em: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_creator_guidelines_booklet--portuguese.pdf

JESUS, J. D. P., & KAFURE, I. (2010). Preservação da informação em objetos digitais. Biblionline, 6(2), pp. 29-43, João Pessoa. Disponível em: https://pdfs.semanticscholar.org/c13a/a28637d3cf233c3afd106b7d1f547715a423.pdf

LUNA, S. V. D. (1997). Planejamento de pesquisa: uma introdução. São Paulo: Educ.

MÁRDERO ARELLANO, M. A. (2004). Preservação de documentos digitais. Ciência da Informação, 33(2), pp. 15-27, Brasília. Disponível em: http://revista.ibict.br/ciinf/article/view/1043

PEREIRA, P. J. F. (2005). Segurança da Informação Digital. Cadernos BAD: Bibliotecários, Arquivistas e Documentalistas, (1), pp. 66-80, Lisboa. Disponível em: https://www.bad.pt/publicacoes/index.php/cadernos/article/view/822/821

PINTO, M. M. G. A. (2009). PRESERVMAP - Um roteiro da preservação na era digital. Porto: Edições Afrontamento.

SANTOS, H. M., & FLORES, D. (2015a). As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital. Biblios: Revista de Bibliotecología y Ciencias de la Información, 59(2), pp. 45-54, Brasília/Lima. Disponível em: https://doi.org/10.5195/biblios.2015.215

SANTOS, H. M., & FLORES, D. (2015b). Políticas de preservação digital para documentos arquivísticos. Perspectivas em Ciência da Informação, 20(4), pp. 197-217, Belo Horizonte. Disponível em: http://dx.doi.org/10.1590/1981-5344/2542

SANTOS, H. M., & FLORES, D. (2018). Preservação de documentos arquivísticos digitais: reflexões sobre o uso de padrões abertos nos acervos. Investigación Bibliotecológica: archivonomía, bibliotecología e información, 74(32), pp. 35-53, Cidade do México. Disponível em: http://dx.doi.org/10.22201/iibi.24488321xe.2018.74.57905

SANTOS, H. M., & FLORES, D. (2019). Responsabilidades de um Repositório Arquivístico Digital Confiável na perspectiva do Open Archival Information System. Páginas a&b: arquivos e bibliotecas, 11(3), pp. 116-132, Porto. Disponível em: https://doi.org/10.21747/21836671/pag11a9

SILVA, E. L., & MENEZES, E. M. (2005). Metodologia da pesquisa e elaboração de dissertação. (4a ed). Florianópolis: UFSC. Disponível em: https://projetos.inf.ufsc.br/arquivos/Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes_4ed.pdf

SOMASUNDARAM, G., & SHRIVASTAVA, A. (2011). Armazenamento e gerenciamento de informações: como armazenar, gerenciar e proteger informações digitais. Porto Alegre: Bookman.

SOUZA, A. H. L. R., OLIVEIRA, A. F., D'AVILA, R. T., & CHAVES, E. S. S. (2012). O modelo de referência OAIS e a preservação digital distribuída. Ciência da Informação, 41(1), pp. 65-73, Brasília. Disponível em: http://revista.ibict.br/ciinf/article/view/1352

VOLPATO, G. L., BARRETO, R. E., UENO, H. M., VOLPATO, E. D. S. N., GIAQUINTO, P. C., & FREITAS, E. G. D. (2013). Dicionário crítico para redação científica. Botucatu: Best Writing.