ARCHEION ONLINE
ISSN 2318-6186

O GERENCIAMENTO DE RISCO NO CICLO DA CURADORIA DIGITAL

Aureliana Lopes de Lacerda Tavares
Professora Ms. DCI/UFPE. Doutoranda em Ciência da Informação/UFPB
lianapb@gmail.com
http://lattes.cnpq.br/5237281447931783

Sandra de Albuquerque Siebra
Professora do DCI/UFPE). Doutora em Ciência da Computação (UFPE)
Coordenadora do PPGCI (UFPE).
E-mail: sandra.siebra@gmail.com
Lattes: http://lattes.cnpq.br/4923627544089379

Marcos Galindo de Lima
Professor do DCI/ UFPE. Doutor em História pela Leiden University.
galyndo@gmail.com
http://lattes.cnpq.br/7413464711814360

Resumo

No contexto das Humanidades Digitais, a curadoria de objetos digitais durante todo seu ciclo de vida é um compromisso exigido a todos os profissionais que lidam/trabalham com acervos de relevância documental, memorial, histórica social e/ou cultural. Pois, o acesso contínuo aos objetos digitais e sua gestão e preservação tornam-se cada vez mais urgentes. Nessa perspectiva, a Gestão de Risco surge como uma forma de proteger os acervos digitais de ameaças e vulnerabilidades, próprias dos sistemas de armazenamento e acesso a informação digital. Dessa forma, o presente artigo busca explorar a literatura publicada sobre Gestão de Risco, com foco na preservação digital, a fim de identificar os riscos mapeados e as medidas de controle indicadas, buscando refletir sobre esses processos no contexto do ciclo de vida da curadoria digital. A pesquisa é de natureza exploratória e foi delineada através de um levantamento bibliográfico realizado em bases de dados nacionais e internacionais através da ferramenta de busca *Google Schoolar*. Os resultados trazem reflexões acerca dos riscos, ameaças, falhas e vulnerabilidades que incidem sobre os estoques de informação digital e como estes vêm sendo tratados e/ou controlados por meio da aplicabilidade de ferramentas da Gestão de Risco em repositórios digitais. Urge nesse sentido, pensar a inclusão dessas ferramentas no ciclo da Curadoria Digital, como uma das etapas de gerenciamento do objeto digital. Assim, propõe-se que a Gestão De Risco possa ser incorporada ao ciclo de curadoria digital nas ações que permeiam todo o ciclo de vida do objeto digital, sendo considerada uma atividade contínua de gerenciamento.

Palavras chave: Curadoria Digital. Gestão de Risco. Preservação Digital. Objeto Digital.

1 INTRODUÇÃO

No contexto das Humanidades Digitais, as pressões trazidas pelas contínuas mudanças tecnológicas exigem dos profissionais compromissos com a curadoria dos objetos digitais durante todo seu ciclo de vida, desde sua criação, até sua utilização e reuso ou eliminação, de forma a garantir a preservação desses objetos a longo prazo. Assim, a Curadoria Digital emerge com um duplo significado, o primeiro como um processo de gestão de ativos informacionais e o outro como um novo campo de pesquisa e prática interdisciplinar que reflete uma abordagem holística para o gerenciamento do objeto digital e inclui atividades que abrangem todo o ciclo de vida desse objeto (TAVARES, 2014). Ela vem contribuindo para os processos de manutenção da informação digital, tendo como foco sua preservação. Nessa conformidade, a preservação digital é vista como uma etapa da curadoria, cujo objetivo é proteger os objetos digitais contra as ameaças que podem interferir em seu uso futuro, o que equivale a reduzir os riscos que circundam o objeto digital, que é o objetivo principal da Gestão de Risco.

Desse modo, entende-se a preservação digital como as ações envolvidas na manutenção do nível exigido de acesso e uso dos objetos digitais ao longo do tempo. Ou seja, como uma forma de lidar com os riscos inerentes ao ambiente digital. Esses riscos tornaram-se questão fulcral, e muitas pesquisas foram publicadas, ao longo dos anos, buscando formas e estratégias para identificar, analisar e avaliar os riscos com foco na mitigação dos fatores causais e/ou no acompanhamento permanente dos sistemas de armazenamento. Nesse escopo, é perceptível a mudança no campo de ação da preservação digital, desde que Paul Conway publicou o seu célebre artigo Preservação no universo digital em 1996, aquela época o foco da preservação digital recaia sobre técnicas e processos. Hoje é evidente, a migração do olhar do pesquisador que trabalha em um campo bem definido, inserido no domínio da Curadoria Digital.

Nesse cenário, o objetivo deste artigo é explorar a literatura publicada sobre Gestão de Risco, com foco na preservação digital, a fim de identificar os riscos

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

levantados e as medidas de controle indicadas, buscando refletir sobre esses processos no contexto do ciclo de vida da curadoria digital.

De acordo com Tavares (2014) a Gestão de Risco evolui das políticas prevencionistas que surgiram ao longo dos tempos a partir do desenvolvimento de métodos que buscavam a redução dos riscos industriais, por meio da análise criteriosa destes. A autora destaca que esta é a área da organização que visa proteger todos os recursos humanos, financeiros e materiais das consequências de possíveis eventos aleatórios que possam ameaçar o crescimento ou desempenho da mesma. Barateiro et al. (2010) destacam que esta área traz uma contribuição para o problema da preservação digital em contextos genéricos, sendo seu principal objetivo definir mecanismos de controle para proteger bens valiosos. Esta pesquisa é de natureza exploratória (GIL, 2007) que utiliza o levantamento bibliográfico em base de dados para explorar as publicações cientificas sobre as temáticas "curadoria digital" e "gestão de risco". O levantamento foi realizado na ferramenta de busca *Google Schoolar* (que indexa bases de dados nacionais e internacionais) com as palavras chave em português e inglês. O material recuperado foi selecionado, analisado, e discutido, buscando atender ao objetivo delineado para a pesquisa.

2 GESTÃO DE RISCOS

A ISO 31000 (2009:2018) define risco como sendo o efeito que as incertezas têm sobre os objetivos de uma organização. Dessa forma, tem-se que o risco é composto por causa e efeito, onde a causa é relacionada à incerteza da ocorrência do evento e o efeito é associado às consequências ou impactos. Assim, o risco pode ser considerado como a combinação da probabilidade e da consequência de não se atingir os objetivos propostos. Nesse sentido, o risco constitui a incerteza dos eventos que possam ocorrer no futuro, ou a materialização da incerteza nos objetivos de uma organização ou de um indivíduo (TAVARES, 2014).

Como depreende Aguiar (2006), o risco é uma medida da probabilidade e da perda, relacionadas à ocorrência de um evento negativo que afete o próprio projeto, seu

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

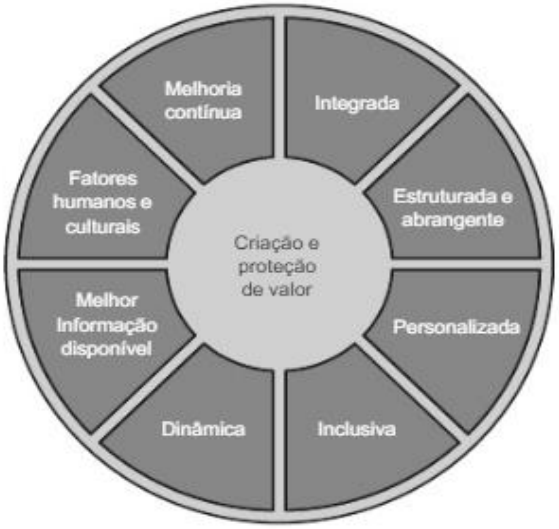
processo ou o seu produto. Em outras palavras, o risco é a possibilidade de um evento ocorrer e conduzir a organização a um resultado desfavorável. Para Ribeiro (2012, p. 107), o risco compreende a possibilidade de efeitos adversos, indesejáveis ou imprevistos, como perda e prejuízo causados por exposição a um perigo. Nesse sentido, o perigo constitui uma ou mais condições que pode causar ou contribuir para que o risco ocorra.

Relacionando as definições acima, pode-se apontar que os riscos são condições ou circunstâncias futuras que poderão proporcionar um impacto desfavorável a organização. O risco também é algo que está relacionado à escolha, não ao acaso (BERNSTEIN, 1997), pois decorre da incerteza inerente ao conjunto de possíveis consequências que resultam de decisões tomadas diariamente pelas organizações. Dessa forma, faz-se necessário a identificação do risco para possível gerenciamento.

Na ISO 31000 (2009), a Gestão de Risco (GR) é definida como as "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos". Essa norma também destaca a diferença entre a Gestão de Risco e o gerenciamento de risco. A primeira refere-se à arquitetura (princípios, estrutura e processo) para gerenciar riscos eficazmente. Enquanto que a segunda diz respeito à aplicação dessa arquitetura para riscos específicos. Essa norma foi atualizada e revisada em 2018. Esta nova versão destaca que o propósito da Gestão de Risco é a criação e proteção de valor, pois busca melhorar o desempenho e encorajar a inovação, apoiando o alcance dos objetivos nas organizações. Assim, destaca os princípios norteadores para gerenciar riscos, como pode ser visto na Figura 1, que devem ser considerados por uma organização. Esses princípios possibilitarão gerenciar os efeitos da incerteza nos seus objetivos.

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

Figura 1 - Princípios para gestão de risco



Fonte: ISO 31000 (2018)

Os princípios ilustrados na Figura 1 primam: por uma gestão **Integrada,** que deve fazer parte de todas as atividades organizacionais; por uma abordagem **estruturada** e **abrangente** na GR que contribui para resultados consistentes; que a estrutura e o processo de GR devem ser **personalizados** e proporcionais aos contextos internos e externos relacionados aos objetivos da organização. Também que a GR deve ser **inclusiva** e **dinâmica.** A primeira porque o envolvimento das partes interessadas possibilita que seus pontos de vista, conhecimentos e percepções sejam considerados e a segunda, pois os riscos podem emergir, mudar ou desaparecer e a GR pode antecipar, detectar, reconhecer e responder a essas mudanças repentinas.

Na GR convém que a **informação seja a melhor disponível**, para tanto precisa ser clara, oportuna e disponível para todos, pois essa gestão é baseada em informações históricas e atuais, bem como em expectativas futuras. Os fatores **humanos e culturais** devem ser considerados, pois o comportamento humano e a cultura influenciam significativamente nos aspectos da GR, em cada nível e estágio. E ainda a GR precisa de **melhoria contínua** e esta ocorrer por meio do aprendizado e experiências.

A estrutura da Gestão de Risco depende do apoio das partes interessadas, principalmente da alta direção. E sua eficácia vai depender da integração no processo de

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

governança e em todas as atividades da organização, incluindo a tomada de decisão, pois essa estrutura tem como propósito apoiar a organização na integração da GR nas atividades significativas e funções. Para tanto, deve englobar integração, concepção, implementação, avaliação e melhoria da gestão de risco através da organização, como ilustrado na Figura 2.

Figura 2 - Estrutura da Gestão de Risco

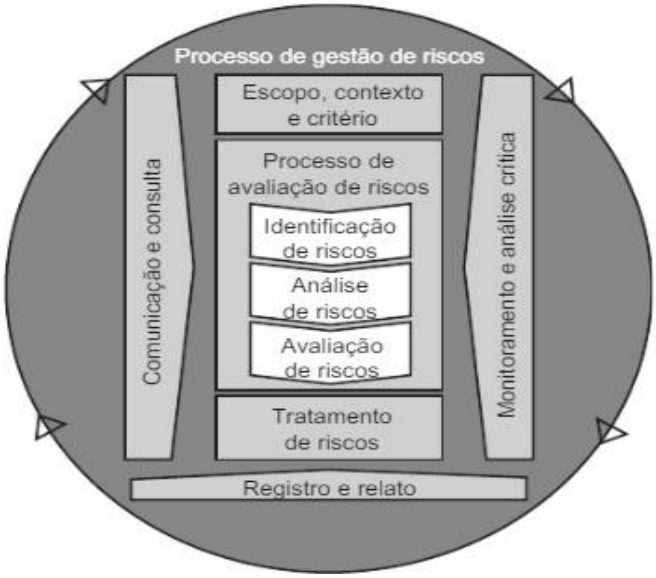
Fonte: ISO 31000 (2018)

Assim, recomenda-se que as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cuja finalidade seja integrar o processo para gerenciar risco na governança, estratégia e planejamento, gestão, processos de reportar dados e resultados, políticas, valores e cultura em toda a organização (ISO 31000, 2009).

Outro ponto da GR diz respeito ao processo, como pode ser visualizado na Figura 3, que envolve a aplicação sistemática de políticas, procedimentos e práticas que vão nortear as atividades de comunicação e consulta, o estabelecimento do contexto e, ainda, avaliação, tratamento, monitoramento, análise critica, registro e relato de riscos. Esse processo deve ser parte integrante da gestão e tomada de decisão, e, integrado à estrutura, operações, e processos da organização.

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

Figura 3 – Processo da Gestão de Risco



Fonte: ISO 31000 (2018)

Da Figura 3, conforme a ISO 31000 (2018), tem-se que o estabelecimento do **escopo, contexto** e **critérios** visa personalizar o processo de GR e envolve a definição do escopo do processo, a compreensão do contexto interno e externo e os critérios para avaliar a significância do risco.

O processo **de avaliação de risco** compreende **a identificação, a análise** e a **avaliação de riscos**, e convém que esse processo seja conduzido de forma sistemática, interativa e colaborativa. A **identificação do risco** é um processo de busca, reconhecimento e descrição dos riscos. É nesta fase que será gerada uma lista abrangente de riscos relacionados a possíveis eventos que possam criar, aumentar, reduzir, acelerar ou atrasar a realização dos objetivos. A **análise de risco** envolve a apreciação das causas e as fontes de risco, suas consequências positivas e negativas e a probabilidade de que essas consequências possam ocorrer. Ou seja, a análise visa entender a probabilidade de aquilo acontecer e o impacto que isso trará, se acontecer. A avaliação do risco envolve a comparação dos resultados da análise com os critérios estabelecidos para determinar a ação necessária. O **tratamento do risco** é a etapa de ação, é o processo que será usado para modificar o risco. Considera probabilidade,

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

consequência e estão ligados a estratégias como, por exemplo: mitigar, prevenir, eliminar, etc.

A **comunicação e consulta** é um processo contínuo onde se fornece, compartilha ou se obtém informações sobre todo o processo. O **monitoramento** é uma etapa de supervisão, observação critica , deve ser continuo e dinâmico. A **análise crítica** é uma atividade realizada para determinar adequação e eficácia do assunto em questão para atingir os objetivos, deve apontar melhorias. Convém que todo processo seja relatado e documentado por meio de mecanismos apropriados.

Nessa conformidade, percebe-se que a Gestão de Riscos está envolvida com a evolução da tecnologia e com o desenvolvimento de aparatos lógico de gestão de riscos associados a esta evolução, conferindo uma abordagem gerencial e sistêmica ao tratamento de problemas relativos a riscos Nesse contexto, a Gestão de Risco constitui-se em uma ferramenta eficaz para aprimorar a tomada de decisões dirigida às organizações como forma de mensurar a probabilidade de ocorrência de um evento não desejado e as consequências de seu impacto.

3 OS RISCOS NOS PROCESSOS DE PRESERVAÇÃO DIGITAL

A preservação digital é um desafio complexo que se configura como uma das grandes problemáticas dos conteúdos em ambiente digital. Assim, a aplicação do gerenciamento de risco na preservação dos acervos digitais permite um "um constante controle de riscos, além de antecipar e diagnosticar os diversos perigos que incidem nos serviços de informação" (RIBEIRO, 2012, p. 115), como também se mostra capaz de identificar os acidentes que podem ocorrer no processo de guarda e acesso da memória em meio digital.

Nesse contexto, estudos que discutem, levantam e refletem os riscos inseridos na conjuntura da preservação digital vem sendo publicados, buscando trazer à tona esses riscos, cenários ou possíveis falhas que podem incidir nos ambientes de preservação e, também, estudar novos instrumentos eficientes e capazes de reduzir as incertezas do contexto da preservação digital.

Com o propósito de desenvolver pesquisas buscando avaliar riscos associados com a migração de vários formatos de arquivos Lawrence et al. (2000) levantaram questões relacionadas a preservação digital baseadas nessa avaliação. Os pesquisadores partiram da premissa de que a estratégia de migração está propensa a gerar erros, e estes erros poderiam fornecer ferramentas práticas para quantificar os riscos Dessa forma, os autores identificaram três categorias de riscos relacionados à migração, quando considerada uma estratégia de preservação digital: Os riscos associados com a coleção geral (inclui a presença ou ausência de apoio institucional, financiamento, sistemas de *software* e *hardware* e os gerenciadores dos arquivos); riscos associados com o formato de arquivo de dados (inclui os elementos estruturais do arquivo que estão sujeitos a modificações); e riscos associados a um processo de conversão de formato de arquivo (a conversão pode ou não produzir o resultado esperado).

Pôde-se inferir com os resultados da pesquisa que a migração como estratégia de preservação digital pode ser caracterizada como um processo incerto, gerando outras incertezas. Uma forma de minimizar os riscos associados a tais incertezas é desenvolver um sistema de qualificação de risco, que desconstrói o processo de migração em etapas que podem ser descritas e quantificadas. Dessa forma, os autores indicam que os riscos associados à migração, ou à conversão de dados de um formato para outro pode ser mensurável, e a nível de risco vai variar conforme o contexto do projeto de migração (LAWRENCE, et al., 2000).

Rosenthal et al. (2005) destacam que um projetista de sistema de preservação digital precisa ter uma visão clara das ameaças das quais precisam proteger o conteúdo de seus sistemas. Para tanto, desenvolveram uma taxonomia de ameaças que devem ser observadas por esses profissionais ao desenvolverem sistemas de preservação digital. Na taxonomia se destacam: falha de mídia/hardware/software, erros de comunicação, falhas dos serviços de rede, obsolescência de mídia/hardware/software, erro do operador, desastre natural, ataque externo e interno e, ainda, falhas econômicas e organizacionais. Os autores destacam que os profissionais devem estar cientes de que muitas destas falhas estão relacionadas. Por exemplo, falhas de software provavelmente são desencadeadas por falhas de hardware, que apresentam ao software condições que

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

seus projetistas não previram e sob as quais nunca foram testadas. Desse modo, apresentam estratégias que os projetistas de sistemas podem empregar para sobreviver a essas ameaças, que serão descritas a seguir.

A **replicação** é uma estratégia básica que explora o atributo que distingue informação digital de analógica, e a possibilidade de copiá-la sem perda de informação, para armazenar múltiplas réplicas da informação a ser preservada. É um atributo necessário a um sistema de preservação digital, mas está longe de ser suficiente. A **migração** pode ser uma estratégia eficaz contra falhas de mídia, hardware e software e obsolescência. A **transparência** é uma estratégia eficaz contra todas as formas de obsolescência, pois o acesso à fonte incentiva uma ampla revisão do sistema, em busca de vulnerabilidades. O **código aberto** também pode ser eficaz contra falhas econômicas, impedindo que os problemas financeiros de uma organização consigam condenar a tecnologia do sistema. A **diversidade** é uma estratégia citada pelos autores contra falhas catastróficas. Idealmente, um sistema de preservação digital deve fornecer diversidade em todos os níveis. Porém, a maioria dos sistemas fornece isso em apenas alguns, por exemplo, diversidade de mídias de armazenamento, dispersão geográfica de réplicas (como por exemplo o padrão LOCKSS), diversidade em hardware e fornecedores e ainda de softwares entre as réplicas, etc. Outra estratégia necessária nesses sistemas, são as auditorias, que devem ser regulares, a fim de manter a probabilidade de falha em níveis aceitáveis. E, por fim, os autores citam **a economia** como uma técnica para reduzir os custos dos sistemas de preservação digital. Esses custos devem ser pensados para a ingestão de material, para a preservação e na disseminação.

Baker et al. (2006) listam algumas ameaças que podem prejudicar o armazenamento a longo prazo. Destacam que essas ameaças não são falhas ligadas apenas a hardware e software, mas também falhas devido a seres humanos e organizações. Assim citam: desastre em larga escala (como inundações, incêndios, terremotos, e atos de guerra que por ventura acionam outros tipos de ameaças); erro humano; falhas de componentes; falhas de mídias; obsolescência de mídia/hardware; obsolescência de software/formato; perda de contexto; ataques (que podem incluir

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

censura, modificação e roubo do conteúdo dos repositórios, e perturbação dos seus serviços); falhas organizacionais e falhas econômicas. Os autores destacam que, mesmo com o conhecimento dessas ameaças, os dados ainda estão sendo perdidos. Pois muitas dessas falhas ocorrem silenciosamente e não é possível identificá-las com facilidade. Os autores também destacam a correlação entre as falhas do sistema e destacam a replicação de dados, a replicação geográfica, a diversidade no controle administrativo, o espelhamento síncrono e a independência dos componentes como formas de reduzir essas falhas ou isolá-las.

Pinto (2009) aborda alguns dos riscos que circundam a informação digital quando reconhece os perigos de perda e vulnerabilidade desta perante a complexidade que a cerca. A autora destaca como obstáculos: a fragilidade física dos suportes, a obsolescência tecnológica, a pluridimensionalidade e a vulnerabilidade do ambiente digital. Destaca. ainda, o risco de perda da autenticidade, fidedignidade, integridade e usabilidade/inteligibilidade da informação produzida e armazenada nesses suportes (PINTO, 2009).

Barateiro et al. (2010) apresentam uma taxonomia baseada na terminologia do gerenciamento de risco, considerando as vulnerabilidades e ameaças para a preservação digital, ressaltando que "vulnerabilidades são pontos fracos (possíveis pontos de falha) no ambiente e ameaças são eventos que afetam o comportamento normal" (BARATEIRO et al., 2010, p. 8). Os autores sublinham que a arquitetura de um sistema de preservação digital agrega diferentes componentes, que são: as entidades de informação, incluindo objetos e metadados preservados; os processos que controlam as entidades de informação e a infra-estrutura tecnológica que suporta o ambiente de preservação. Cada um desses componentes pode apresentar vulnerabilidades, que os autores classificam em: vulnerabilidades nos processo que afetam a execução de processos que controlam as entidades de informação; as vulnerabilidades de dados, que afetam as entidades de informação; e as vulnerabilidades de infra-estrutura, incluindo os problemas técnicos nos componentes da infraestrutura. Esses autores classificam as ameaças à preservação digital em: desastres, ataques, gestão e legislação. Onde os desastres e ataques correspondem, respectivamente, a ações não deliberadas e deliberadas que afetam o

sistema ou seus componentes; as falhas de gestão são as consequências de decisões erradas que produzem várias ameaças ao ambiente de preservação; e as ameaças legislativas ocorrem quando os processos de preservação ou os dados preservados violam a legislação nova ou revisada (BARATEIRO et al., 2010,). Assim, apresentam a redundância, a migração, a emulação, o refrescamento, a diversidade, a inércia do sistema, a adoção de metadados e a auditoria como técnicas e estratégias relevantes para lidar com vulnerabilidades e ameaças, aumentando a probabilidade de corresponder aos requisitos de preservação digital. Dessa forma, criaram um quadro, apresentado no Quadro 1, indicando como essas técnicas podem ser usadas para tratar os riscos associados, ameaças e vulnerabilidades de preservação digital identificadas por eles.

Quadro 1 - Abordando ameaças e vulnerabilidades de preservação digital.

Ameaças e Vulnerabilidades			**Técnicas/estratégias**							
			Redundânci	**Migração**	**Emulação**	**Refrescamen**	**Diversidade**	**Inércia**	**Metadados**	**Auditoria**
Vulnerabilidades	Dados	Falhas de mídia	R	-	-	r	-	-	R	R
		Obsolescência da mídia	-	r	r	-	-	-	R	R
	Infraestrutura	Falhas de hardware	-	-	-	r	r	-	-	R
		Obsolescência de hardware	-	-	-	r	r	-	-	R
		Falhas de comunicação	-	-	-	r	r	-	-	R
		Falhas de serviço de rede	-	-	-	r	r	-	-	R
	Processo	Falhas de software	-	-	-	r	r	-	-	R
		Obsolescência de software	-	-	-	r	r	-	-	R
Ameaças	Desastres	Desastres naturais	R	-	-	-	r	-	-	-
		Erros operacionais humanos	R	-	-	-	r	r	R	R
	Ataques	Ataques internos	R	-	-	-	r	r	R	R
		Ataques externos	R	-	-	-	r	r	R	R
	Gestão	Falhas econômicas	-	-	-	-	r	-	-	R
		Falhas organizacionais	-	-	-	-	r	-	-	R
	Legislação	Mudanças legislativas	-	-	-	-	r	-	r	-

Legenda: r =: reduz o risco da ameaça/vulnerabilidade; R =: requerido para recuperação; -: não serve.

Fonte: BARATEIRO et al., 2010

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

Em pesquisa desenvolvida no Laboratório Liber do Departamento de Ciência da Informação da Universidade Federal de Pernambuco, Galindo e Lima (2011) identificaram as ameaças que podem incidir sobre os estoques de informação digital, especificadas a seguir. **Ameaças físicas** são os agentes externos que podem danificar os suportes e se subdividem em: físicas (temperatura e umidade relativa do ar), químicas (poeira) e físicas mecânicas (armazenamento, manuseio e desastres). A segunda categoria de ameaças são **as ameaças humanas** que podem ser percebidas devido à ausência de políticas de preservação e a falta de pessoal especializado em preservação digital. Por fim, as ameaças **tecnológicas** que são causadas por problemas no *hardware* e/ou *software*.

Ribeiro (2012), em sua pesquisa de mestrado, propôs o desenvolvimento de uma ferramenta lógica capaz de antecipar e diagnosticar os riscos que incidem nos estoques de informação, além dos acidentes significativos ocorridos durante o processo de guarda e acesso da memória em meio digital. Dessa forma, a autora aplicou a Análise Preliminar de Risco (APR) em Repositórios Institucionais do Brasil. E, por meio dessa análise, identificou os principais fatores geradores de riscos que, de acordo com a mesma, se concentraram nas instalações, nos processos, na equipe, nos materiais e nos suportes. Além da identificação desses fatores, a autora propôs também uma categorização de potenciais acidentes, como pode ser visualizado no Quadro 2, que podem ocorrer durante o processo de guarda e acesso à memória digital. A visualização destes, segundo a autora, podem "despertar" os gestores para a importância de incrementar a eficiência dos processos de vigilância e as estratégias de preservação dessa memória digital.

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

Quadro 2 - Cenário de acidentes para a preservação digital

CENÁRIO DE ACIDENTES DE RISCOS			
ACIDENTE	**PERIGO**	**CAUSA**	**EFEITO**
Nº 1	Obsolescência de hardware e software	Mercado altamente competitivo da tecnologia da informação	Leva a ciclos de renovação de tecnologia a cada 3 / 5 anos (HEDSTRON, 1998)
Nº 2	A falta de especialização e capacidade de domínios técnicos daqueles que lidam com nossa herança digital	Falta de investimento e recursos oferecidos pelas suas instituições	Insegurança desses profissionais em trabalhar com novas tecnologias, originando sentimentos como o medo
Nº 3	A falta de administração dos riscos que envolvem a preservação digital da produção intelectual de uma instituição a longo prazo	1) Falta de cooperação com outras iniciativas de preservação digital. 2) Falta de elaboração de manuais que ofereça orientações gerais quanto ao tratamento de objetos digitais e o gerenciamento dos riscos envolvidos na sua preservação	Vulnerabilidade dos seus processos de preservação digital e elaboração de projetos redundantes, além da minimização de esforços de preservação.
Nº 4	A ausência de clareza no papel de cada indivíduo envolvido no processo de gestão de instituições e serviços de informação	A falta de equipe específica para desempenhar as diferentes atividades realizadas nessas instituições serviços de informação	Incapacidade de identificar e apontar responsabilidades, entre elas a de manter o acesso a longo prazo das informações contidas nessas instituições
Nº5	Degradação de mídias digitais	Inadequado acondicionamento dos materiais digitais nas instalações dessas instituições	Ilegibilidade da informação registradas nessas mídias
Nº 6	Instabilidade de suporte por longo prazo	Falta de uso de padrões e formatos de arquivos de dados abertos, com amplo acesso e assistência técnica (THOMAZ E SOARES, 2004	Complexidade no momento de selecionar e aplicar estratégias de preservação, minimizando sua efetividade
Nº 7	Condições inadequadas do ambiente no qual estão depositados e do manuseio dos mesmos.	Condições ambientais, econômicas e políticas no território latino-americano, que se apresentem de formas mais adversas a prática de preservação digital. (GALINDO, 2005)	Levam ao desgaste e até mesmo a perda de leitura das informações registradas em objetos digitais. Sendo considerado um dos principais causadores da perda da informação contidas em hardwares e softwares.
Nº 8	A falta de clareza na definição de quais elementos dos objetos	Ausência de planejamento do que será selecionado para ser preservado, ou	Prejudica a consolidação de uma coleção digital e a compreensão da mesma,

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

	digitais e quais informações serão efetivamente preservadas	seja, de uma criteriosa política de seleção	por parte dos usuários.
Nº 9	A falta de autenticidade do objeto digital preservado	Falta de identificação da origem e do histórico do objeto digital durante processo de preservação	Dificulta a confirmação a integridade e a preservação do objeto na sua forma original
Nº 10	O dilema da escolha das estratégias e ações de preservação	Ausência de um uma solução prática aplicável universalmente ao problema da obsolescência tecnológica e da degradação dos objetos digitais	Adoção de estratégias pouco significativas, a qual compreende uma decisão não ponderada e sem base nos vários fatores que envolvem a preservação do objeto digital
Nº 11	A Escolha não ponderada de estratégias para a preservação dos materiais digitais	Falta de conhecimento técnico daqueles que lidamcom nossaherançadigital	Maximização de esforços desnecessários à preservação de objetos digitais
Nº 12	A falta de métodos organizados para a realização das atividades de preservação	Falta de políticas institucionais voltadas à guarda e preservação de objetos digitais	Ausência de organização e clareza dos objetivos, diretrizes, práticas e intenções organizacionais que servem para fortalecer as decisões locais, ou seja, o caminho para alcançar o consenso corporativo

Fonte: Ribeiro (2012)

Como foi possível observar com esse levantamento, as pesquisas sobre gerenciamento de risco vêm se ampliando dentro da área da preservação digital. Visto que identificar riscos, analisá-los e buscar mitigá-los é necessário em todos os níveis da organização. Sejam eles riscos estruturais, operacionais, processuais ou nos materiais e suportes, apenas a partir da identificação e análise sistemática, é possível estabelecer prioridades de ação e alocação de recursos para mitigá-los ou acompanhá-los.

3 GERENCIAMENTO DE RISCO E CURADORIA DIGITAL

A Curadoria Digital envolve os processos de manutenção, preservação e agregação de valor aos objetos digitais em todo o seu ciclo de vida. Ainda, conforme Abbott (2008) engloba atividades envolvidas na gestão de dados, desde o planejamento da sua criação, passando pelas boas práticas na digitalização, na seleção dos formatos,

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

na documentação e na garantia de estarem sempre disponíveis e adequados para serem descobertos e reusados, agora e no futuro. Para Hedges et al. (2007 apud SANTOS, 2016), a Curadoria Digital é um conjunto de ações que garantem a qualidade, integridade e auditoria de conjuntos complexos de informação, a partir de ações executadas durante o ciclo de vida dos objetos digitais.

Desse modo, a Curadoria Digital tem emergido na literatura como uma resposta aos desafios oriundos dos problemas que cercam a informação digital, como a obsolescência tecnológica própria do ambiente dinâmico e interativo das tecnologias de informação e comunicação. Para Tavares (2014), uma curadoria sendo bem aplicada pode reduzir a obsolescência digital e manter a informação acessível aos usuários por longo tempo, assegurando, assim, o objetivo da preservação digital.

Buscando auxiliar criadores e curadores de dados a organizarem e planejarem seus objetos digitais, a fim de ajudar as instituições/organizações a identificar riscos e formular estratégias para uma curadoria de sucesso, o *Digital Curation Centre (DCC)* desenvolveu um modelo que oferece uma visão geral dos estágios do ciclo de vida necessários ao processo de curadoria e preservação dos objetos digitais (DCC, 2018). Esse modelo permite que os curadores acompanhem o objeto digital, no recebimento, avaliação, seleção (ou descarte), e na implementação das ações de preservação, armazenamento, acesso, além de em possíveis transformações ou reavaliações desse objeto. O modelo possibilita, também, a identificação de fraquezas nas políticas e possíveis lacunas no encadeamento dos arquivos. Pode ser usado para planejar atividades dentro de uma organização, buscando garantir que todas as etapas necessárias sejam realizadas, cada uma na seqüência correta (DCC, 2018). De acordo com Higgins (2008), este modelo é indicativo e não exaustivo, sendo de natureza genérica, o que configura que nem toda instituição/organização deve cumprir todos os estágios do ciclo, dependendo das necessidades de cada uma.

Nesse sentido, no contexto da curadoria e dos modelos de curadoria, a preservação digital torna-se uma etapa a ser realizada. Para Santos (2016), a preservação digital evolui de abordagens simplistas, em que eram consideradas as atividades para tratamento das particularidades do documento digital separadamente, e

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

passa para abordagens holísticas, em que esse documento é considerado em todo o seu ciclo de vida.

> a criação de ciclos de vida da informação digital emergiu da necessidade de se gerir conteúdo, considerando a formulação e fluxos de trabalho para tipos específicos de proprietários de conteúdo. Neles, a informação em meio digital se move através de estágios, desde a sua criação até a preservação contínua, gestão e acesso ao longo do tempo (SANTOS, 2016, p.459).

Ao comparar os termos curadoria e preservação digital na literatura, Santos (2016) diz que a curadoria digital pode ser vista como evolução do entendimento das questões da preservação, mas ainda não é uma panacéia, para isso, seriam necessários muitos esforços, em todas as direções. A autora destaca, ainda, que a curadoria "não veio para substituir a preservação e sim incorporar as melhores práticas criadas e contribuir para a preservação da memória cultural e científica que é construída de modo distribuído, massiva e não estruturada" (SANTOS, 2016, p. 461).

Entendendo a preservação como uma preocupação da curadoria digital, percebe-se que o corpo de conhecimento apresentado na área de Gestão de Risco pode ser visto como um fortalecimento para as ações do ciclo de vida do objeto digital. Conforme Bairrão et al. (2017), a Gestão de Risco pode ser útil para o domínio da curadoria digital, uma vez que boa parte desta, lida com incertezas. Para os autores, a Gestão de Risco,

> compreende as ações de estabelecer uma infra-estrutura e cultura apropriadas, aplicando um método sistemático de estabelecer o contexto, identificando, analisando, avaliando, tratando, monitorando e comunicando os riscos associados a qualquer atividade, função ou processo (BAIRRÃO et al. 2017, p. 553-554, tradução nossa).

De fato, por ser a curadoria mais ampla que a preservação digital, englobando ações de gestão e, às vezes, até da arquivística, os riscos a mitigar no ciclo como um todo são maiores e mais diversos do que os riscos identificados no contexto da preservação digital. Assim, como afirmam Bairrão et al. (2017), as ferramentas e metodologias da Gestão de Risco são essenciais para identificar o risco, avaliá-lo e buscar formas de controlá-lo. Muito embora aplicar uma gestão de risco conforme pede a ISO 31000 pode ser caro, apenas acessível a grandes organizações com recursos disponíveis para tal.

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

Nesse cenário, os autores, apresentam um método capaz de estimar os custos relacionados aos controles que "são as medidas que temos que colocar em prática para minimizar a perda (preservação digital) ou maximizar o ganho (curadoria digital)" (BAIRRÃO et al. 2017, p. 555, tradução nossa).

O *Digital Curation Centre* juntamente com o *Digital Preservation Europe* desenvolveram um método baseado em avaliação de risco para ser aplicado em auto auditoria de repositórios digitais denominado de DRAMBORA[1]. Nesse método, o curador digital procura racionalizar as incertezas e ameaças que podem atingir a autenticidade e inteligibilidade do objeto digital, tranformando-os em riscos gerenciavéis. O processo permite a alocação eficaz de recursos, permitindo que os administradores do repositório identifiquem e categorizem as áreas onde as falhas são mais evidentes ou têm o maior potencial de interrupção. "O processo em si é interativo e, portanto, as recursões subsequentes avaliarão a eficácia das implementações anteriores de gerenciamento de riscos" (DRAMBORA, 2018, n.p.).

Apesar de não terem sido encontrados, ainda, muitos trabalhos de aplicação da Gestão de Risco no contexto da Curadoria Digital, mediante os trabalhos que fazem uso dela no contexto da preservação digital e das duas iniciativas apresentadas anteriormente (DRAMBORA e o trabalho de BAIRRÃO et al., 2017), é possível afirmar que a Gestão de Risco tem sido estudada no contexto da Curadoria Digital. Porém, ressalta-se que ainda não foi possível idealizar um modelo que contemple as ferramentas e metodologias dessa área, incorporadas a um ciclo de curadoria completo, como o desenvolvido pelo DCC.

Nesse modelo de ciclo de vida, a preservação é incorporada em duas etapas: nas **Ações para todo o ciclo de vida,** onde se encontra a etapa de **planejamento da preservação,** que compreende a formulação de um plano de preservação ao longo do ciclo de vida de curadoria do objeto digital. Isso inclui planos de gestão e administração de todas as ações do ciclo de vida de curadoria. Como também nas **Ações sequenciais** que incorpora a etapa de **Ações de preservação** que objetiva empreender ações para

[1] Método de Auditoria de Repositório Digital Baseado na Avaliação de Risco. Disponível em: https://www.repositoryaudit.eu/about/

DOI - 10.22478/ufpb.2318-6186.2019v6n2.43862
http://periodicos.ufpb.br/ojs2/index.php/archeion. ISSN 2318-6186. Licença

garantir a preservação em longo prazo. Ações de preservação devem garantir que o objeto permaneça autêntico, confiável e utilizável, mantendo a sua integridade.

Dessa forma, entende-se que o gerenciamento de risco deve ser incorporado nas ações do ciclo de curadoria, principalmente na etapa de planejamento, especialmente no planejamento da preservação, uma vez que é nessa etapa que é pensada toda a gestão do objeto digital nesse ciclo. Destaca-se que os riscos identificados não devem se restringir aos que já haviam sido mapeados no contexto da preservação digital, mas englobar também riscos concernentes à gestão dos objetos digitais, tais como os relacionados: a questões financeiras; ao mau dimensionamento/planejamento do projeto de curadoria; a falta de capacitação ou das competências necessárias nos recursos humanos para realização de atividades de curadoria; ao atraso na realização de atividades; a falta de documentação de ações realizadas; a falta de atualização de metadados ou o preenchimento inadequado destes, entre outros.

A partir de uma identificação mais ampla, seria possível pensar em quais ferramentas, metodologias, quais os especialistas envolvidos e qual o custo. Pois, como já colocado, cada processo de curadoria deve ser observado no contexto de um projeto específico, não havendo receitas genéricas que podem ser aplicadas a todo contexto. Visto que, cada acervo, cada instituição/organização, cada equipe e trabalho terão realidades diferentes e particularidades que precisarão ser analisadas para a Gestão de Risco.

4 CONSIDERAÇÕES FINAIS

Na ausência de contingências apropriadas que possam garantir a autenticidade, integridade e acesso dos objetos digitais a longo prazo, o desenvolvimento tecnológico, as mudanças organizacionais e políticas representam ameaças consideráveis para a continuidade desse objetos. Ou seja, objetos digitais podem estar em risco desde o momento de sua criação e inúmeros desafios são colocados buscando formas para identificar e mitigar esses riscos.

Nesse sentido, foram abordados nesse artigo os riscos a que esses objetos estão expostos e algumas medidas preventivas que podem ser utilizadas buscando minimizar

ou mitigar esses riscos e, com isso, buscar a defesa da informação digital contra ameaças e vulnerabilidades inerentes ao meio digital.

No tocante a Curadoria Digital, é importante destacar que, como ela envolve ações relacionadas a gestão, preservação e acesso, a Gestão de Risco acaba precisando englobar um mapeamento maior e mais completo, tornando-se, consequentemente, mais complexa. As reflexões aqui trazidas denotam a importância que a área de Gestão de Risco trás para o contexto da Curadoria Digital, a fim de prevenir ou amenizar que problemas ocorram durante o processo como um todo e, se ocorrerem problemas, que possam ser sanados com brevidade, com o mínimo de prejuízo e perdas. Nesse sentido garantindo a preservação e acesso a longo prazo aos objetos digitais.

RISK MANAGEMENT IN THE DIGITAL CURATION CYCLE

Abstract

In the context of the Digital Humanities, curating digital objects throughout their life cycle is a commitment required of all professionals who deal/work with collections of documentary, memorial, social and/or cultural historical relevance. For continuous access to digital objects and their management and preservation are becoming increasingly urgent. From this perspective, Risk Management emerges as a way to protect digital holdings from threats and vulnerabilities inherent in digital information storage and access systems. Thus, the present article seeks to explore the published literature on Risk Management, focusing on digital preservation, in order to identify the mapped risks and the indicated control measures, seeking to reflect on these processes in the context of the digital curation life cycle. The research is exploratory in nature and was delineated through a bibliographic survey conducted in national and international databases through the Google Schoolar search tool. The results reflect on the risks, threats, failures and vulnerabilities that affect digital information stocks and how they are being treated and/or controlled through the applicability of Risk Management tools in digital repositories. In this sense, it is urgent to think about the inclusion of these tools in the Digital Curator cycle, as one of the digital object management steps. Thus, it is proposed that Risk Management can be incorporated into the digital curation cycle in actions that permeate the entire life cycle of the digital object, being considered a continuous management activity.

Keywords: Digital Curator. Risk Management. Digital Preservation. Digital Object.

REFERÊNCIAS

ABBOT, Daisy**. What is digital curation?** Digital Curation Centre, 2008. Disponível em: <http://www.era.lib.ed.ac.uk/bitstream/1842/3362/3/Abbott%20What%20

is%20digital%20curation_%20_%20Digital%20 Curation%20Centre.doc>. Acesso em: 02 Jun. 2019

AGUIAR, Laís Alencar de. **Metodologias de análise e riscos APP e Hazop**. Rio de Janeiro, 2006?. Disponível em: <http://professor.ucg.br/SiteDocente/admin/arquivosUpload/13179/material/APP_e_HAZOP.pdf >. Acesso em: 20 fev. 2019.

BAIRRÃO, Raquel; PRADIANTE, Nuno; VIEIRA, Ricardo; BORBINHA, José. How can Risk Assessment techniques be used to estimate Costs for Digital Curation? In: VAQUINHAS, Nelson; CAIXAS, Marisa; VINAGRE, Helena. **Da produção à preservação informacional:** desafios e oportunidades. Évora: Publicações do Cidehus, 2017. Parte III Preservação Digital. p. 551-567. Disponível em: https://books.openedition.org/cidehus/2846. Acesso em: 20 fev. 2019.

BAKER, Mary; SHAH, Mehul; ROSENTHAL, David S. H.; ROUSSOPOULOS, Mema; MANIATIS, Petros; GIULI, TJ; BUNGALE, P.rashanth **A fresh look at the reliability of long-term digital storage**. 1 st EuroSys Conference. Leuven, Belgium, 2006.

BARATEIRO, José.; ANTUNES, Gonçalo; FREITAS, Filipe; BORBINHA, José. Designing Digital Preservation Solutions: A Risk Management-Based Approach. **The International Journal of Digital Curation**, n. 1, v. 5, 2010. Disponível em: http://repositorio.lnec.pt:8080/bitstream/123456789/1001078/1/205.pdf. Acesso em 13 fev. 2019.

BERNSTEIN, Peter L. **Desafio aos Deuses:** a fascinante história do risco. Rio de Janeiro: Campus, 1997

GALINDO, Marcos; LIMA, Arabelly Karla Ascoli . **Núcleo de Curadoria Digital da UFPE**: modelo de preservação da memória digital. In: XIX CONIC; III CONITI; VII JOIC. Recife, 2011.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

LAWRENCE, Gregory W.; KEHOE, William. R.; RIEGER, Oya Y.; WALTERS, William. H.; KENNEY, Anne R. **Risk Management of Digital Information:** A File Format Investigation, 2000, ISBN 1-887334-78-5. Disponível em: <http://www.clir.org/pubs/reports/pub93>. Acesso em: 23 fev. 2019.

NBR ISO 31000:2018. **Gestão de Risco**: diretrizes. Disponível em: <https://iso31000.net/norma-iso-31000-de-gestao-de-riscos/>. Acesso em: 15 fev. 2019.

SANTOS, Thayse Natália Cantanhede. Curadoria Digital e Preservação Digital: Cruzamentos Conceituais. **Rev. Digit.Bibliotecon. Cienc. Inf.** Campinas, SP, v.14, n.3, p.450-464, set/dez. 2016. Disponível em:

<https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8646336>. Acesso em: 12 fev. 2019.

PINTO, Maria Manuela. **Preservmap**: um roteiro da preservação na era digital. Porto: Edições Afrontamento, 2009.

ROSENTHAL, David S. H.; ROBERTSON, Thomas; LIPKIS, Tom; REICH, Vicky; MORABITO, Seth. Requirements for digital preservation systems: a bottom-up approach. **D-Lib Magazine**, v. 11, n. 11, 2005. Disponível em: <http://www.dlib.org/dlib/november05/rosenthal/11rosenthal.html>. Acesso em: 22 fev. 2019.

RIBEIRO, Fanny do Couto **Análise de Risco**: uma metodologia a serviço da preservação digital. 2011. Dissertação. (Mestrado em Ciência da Informação) – Universidade Federal de Pernambuco, Recife – PPGCI/UFPE, 2012. 285p.

TAVARES, Aureliana Lopes de Lacerda. **Análise de Risco e Preservação Digital**: uma abordagem sistêmica na rede memorial Pernambuco. 2014. Dissertação. (Mestrado em Ciência da Informação) - Universidade Federal de Pernambuco, Recife, 2014.