Análise comparativa entre os requisitos da RDC-Arq e a tecnologia *Blockchain*: uma perspectiva de profissionais arquivistas

Análisis comparativo entre los requisitos de RDC-Arq y la tecnología Blockchain: una perspectiva desde los archiveros profesionales

Comparative analysis between the requirements of RDC-Arq and Blockchain technology: a perspective from professional archivists

Alexandre MORI (1), Cláudio Gottschald DUQUE (1), Tomás Roberto Cotta ORLANDI (1), Wagner de Oliveira PEQUENO (2)

(1) Faculdade de Ciência da Informação – Universidade de Brasília – Campus Darcy Ribeiro – Brasília/DF – Brasil – CEP 70297-400, xmorihome@gmail.com, klauss@unb.br, tomasrober-to@gmail.com. (2) CEM 01 Sobradinho – Secretaria de Educação do Distrito Federal – Brasí-lia/DF – Brasil – CEP 73025-040, prof.wpequeno@gmail.com

Resumen

Se pretende analizar la tecnología blockchain en el contexto de los requisitos del RDC-Arq, guiados por la percepción de los conceptos de autenticidad e integridad de los documentos digitales, desde el punto de vista de los archiveros. Se buscó explorar las características de seguridad del software utilizado en la gestión de documentos digitales de archivo desde su perspectiva. Se investigó cómo se utiliza dicho software para garantizar la autenticidad e integridad de los documentos digitales y la opinión de los profesionales sobre el tratamiento que este software brinda a la cadena de custodia. Al final, se hace una comparación entre la tecnología blockchain y las características del RDC-Arq tal y cómo eran percibidas por los archiveros que participaron en la investigación. El análisis mostró que la tecnología blockchain tiene potencial para mantener la integridad y autenticidad de los documentos digitales, destacando la importancia de seguir las pautas del RDC-Arq.

Palabras clave: Blockchain. Documentos digitales. Autenticidad. Integridad. Brasil. Archiveros.

Abstract

Blockchain technology possibilities are analysed in the context of RDC-Arq requirements form the point of view of archivists' perception about digital documents authenticity and integrity. In particular, this article sought to explore software security features used for digital documents management by archivists. It was considered how that software is been used to preserve the authenticity and integrity of digital documents, and the professional opinion about how it contributes to preserve the chain of custody. Finally, a comparative between blockchain technology and the RCD-Arq features is elaborated from the perspective of the archivists participating in the research. The research shows that blockchain technology have good potential for maintening the authenticity and integrity of digital documents, highlighting the importance of following RDC-Arq guidelines.

Keywords: Blockchain. Digital documents. Authenticity. Integrity. Archivists. Brazil.

1. Introdução

A Internet surgiu de uma iniciativa militar americana em 1957 (DARPA, __) como contramedida ao avanço tecnológico soviético e se popularizou mundialmente através dos sistemas de hipertextos (Berners-Lee, 1990). Desde então, a Internet cresceu, se expandiu e se tornou peça-chave para as comunicações no mundo. Porém, ao mesmo tempo em que a Internet é utilizada para gerar benefícios, também é utilizada de maneira fraudulenta. Um dos grandes problemas enfrentados atualmente são as *fake news* (ou notícias falsas) (Buschman, 2019) (Dempsey, 2017).

Em ambientes onde não há um controle rigoroso da produção da informação digital, perde-se a garantia da autenticidade, uma vez que não será possível rastrear seu produtor. A produção, a cópia, a distribuição, a retenção, o versionamento de dados digitais, entre outras atividades, realizadas sobre a informação, fazem com que ela seja passível de adulteração e, assim, coloca-se em xeque sua originalidade.

Uma das preocupações dos arquivistas na atualidade é a manutenção da autenticidade dos documentos digitais (Kroth e Flores, 2018). Como garantir a inviolabilidade de um documento digital durante seu ciclo de vida? Quais as chances de sustentar esta autenticidade mesmo quando o documento atinge a idade de arquivo permanente? Um dos grandes problemas atualmente é a manutenção e garantia da integridade da

cadeia de custódia de um documento digital (Rogers, 2015) (Almeida *et al.*, 2012) (Seadle, 2012). Sustentar a autenticidade e integridade de um documento digital não depende somente de um sistema de informação que o guarde por longo período. É necessário criar mecanismos que garantam a manutenção da cadeia de custódia, integridade e autenticidade do documento digital.

O que se propõe neste texto é estabelecer uma correlação entre as respostas de arquivistas (obtidas através da aplicação de questionário) e os requisitos de um RDC-Arq de maneira que seja possível observar as percepções dos arquivistas em termos de preservação digital, mais especificamente em relação à autenticidade e à integridade de documentos arquivísticos digitais. Além disso, objetiva-se associar tais percepções com características da tecnologia *Distributed Ledger Technology* (DLT). Tais comparativos servirão de insumo para a proposta de uma arquitetura informacional que aborde as preocupações dos arquivistas em relação à preservação digital de documentos arquivísticos, requisitos do RDC-Arq e a tecnologia *blockchain*.

Além dos objetivos citados no parágrafo anterior, o intuito desta pesquisa é fomentar estudos posteriores sobre padrões ou propostas que contemplem os requisitos de segurança, integridade e autenticidade do CONARQ e OAIS (que contempla a ISO 14721) e que possibilitem aderência ao RDC (Repositório Digital Confiável, norma ISO 16363), culminando na melhoria das técnicas e estratégias de manutenção de integridade e autenticidade de documentos digitais por toda a cadeia de custódia.

2. Marco teórico

A seleção de obras seguiu a revisão não sistemática ou revisão narrativa (Cordeiro *et al*., 2007), por terem sido selecionadas aleatoriamente, mas com maior proximidade dos autores. No entanto, foram selecionados autores teóricos da arquivística e estudiosos da DLT. Além disso, para esta pesquisa, foram delimitadas fontes de pesquisa como se segue: site de periódicos da Capes, bancos de teses e dissertações, Google Scholar bem como fontes diretas de documentos normativos, como o site do CONARQ. Como tema para as buscas, seguiu-se as palavras-chave "arquivística", "cadeia de custódia" ou "arquivo permanente" em conjunção com os termos "*blockchain*" ou "DLT" ou "*distributed ledger technology*".

2.1. Documentos digitais

Há algum tempo, a crescente produção de documentos digitais já era percebida (CONARQ, 2004, p. 1). Duranti (2010, p. 79) cita que foram produzidos mais registros entre os anos de 2000 e 2010 do que em toda a atividade humana anterior a esta década. Saracevic (1995, p. 2) já afirmava que a Ciência da Informação está intrinsecamente ligada à tecnologia da informação. A natureza dos artefatos digitais que circulam pela Internet, faz deles objetos efêmeros ao mesmo tempo em que reduzem o esforço necessário para o deslocamento físico dos artefatos que os representam.

Tais espaços físicos remetem à Teoria das Três Idades, popularizada por Schelenberg (Stapleton, 1983) e ao conceito de custódia, um dos fundamentos na definição de arquivo de Jenkinson (1922).

A digitalização facilitou e agilizou a tramitação e o gerenciamento de documentos arquivísticos. No entanto, para viabilizar esta facilidade e rapidez, os dados são convertidos em bits e bytes, que são voláteis. Considera-se que isto seja um dos grandes problemas para a Arquivologia. Converter um sinal elétrico em algo persistente a longo prazo – similarmente a um livro – é, de fato, um desafio aos cientistas (Almeida *et al*., 2012, p. 104).

O documento digital é definido como "informação registrada, codificada em dígitos binários, acessível interpretável por meio de um sistema computacional" (CONARQ, 2016, p. 21). O documento arquivístico digital é o documento arquivístico que segue a definição de documento digital. O documento arquivístico é definido como: "documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência" (CONARQ, 2016, p. 20). Portanto, deduz-se que o documento arquivístico digital é o documento digital de natureza arquivística e que possui valor para a instituição, empresa ou entidade que o produziu ou o recebeu.

Os documentos digitais, por um lado, trouxeram grandes vantagens como a redução de espaço físico de armazenamento, a agilidade de recuperação e tramitação, a facilidade de distribuição e a possibilidade de duplicação a um custo irrisório. Por outro lado, trouxeram a efemeridade (conforme os mecanismos de deleção dos SIGAD – Sistemas Informatizados de Gestão Arquivística de Documentos), a dificuldade em se determinar a originalidade e autenticidade dos documentos, bem como problemas de segurança e confidencialidade da informação. Da mesma maneira como muitas soluções foram vislumbradas, muitos problemas também foram identificados. Esta discussão também é abordada em Santos e Flores (2015).

Há ainda que se garantir a organicidade dos documentos arquivístico. A organicidade é um

conceito essencial nos estudos da arquivologia, pois manter as características individuais de um documento associadas às características organizacionais é importante para as empresas e instituições (Belloto, 2002, p. 23).

Para se manter a organicidade dos documentos digitais é necessário armazenar os metadados corretamente. Isto significa dizer que é importante que o profissional arquivista determine quais os metadados de um documento digital são relevantes (indispensáveis e/ou necessários) para se estabelecer o vínculo do documento digital à entidade que o detém. Cabem aí propriedades temporais (em qual data), organizacionais (em qual área/seção/departamento), motivacionais (o porquê de se reter tal documento), estruturais (características do documento, como campos, trechos ou blocos de informação) e outros mais que forem necessários (Arellano, 2004, p. 19). É importante ainda criar mecanismos que garantam a originalidade e autenticidade dos documentos digitais mesmo depois de receberem assinaturas (ou quaisquer outras marcações) durante sua tramitação.

2.2. Distributed Ledger Technology (DLT)

Distributed Ledger Technology pode ser traduzido literalmente por Tecnologia de Livro-Razão Distribuído. Esta tecnologia fundamenta-se em registros (como nos livros-razão de contabilidade) adicionados a uma lista de registros de maneira distribuída. Ou seja, é como se vários livros-razão iguais fossem mantidos por várias pessoas. Essa tecnologia é bastante reconhecida atualmente pelo seu uso em *blockchains*.

A tecnologia *blockchain* é recente e está sendo aplicada a vários cenários do mundo digital (Rossum, 2017, p. 2). Supostamente ela surgiu em 2008 no Japão através do seu criador, conhecido por Satoshi Nakamoto (Nakamoto, 2008), que apresentou através de seu artigo uma estratégia tecnológica de distribuição de confiança, baseado em distribuição de *hashes*, ou chave criptográfica.

Blockchain significa – em sua literalidade – cadeia de blocos, que é frequentemente relacionado às criptomoedas (Lemieux, 2016, p. 118). Não é por acaso que a tecnologia *blockchain* é a base de vários sistemas de moedas virtuais (Bitcoin, Ethereum, Ripple, Bitcoin Cash, EOS, Litecoin, Stellar Lumens, Cardano, IOTA, entre outras). Há que se garantir confiança para que pessoas possa comprar tais moedas virtuais, que é um dos fundamentos do *blockchain*.

Para compreender o conceito desta tecnologia, considere vários cartórios que trabalham em sincronia para todos os documentos que eles autenticam, emitem ou cancelam. Para qualquer atividade que um único cartório execute, todos os outros recebem a informação de tal atividade e a anotam em suas respectivas trilhas de atividades executadas (independentemente do cartório que a executou). Neste cenário, é de se esperar que todas as trilhas de qualquer um destes cartórios estejam iguais. É como se cada cartório, após criar uma atividade na trilha, enviasse tal trilha para os demais cartórios. Assim, todos eles teriam trilhas idênticas.

O *blockchain* funciona distribuindo as cadeias entre os nós. No entanto, os cartórios são computadores (normalmente, denominado de servidores ou nós da rede) que replicam a informação executada por qualquer outro computador na rede. Para cada atividade ou operação, todas as trilhas (chamada de *chain* ou *ledger*) são atualizadas em todos os computadores.

Esta trilha é composta de *hashes*, e um *hash* é uma sequência de letras e número aleatórios gerados por uma técnica computacional de criptografia de dados (Carter e Wegman, 1979). A característica principal de um *hash* é a geração de uma sequência aleatória de números e letras de maneira que nunca uma combinação seja igual a outra, mesmo que os dados de origem sejam muito parecidos. Desta forma, para todas as atividades executadas por um servidor, um *hash* (bloco ou *block*) é gerado e adicionado ao *hash* anterior (cadeia ou *chain*). Daí o termo *blockchain*, pois cada atividade gera um bloco e este bloco é adicionado à cadeia de blocos anterior.

Para se adulterar um *blockchain* seria necessário alterar a trilha ou todos os *hashes* de um nó e replicá-lo para os outros nós. Trata-se de uma tarefa árdua. No entanto, o *blockchain* funciona somente com adição de blocos e nunca com alteração ou exclusão deles. Assim, garante-se autenticidade dos dados e a guarda de um histórico das operações. Os documentos digitais podem, então, ser armazenados seguramente em um *blockchain* e, através disso, estabelecer um repositório digital confiável. O que é o RDC-Arq e quais os requisitos a serem atendidos são explanados na seção seguinte.

2.3. Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq)

O RDC-Arq é a especificação de um repositório arquivístico digital confiável que segue a ISO 14721 (ISO, 2012). Conforme o CONARQ (2015, p. 9): “Um repositório arquivístico digital é um repositório digital que armazena e gerencia esses documentos, seja nas fases corrente e intermediária, seja na fase permanente.” O repositório é também capaz de manter o acesso aos

documentos garantindo o armazenamento, os metadados, a organicidade e a autenticidade (identidade e integridade) dos documentos.

Para se tornar confiável, um repositório digital arquivístico deve atender a todos os procedimentos arquivísticos bem como os requisitos de um repositório digital confiável (RLG e OCLC, 2002, p. 5). Para tanto, os sistemas que se propõem a ser um RDC-Arq devem cumprir os seguintes requisitos, que se subdividem em três partes (seção II.2 de CONARQ, 2015):

Infraestrutura organizacional	*1a. Governança e viabilidade organizacional – continuidade do repositório ou plano de contingência nos casos de extinção da organização ou mudança de escopo.*
	1b. Estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficiente.
	1c. Transparência de procedimentos e arcabouço político – definição de procedimentos e auditorias que assegurem que o repositório está fazendo para o qual foi definido e de maneira correta e eficiente.
	1d. Sustentabilidade financeira – capacidade de despender menos do que arrecada.
	1e. Contratos, licenças e passivos – estes instrumentos devem especificar todos os direitos e deveres do repositório para com seus documentos digitais.
Gerenciamento do documento digital	2a. Admissão: captura de documentos digitais – SIP (Submission Information Package) >> AIP (Archival Information Package) >> seguro em um repositório.
	2b. Admissão: criação do pacote de arquivamento – complementar o SIP para arquivamento.
	2c. Planejamento da preservação – planejamento para evitar obsolescência e fragilidade do suporte.
	2d. Armazenamento e preservação / manutenção do AIP – garantia de preservação de longo prazo (guarda do documento original e das migrações – refrescamentos).
	2e. Gerenciamento de informação – garantia de recuperação da informação.
	2f. Gerenciamento de acesso – gestão das permissões e distribuições dos documentos e cópias.
Tecnolog.	3a. Infraestrutura de sistema – gestão.
	3b. Tecnologias apropriadas – hardware e software.
	3c. Segurança – garantia de segurança em todos os sentidos.

Quadro 1. Requisitos de um RDC-Arq

2.4. Arquitetura da Informação

A proposta deste texto é a organização da informação, mais especificamente a arquitetura da informação a ser direcionada ao estabelecimento de um espaço informacional que permita a estruturação da informação arquivística compartilhada e ao mesmo tempo flexível para toda espécie de arquivo.

Segundo Dillon e Turnbull (2003, p. 2), as definições de Arquitetura da Informação se concentram na ideia de espaços informacionais estruturados (organizados) para gestão e uso da informação. Os espaços informacionais, por sua vez, são locais onde a informação está disponível. Considerando estes conceitos, a definição de um modelo de arquitetura informacional é a definição de mecanismos ou processos organizadores da informação visando ao atendimento dos usuários de tal espaço informacional.

Conforme Rosenfeld *et al*. (2015, p. 24), a Arquitetura da Informação pode ser definida através da composição de quatro "sub-definições", a seguir:

> O desenho de estruturas de ambientes de compartilhamento de informação.
>
> A combinação de sistemas de organização, de rotulação, de busca e de navegação em websites e intranets.
>
> A arte e ciência de moldar produtos e experiências de informação de forma a suportar a usabilidade e a localização (da informação).
>
> Uma disciplina emergente e uma comunidade de prática focada em trazer princípios de desenho e arquitetura a um cenário digital.

Esta última definição, mais detalhada, diz respeito à organização da informação de maneira que ela se torne útil ao usuário. Dentre estas quatro "sub-definições", duas citam ambientes digitais, demonstrando que tais ambientes têm grande influência sobre a definição da Arquitetura da Informação. No entanto, a essência da definição é a mesma de Dillon e Turnbull (2003, p. 2) citada anteriormente.

Ainda segundo Rosenfeld *et al.* (2015, p. 82-83), uma arquitetura da informação é composta pelos seguintes componentes: sistemas de organização da informação: diz respeito sobre como estruturar a informação; sistemas de rotulagem: diz respeito sobre como dar nome às coisas; sistemas de navegação: diz respeito sobre como navegar pela informação; e sistemas de busca: diz respeito sobre como procurar a informação.

Para a proposta deste texto, a definição e os componentes servirão como passos ou características a serem seguidas na elaboração de um possível protótipo nos trabalhos seguintes. Ao adotar-se a DLT para melhorias da cadeia de custódia dos documentos arquivísticos digitais, percebe-se que a definição de um modelo de arquitetura de informação é imprescindível.

3. Metodologia

A pesquisa qualitativa era utilizada para fins exploratórios no início de projetos (Bauer e Gaskell, 2003, p. 26). Nesse mesmo intuito, neste experimento, foram aplicados questionários de treze (13) questões que contemplam a descoberta da relação entre alguns problemas da arquivologia sobre custódia de documentos arquivísticos.

O objetivo do método adotado foi delinear preliminarmente os problemas relacionados à integridade e à autenticidade dos documentos arquivísticos de maneira a guiarem os autores a relacionar os requisitos do RDC-Arq à tecnologia *blockchain*. Além disso, os participantes foram instigados a comparar a segurança dos softwares atualmente utilizados em relação à segurança bancária, que hoje é uma das mais evoluídas em termos tecnológicos. Não foi objetivo deste trabalho levantar os principais problemas dos SIGADs (ou outros softwares) ou ainda ter uma representatividade de tais problemas em um determinado universo, mas perceber a existência de problemas de softwares ligados à gestão arquivística.

A precisão dos conceitos também foi implicitamente posta em avaliação, com menção a termos como cadeia de custódia, SIGAD e GED. Antes mesmo da aplicação do questionário, durante a sua criação, alguns arquivistas foram consultados sobre a coerência e consistência dos conceitos e estruturação das perguntas. Também são citados alguns softwares de mercado que gerenciam documentos. Não necessariamente no sentido arquivístico da gestão documental, mas softwares que têm alguma relação com o armazenamento de documentos.

Outro intuito da adoção da pesquisa qualitativa para este trabalho foi dar voz aos pesquisados, uma vez que se pretendeu ver "através dos olhos daqueles que estão sendo pesquisados" (Bryman, 2012, p. 399). Assim, optou-se pela pesquisa estruturada com questões iguais a todos os participantes, com respostas abertas. Ou seja, não havia limitação de tamanho ou do conteúdo da resposta favorecendo a coleta da opinião de cada participante.

No trabalho foram aplicadas as codificações descritiva, tópica e analítica. A codificação consistiu em criar códigos para sintetizar as características das respostas dos participantes e permitir melhor compreensão do teor dessas respostas. Ela segue em um sentido de uniformização das respostas pelos códigos. A codificação analítica comumente exige interpretação da resposta. Registra-se que tais codificações basearam-se no método de análise de conteúdo.

Esta pesquisa seguiu ainda o viés exploratório, pois teve por objetivo fornecer insumos para a melhor compreensão do objeto de estudo que é a relação entre os requisitos de autenticidade e integridade do RDC-Arq com a tecnologia *blockchain*. Também visou auxiliar o aprofundamento no assunto bem como identificar hipóteses e estratégias de experimentos para as próximas pesquisas.

3.1. Questionário aplicado

No.	*Questão*
01	A sua função na empresa/instituição onde trabalha é de arquivista?
02	Qual é a sua empresa/instituição onde trabalha?
03	Qual é a unidade federativa de sua empresa / instituição?
04	Qual é(são) o(s) nome(s) do(s) software(s) para tratamento do ciclo de vida dos documentos digitais (SIGAD's, GED's, ECM's, repositórios digitais, etc.) utilizado(s) em sua empresa/instituição?
05	O(s) software(s) utilizado(s) possui(em) características ou capacidades para garantir a integridade da cadeia de custódia dos arquivos digitais, inclusive na fase permanente?
06	Os documentos digitais da empresa/instituição em que atua estão efetivamente seguros (íntegros e autênticos) com o(s) software(s) de tratamento arquivístico que utilizam?
07	A segurança citada na questão anterior aplica-se a toda a cadeia de custódia?
08	Você acredita que a informações armazenadas/tramitadas em/entre bancos (Bradesco, Itaú, Banco do Brasil entre outros) estão mais seguras do que os documentos digitais armazenados ou transferidos em/entre softwares de tratamento arquivístico atuais? Por que?
09	Na sua opinião, por que preservar a autenticidade, segurança e a integridade de documentos digitais é uma tarefa difícil?
10	Comente a seguinte afirmação: atualmente, no mercado, já existem softwares suficientes para tratamento do ciclo de vida dos documentos arquivísticos digitais, mantendo-os autênticos, seguros e íntegros.
11	O que você acha do SEI (http://www.planejamento.gov.br/sei) em termos de cadeia de custódia, autenticidade, integridade e segurança de documentos digitais?
12	Qual a sua opinião sobre o Archivematica (https://www.archivematica.org/en/) em termos de cadeia de custódia, autenticidade, integridade e segurança de documentos digitais?
13	Qual a sua opinião sobre o AtoM (https://www.accesstomemory.org/pt-br/) em termos de cadeia de custódia, autenticidade, integridade e segurança de documentos digitais?

Quadro 2. Questões aplicadas aos participantes

O conjunto de questões foi elaborado e posteriormente submetido a dois arquivistas como meio de refinar a coerência e consistência das perguntas. Posteriormente às críticas, foi gerada uma segunda versão do questionário que foi, então, enviada por e-mail aos participantes, profissionais que atuam como arquivistas em diversas organizações do Brasil convidando-os a responder um questionário registrado no Google Forms.

O questionário foi enviado para as seguintes associações de arquivistas: Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Minas Gerais, Paraíba, Paraná, Rio de Janeiro, Rio Grande do Sul, Santa Catarina e São Paulo. As referidas associações estão disponíveis na página de associações de profissionais arquivistas do CONARQ (2014) e foram consideradas como existentes, uma vez que outras associações não são encontradas facilmente pela Internet ou são inexistentes. As perguntas foram elaboradas com o intuito de levantar o cenário da situação e das ferramentas utilizadas atualmente por arquivistas no país. As questões aplicadas são apresentadas no Quadro 2.

Quanto às questões de 1 a 3, são sociológicas e têm por objetivo visualizar a distribuição dos respondentes e se eles têm relação ou trabalham com arquivos.

A questão 4 foi necessária para validar o envolvimento do respondente com um sistema de gestão arquivística e gerar essa consciência por parte dele para as demais questões.

As questões 5 e 6 têm relação com o objetivo de identificar a percepção de arquivistas em relação à garantia de integridade do arquivo.

As questões 6 e 7 referem-se ao objetivo de capturar a percepção dos arquivistas em relação à autenticidade de arquivos.

A questão 8 teve por objetivo verificar o grau de confiabilidade em termos de integridade e autenticidade do arquivo em relação aos sistemas bancários, tidos como muito seguros atualmente.

As questões 9 e 10 têm relação com a captura da percepção do respondente em relação aos temas abordados na pesquisa.

As questões 11, 12 e 13 são similares às questões 9 e 10, mas com foco em softwares bem conhecidos pelos arquivistas.

Apesar do questionário permitir respostas abertas, foi possível estabelecer uma categorização das respostas conforme segue:

Nas questões 1, 6 e 7, as categorias identificadas nas respostas foram “Sim” e “Não”.

Na questão 2, as categorias identificadas nas respostas foram “pública”, “privada” ou “mista” em relação ao tipo de economia de cada instituição ou empresa.

Na questão 3, as categorias identificadas nas respostas foram as unidades federativas do país.

As questões 5 e 8 continham respostas com categorias similares às questões 1, 6 e 7, isto é, “sim” e “não”, mas também continham a categoria “não sei”.

Na questão 9, as categorias identificadas foram “problemas tecnológicos”, “problemas humanos” e “Não concordam ou não souberam responder”.

Finalmente, na questão 10, foram identificadas as seguintes categorias nas respostas dos pesquisados: “poucos”, “não existe”, “raros”, “existem” e “não sei”.

As demais questões não tiveram suas respostas categorizadas.

4. Resultados e discussões

Esta seção é subdividida em duas subseções: a primeira apresenta os resultados da pesquisa com foco nas questões relacionadas à cadeia de custódia, segurança, autenticidade e integridade dos documentos digitais. Na segunda parte, considerando as respostas obtidas, os pontos relevantes do RDC-Arq são identificados e relacionados à tecnologia *blockchain*.

4.1. Análise das respostas ao questionário

Dentre os vinte (20) participantes da pesquisa, um quarto (5 ou 25%) não são arquivistas, mas trabalham com arquivo. Tal número de participantes foi suficiente dado que o objetivo da pesquisa era identificar quantidade suficiente de percepções relacionadas aos requisitos de um RDC-Arq.

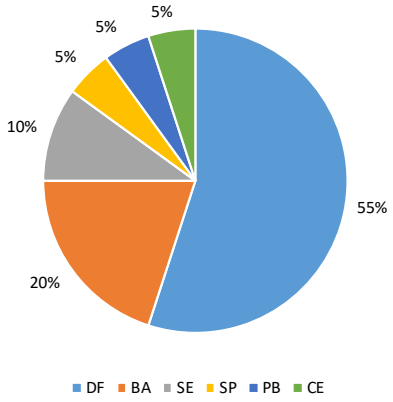

Figura 1. Unidade federativa dos participantes

Três quartos dos participantes (15 ou 75%) trabalham diretamente na função de arquivista e mais da metade dos participantes (11 ou 55%) são do Distrito Federal. Bahia e Sergipe estão representados nesta pesquisa com quatro (4 ou 20%) e dois (2 ou 10%) participantes, respectivamente. São Paulo, Paraíba e Ceará possuem participação igual (1 participante ou 5%). Das instituições ou entidades que foram representadas, dezoito (18 ou 90%) são públicas, uma (1 ou 5%) é privada e uma (1 ou 5%) é de economia mista.

As respostas às questões 5, 6 e 7 demonstram que a maioria dos participantes não acredita que os softwares utilizados garantem integridade da cadeia de custódia, bem como a integridade e autenticidade dos documentos digitais. Na questão 5, sobre a existência de características ou capacidades no software para garantia de integridade dos documentos digitais na cadeia de custódia, sete (35%) participantes responderam sim, onze (55%) responderam não e dois (10%) não souberam responder.

Sobre a questão 6, todos os participantes responderam com sim ou não. Cinco (25%) confiam que seus documentos digitais estão seguros com o software que utilizam e 15 (75%) responderam que não à mesma pergunta.

Na questão 7 foi realizada pergunta semelhante à questão 6, mas diretamente relacionada a toda a cadeia de custódia, evidenciando o objetivo de observar a segurança dos documentos digitais em todas as idades. Sete (35%) responderam que sim e 13 (65%) responderam que não.

O destaque das respostas está na identificação de duas respostas apontando os softwares de arquivo permanente como os menos preparados para garantir tal segurança dos documentos digitais. Além disso, um respondente evidenciou sua desconfiança a tudo que é digital. Isso representa uma grande preocupação dos arquivistas hoje: a falta de suporte físico que coloca o objeto digital em um alto nível de risco de perda. Tal afirmação se sustenta em outras respostas das perguntas posteriores.

Com essa questão foi possível identificar algumas preocupações com os softwares utilizados.

Uma das perguntas do questionário cita a comparação da segurança aplicada aos sistemas bancários e a segurança dos sistemas de gestão arquivística de documentos (questão 8). A maioria (55%) acredita que os sistemas bancários são mais seguros devido ao maior grau de investimento e pela preocupação com a imagem e a confiança da instituição. Três participantes não souberam ou optaram por não responder, conforme a Figura 2.

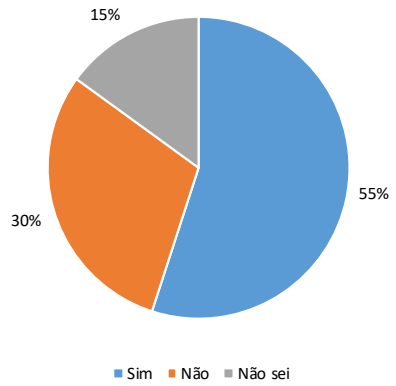

Figura 2. Segurança de sistemas bancários versus segurança de sistemas de gestão arquivística de documentos digitais

As preocupações apresentadas remetem aos requisitos necessários a um RDC-Arq. Uma análise pode ser realizada sobre as respostas dos pesquisados. Os itens que se seguem demonstram os resultados em relação aos requisitos listados na seção 2.3 deste texto.

Primeiramente, observa-se os respondentes que acreditam que softwares bancários são mais seguros que os softwares de gestão arquivística atuais:

- Quatro (4) respondentes disseram que bancos investem mais em segurança, com respostas que remetem ao requisito 1b. (estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficientes) e 3a. (infraestrutura de sistema – gestão).
- Quatro (4) respondentes citam que bancos possuem as melhores tecnologias de segurança atualmente. Estas respostas referenciam o requisito 3b. (tecnologias apropriadas – hardware e software).
- Um (1) respondente opinou dizendo que a área de arquivologia ainda é imatura neste sentido. Os requisitos relacionados são o 1a. (governança e viabilidade organizacional – continuidade do repositório ou plano de contingência nos casos de extinção da organização ou mudança de escopo) e 1b. (estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficientes).

Ainda na questão 8, observa-se os respondentes que não acreditam que softwares bancários são mais seguros que os softwares de gestão arquivística atuais:

- Dois (2) respondentes comentaram que bancos não implementam as recomendações da OAIS ou do RDC-Arq, conforme o requisito

3b. (tecnologias apropriadas – hardware e software).

- Um (1) respondente comentou que sistemas bancários podem ser melhores, mas ainda dependem de pessoas, que podem tornar um sistema seguro ou inseguro. Tal resposta referência o requisito 1b. (estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficientes).

A questão 9 suscitou respostas que também puderam ser vinculadas aos requisitos de um RDC-Arq. O objetivo dela foi extrair dos participantes o porquê da dificuldade em se manter a integridade e a autenticidade dos documentos digitais. Somente um (1) participante mencionou que esta não é uma tarefa difícil. As respostas dos demais participantes podem ser resumidas pela Quadro 3.

#	*Quantidade e teor das respostas*	*Requisito do RDC-Arq correspondente (seção 4)*
	Problemas tecnológicos	
1	Dois (2) participantes citaram a obsolescência da tecnologia utilizada como principal problema.	2e.) Gerenciamento de informação – garantia de recuperação da informação. 3b.) Tecnologias apropriadas – hardware e software.
2	Fácil acesso ao documento foi citado por dois (2) respondentes como sendo o principal problema.	2f.) Gerenciamento de acesso – gestão das permissões e distribuições dos documentos e cópias.
3	Fácil adulteração/corrupção do documento foi citado por dois (2) respondentes como sendo o principal problema.	3c.) Segurança – garantia de segurança em todos os sentidos.
4	Falta de suporte físico como garantia para a preservação foi citado por um (1) respondente como principal problema.	3a.) Infraestrutura de sistema – gestão. 3b.) Tecnologias apropriadas – hardware e software.
	Facilidade de deleção foi citado por um (1) respondente como principal problema	3b.) Tecnologias apropriadas – hardware e software.
6	Criptografia fraca foi citado por um (1) respondente.	3c.) Segurança – garantia de segurança em todos os sentidos.
	Problemas humanos	
7	Falta de capacitação foi citado por quatro (4) participantes.	1b.) Estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficiente.
8	Falta de investimento foi citado por dois (2) participantes.	1a.) Governança e viabilidade organizacional – continuidade do repositório ou plano de contingência nos casos de extinção da organização ou mudança de escopo.
9	Erros são a natureza do ser humano foi citado por uma (1) pessoa.	1b.) Estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficiente. 3b.) Tecnologias apropriadas – hardware e software. 3c.) Segurança – garantia de segurança em todos os sentidos.
10	Falta de cooperação entre pessoas (equipes de TI e arquivistas) foi citado por um (1) participante.	1b.) Estrutura organizacional e de pessoal – pessoal em quantidade e qualidade suficiente.
11	Falta de priorização desta característica foi citado por dois (2) participantes.	1a.) Governança e viabilidade organizacional – continuidade do repositório ou plano de contingência nos casos de extinção da organização ou mudança de escopo.

Quadro 3. Análise das respostas sobre as dificuldades de se preservar a segurança, integridade e autenticidade de documentos digitais

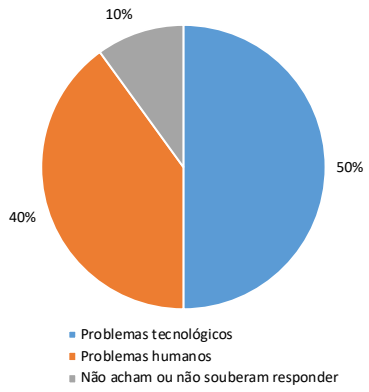

Figura 3. Proporção das respostas divididas em problemas tecnológicos e problemas humanos

Sobre a quantidade de justificativas em relação a problemas tecnológicos e problemas humanos,

as respostas ficaram distribuídas conforme a Figura 3.

Uma das questões abordou a suficiência de softwares que, considerando a cadeia de custódia arquivística, garantam a segurança, integridade e autenticidade dos documentos digitais. Por ser uma pergunta direcionada ao conhecimento dos participantes em relação aos softwares existentes, a proporção das respostas ficou equilibrada, como se pode observar na Figura 4.

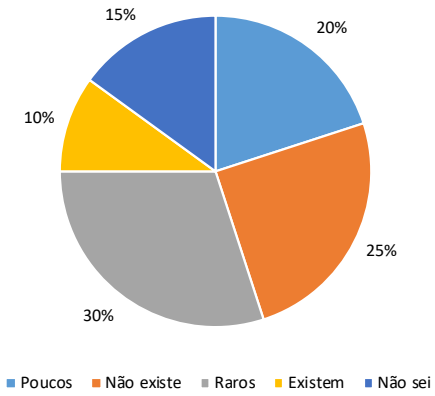

Figura 4. Existência de softwares suficientes para tratamento documental arquivístico

As demais questões foram direcionadas a softwares específicos, a saber: SEI (Brasil, s.f.), Archivemática (Artefactual, 2019) e AtoM (Artefactual, 2015). Desses três, os dois últimos (Archivemática e AtoM) são os menos conhecidos, porém contam com boa reputação dentre os participantes. Os comentários adicionais foram no sentido de que tais softwares necessitam de capacitação técnica para utilização.

Já o SEI é um software do governo e, portanto, conhecido pelos participantes (que em sua grande maioria são de órgãos públicos). Assim, foi possível extrair algumas críticas em relação a este software: não é um SIGAD - não foi desenvolvido para este fim (cinco respondentes); não garante a autenticidade dos documentos; funcional somente para a idade corrente (dois respondentes); não possui um sistema de recuperação eficaz; não possibilita análise detalhada dos processos contidos nele; não possui tabela de temporalidade dos documentos; e não implementa um RDC-Arq.

Muitas melhorias do SEI estão sendo construídas. Porém, por ser um software de uso extensivo na esfera governamental, há que se considerar a capacidade de desenvolvimento de novas funcionalidade e correções demandadas para uma equipe não tão grande. São trezentos e sessenta e seis entidades – das esferas municipais, estaduais ou federais – que ou formalizaram o pedido de utilização, ou já utilizam o software, conforme dados do Ministério do Planejamento, Desenvolvimento e Gestão (2018).

4.2. Pontos relevantes do RDC-Arq e a tecnologia *blockchain*

Foi possível observar através desta pesquisa, a preocupação dos arquivistas em relação à integridade e à autenticidade de documentos digitais através da cadeia de custódia dos softwares utilizados. Na análise de resultados, guiados pelas respostas dos participantes, foram identificados sete pontos relevantes (do total de quatorze), retirados dos requisitos do RDC-Arq:

1) Requisito 1a. do RDC-Arq: Governança e viabilidade organizacional. Esse requisito se preocupa com a continuidade do repositório ou plano de contingência nos casos de extinção da organização ou mudança de escopo. A tecnologia *blockchain* pode garantir a mesma estrutura e funcionamento dos repositórios por um tempo indeterminado, pois o *blockchain* baseia-se na descentralização e compartilhamento dos dados (Lemieux, 2017). Mesmo que uma organização venha a se extinguir, os dados armazenados em um *blockchain* persistirão em outros nós da rede. Não é descartada, porém, a existência de uma política de preservação para cada entidade ou instituição.

2) Requisito 1b. do RDC-Arq: Estrutura organizacional e de pessoal. Esse requisito diz respeito aos recursos humanos em quantidade e qualidade suficiente. Trata-se de um requisito organizacional. A DLT não é capaz de atender totalmente a ele. No entanto, os sistemas de informação computacionais associados à tecnologia *blockchain* podem reduzir muito a necessidade de recursos humanos, porém não os descartando completamente.

3) Requisito 2e. do RDC-Arq: Gerenciamento de informação. A garantia de recuperação da informação é um requisito importante para a área arquivística. É da natureza dos softwares que implementarem um *blockchain* possuírem funcionalidades de recuperação da informação. Um *blockchain* por si só já garante o armazenamento dos dados enquanto os nós de uma rede estiverem funcionando. A recuperação, visualização, permissão entre outras tarefas, deverão ser definidas por uma política de gestão arquivística.

4) Requisito 2f. do RDC-Arq: Gerenciamento de acesso. Trata a gestão das permissões e distribuições dos documentos e cópias, que é um dos pontos importantes no caso do uso de um *blockchain*. As chamadas carteiras (*wallets*) em

blockchains de moedas virtuais armazenam chaves que permitem acesso somente ao proprietário. Assim é um requisito válido para um *blockchain* voltado à gestão arquivística de documentos digitais. Ou seja, as tecnologias de criptografia deverão existir resguardando a confidencialidade de documentos dessa categoria e permitindo o acesso a outros de natureza pública ou aberta.

5) Requisito 3a. do RDC-Arq: Infraestrutura de sistema. Um *blockchain* tem a capacidade de fornecer suporte à gestão de infraestrutura de sistemas, pois uma de suas características é a manutenção de cópias da cadeia em vários nós da rede. Isto simplifica ou elimina a necessidade de procedimentos e estratégias de backups. A sincronia de cópias são processos que propagam e replicam os dados dos próprios blocos pela rede que formam o *blockchain*. No entanto, nós de baixa performance (velocidade de processamento) podem degradar a velocidade de propagação dos dados pela rede. Nesse caso, não é a tecnologia *blockchain* em si que reduz a performance, mas a própria capacidade da empresa ou instituição participante do *blockchain*.

6) Requisito 3b. do RDC-Arq: Tecnologias apropriadas. Um *blockchain* não define ou determina o uso de nenhum hardware ou software específico (somente aqueles necessários à conexão com a rede). Basta que o hardware em conjunto com o software sejam capazes de se conectar a outros conjuntos de hardware e software para criar nós da rede *blockchain*. Obviamente, será necessário desenvolver outras funcionalidades para o tratamento documental arquivístico.

7) Requisito 3c. do RDC-Arq: Segurança. Esse requisito diz respeito à garantia de segurança. O *blockchain* é uma tecnologia que é considerada segura por encadear seus blocos via criptografia de dados. Em outras palavras, a possibilidade de corrupção ou alteração indevida das informações dos blocos de um *blockchain* é reduzida. Para acessar e criar novos blocos será necessário que os usuários acessem um sistema que esteja ligado ao *blockchain* e que os usuários utilizem senhas criptografadas.

5. Conclusões

Este artigo se propôs a identificar, através das respostas dos participantes da pesquisa, questões relacionadas à segurança, integridade e autenticidade dos documentos digitais em softwares utilizados atualmente por arquivistas (ou indivíduos que trabalham diretamente com arquivo). A partir das respostas, buscou-se criar ligações entre elas e os requisitos de um RDC-Arq e comparar os requisitos identificados com características do *blockchain*. Os resultados poderão ser utilizados para elaborar um modelo de arquitetura de informação que contemple o uso da DLT para melhorar questões de segurança abordadas na pesquisa.

É fato que o *blockchain* ainda é uma tecnologia que trabalha com dados em formato digital e isto ainda é motivo de preocupação, pois a informação ainda está sob um suporte efêmero. No entanto, as estratégias de grandes empresas (bancos inclusive) se sustentam em técnicas de replicação e redundância de dados para manter a informação disponível. O mecanismo de distribuição de dados e compartilhamento do *ledger* da DLT é da natureza desta tecnologia. Em outras palavras, a replicação dos dados é parte da DLT. Isto significa que quanto mais nós na rede, maior a confiabilidade e a segurança dos dados e da informação. Se todos os nós forem extintos, os dados se perdem, porém, essa possibilidade é reduzida para cada nó adicionado à rede *blockchain*.

Os passos seguintes a esta pesquisa podem considerar a avaliação de desempenho do *blockchain* quando muitos nós (servidores) estão presentes na rede. Há indícios de que na possibilidade de ocorrência de baixa performance da rede em relação à propagação dos blocos pelos nós, poder-se-ia inviabilizar o uso da DLT como mecanismo de confiança distribuída para documentos arquivísticos. No entanto, a constante evolução da tecnologia faz com que surjam a cada ano equipamentos mais velozes.

Conforme a metodologia utilizada, buscou-se a prospecção de novas perspectivas e novas questões sobre a aplicabilidade da DLT à cadeia de custódia de documentos arquivísticos digitais. De fato, esta pesquisa confirmou tal hipótese e evidenciou vários possíveis caminhos a serem seguidos, uma vez que muitos outros questionamentos surgiram a partir das respostas dos questionários. A definição de um modelo de arquitetura da informação pode abarcar todas estas questões, consolidando em um único ambiente informacional os benefícios da aplicação da DLT em relação à melhoria dos aspectos de segurança, integridade e autenticidade dos documentos arquivísticos digitais.

Mesmo com a adoção de inovação tecnológica, é necessário que cada instituição ou empresa institua primeiramente uma política ou programa de gestão arquivística de documentos. Sem isso, pode-se consumir muito tempo e recursos com resultados insuficientes frente ao investimento. No entanto, qualquer auxílio tecnológico que puder ser utilizado para atingir o máximo dos

requisitos de segurança, integridade e autenticidade deve ser bem aproveitado.

Referências

Albuquerque, Alfram R. R. de; Lima-Marques, Mamede (2011). Sobre os fundamentos da Arquitetura da Informação. // Perspectivas em Gestão & Conhecimento. 2236-417X. 1 (2011) 60-72.

Almeida, Maurício B.; Cendón, Beatriz V.; Souza, Renato R (2012). Metodologia para implantação de programas de preservação de documentos digitais a longo prazo. // Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação. ISSN 1518-2924. 17:34 (2012) 103-130.

Arellano, Miguel A (2004). Preservação de documentos digitais. Artigo. // Ciência da Informação. ISSN 1518-8353. 33:2 (2004) 15-27.

Artefactual (2019). Artefactual Systems Inc. Archivematica. // https://www.archivematica.org/en/ (2018-06-02).

Artefactual (2015). Artefactual Systems Inc. atom. // https://www.archivematica.org/en/ (2019-06-02).

Bauer, Martin W.; Gaskell, George (2003). Pesquisa qualitativa com texto, imagem e som: Um manual prático // Guareschi, Pedrinho A. (tradutor) (2003). Petrópolis, RJ: Vozes, 2003. ISBN 8532627277. 26-26.

Belloto, Heloísa L (2002). Como fazer análise diplomática e análise tipológica de documento de arquivo. // Arquivo do Estado e Imprensa Oficial do Estado. São Paulo, 2002. ISBN 85-7060-133-6. 23-23. http://www.arqsp.org.br/arquivos/oficinas_colecao_como_fazer/cf8.pdf (2019-04-24).

Berners-Lee, Tim (1990). Information Management: A Proposal. // CERN (1990). https://www.w3.org/History/1989/proposal-msw.html (2019-04-24).

Brasil (s. f.). Ministério da Economia. sei! Sistema de Informação Eletrônica. // http://www.fazenda.gov.br/sei (2019-06-02).

Bryman, Alan (2012). Social research methods. // 4a. edição. Oxford: Oxford University Press, 2012. 399-399.

Buschman, John (2019). Good news, bad news, and fake news: Going beyond political literacy to democracy and libraries. // Journal of Documentation. ISSN 0022-0418. 75:1 (2019). https://www.emeraldinsight.com/doi/abs/10.1108/JD-05-2018-0074 (2019-04-18).

Carter, J. Lawrence; Wegman, Mark N (1979). Universal classes of hash functions. // Journal of computer and system sciences. 18:2 (1979) 143-154.

CONARQ – Conselho Nacional de Arquivos (Brasil) - Câmara Técnica de documentos eletrônicos (2004). Carta para a Preservação do Patrimônio Arquivístico Digital. // http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf (2019-04-23).

CONARQ – Conselho Nacional de Arquivos (Brasil) - Câmara Técnica de documentos eletrônicos (2011). e-ARQ Brasil – Modelo de Requisito para Sistemas Informatizados de Gestão Arquivística de Documentos. Versão 1.1. // http://www.siga.arquivonacional.gov.br/images/publicacoes/e-arq.pdf (2018-06-30).

CONARQ – Conselho Nacional de Arquivos (Brasil) - Câmara Técnica de documentos eletrônicos (2015). Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis – RDC-Arq. // http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf (2018-05-18).

CONARQ – Conselho Nacional de Arquivos (Brasil) - Câmara Técnica de documentos eletrônicos (2016). Glossário – Documentos Arquivísticos Digitais. 7ª versão. // http://www.conarq.gov.br/images/ctde/Glossario/2014ctdeglossario_v6_public.pdf (2018-08-15).

Cordeiro, Alexander M.; Oliveira, Glória M. de; Rentería, Juan M.; Guimarães, Carlos A (2007). Revisão sistemática: uma revisão narrativa. // Revista do Colégio Brasileiro de Cirurgiões. ISSN 1809-4546. 34:6 (2007).

DARPA - Defense Advanced Research Projects Agency (EUA) (__). About DARPA. // https://www.darpa.mil/about-us/about-darpa (2019-04-27).

Dempsey, Kathy (2017). What's behind fake news and what you can do about it. // Information Today. ISSN 8755-6286. 34:4 (2017) 6-6. http://link.galegroup.com/apps/doc/A490692851/AONE?u=capes&sid=AONE&xid=33f711d1 (2019-04-18).

Dillon, Andrew; Turnbull, Don (2003). Information Architecture. // Encyclopedia of Library and Information Science. New York, NY: Marcel Dekker, 2003.

Duranti, Luciana (2010). Concepts and principles for the management of electronic, records, or records management theory is archival diplomatics. // Records Management Journal. ISSN 0956-5698. 20:1 (2010) 78-95.

Flores, Daniel; Rocco, Brenda C. de B.; Santos, Henrique M (2016). Cadeia de custódia para documentos arquivísticos digitais. // Acervo – Revista do Arquivo Nacional. ISSN 2237-8723. 29:2 (jul./dez. 2016) 117-132. http://revista.arquivonacional.gov.br/index.php/revistaacervo/article/view/717/732 (2018-07-18).

Gibbs, Graham (2009). Análise de dados qualitativos. // Artmed Editora. São Paulo, 2009.

ISO – International Organization for Standartization (2012). ISO 14721:2012 (CCSDS 650.0-M-2) Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model. // Switzerland, 2012. https://www.iso.org/standard/57284.html (2019-04-30).

Ismail, Aliza; Jamaludin, Adnan (2009). Towards establishing a framework for managing trusted records in the electronic environment. // Records Management Journal. ISSN 0956-5698. 19:2 (2009) 135-146. https://doi.org/10.1108/09565690910972084 (2019-04-25).

Jenkinson, Hilary (1922). A manual of archive administration: including the problems of war archives and archive making. // Oxford: The Clarendon Press, 1922.

Kroth, Marcelo L.; Flores, Daniel (2018). Autenticidade de documentos arquivísticos digitais: análise de um processo de afastamento. // Biblios. ISSN 1562-4730. 72 (2018). http://www.scielo.org.pe/pdf/biblios/n72/a05n72.pdf (2019-04-25).

Lemieux, Victoria L (2016). Trusting records: is Blockchain technology the answer? // Records Managment Journal. ISSN 0956-5698. 26:2 (2016) 110-139. https://doi.org/10.1108/RMJ-12-2015-0042 (2018-06/28).

Lemieux, Victoria L (2017). Blockchain recordkeeping: a SWOT analysis. // Information Management Magazine. ISSN 1535-2897. 51:6 (2017) 20-27. http://www.bluetoad.com/publication/?i=454085&ver=html5&p=22#{%22page%22:%2222%22,%22issue_id%22:454085} (2018-09-01).

Lemieux, Victoria L (2017b). A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation. // IEEE International Conference on Big Data (BIGDATA), 2017.

Lemieux, Victoria L.; Flores, Daniel; Lacombe, Claudia (2018). Registro de transações imobiliárias em

Blockchain no Brasil (RCPLAC-01) - Estudo de Caso 1. // http://www.doi.org/10.13140/RG.2.2.16022.45123 (2018-09-02)>. Acessado em: 02 set. 2018.

Ministério do Planejamento, Desenvolvimento e Gestão (2018). Adesão ao Processo Eletrônico Nacional. // http://www.planejamento.gov.br/pensei/adesao-ao-processo-eletronico-nacional-pen (2018-10-11).

Nakamoto, Satoshi (2008). Bitcon: A Peer-to-Peer Electronic Cash System. // https://bitcoin.org/bitcoin.pdf (2018-07-17).

RLG – Research Libraries Group; OCLC – Online Computer Library Center (2002). Trusted Digital Repositories: Attributes and Responsibilities. An RLG-OCLC Report. // Mountain View, California, EUA, 2002. https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf (2018-07-17).

Rogers, Corinne (2015). Authenticity of Digital Records: A Survey of Professional Practice. // Canadian Journal of Information and Library Science. ISSN 1195-096X. 39:2 (2015) 97-113. https://muse.jhu.edu/article/590936 (2019-04-25).

Rosenfield, Louis; Morville, Peter; Arango, Jorge (2015). Information Architecture for the web and beyond. // 4a. edição. O'Reilly Media: Estados Unidos, California, 2015.

Rossum, Joris Van (2017). Blockchain for Research Perspectives on a New Paradigm for Scholarly Communication. // Digital Science Report (2017). https://www.digital-science.com/resources/digital-research-reports/blockchain-for-research/ (2018-07-17).

Santos, Henrique M. dos; FLORES, Daniel (2017). Preservação de documentos digitais: reflexões sobre as estratégias de refrescamento. // Revista Brasileira de Biblioteconomia e Documentação – RBBD. ISSN 1980-6949. 13:2 (jul./dez. 2017). https://rbbd.febab.org.br/rbbd/article/view/449 (2018-08-15).

Santos, Henrique M. dos; Flores, Daniel (2015). As vulnerabilidades dos documentos digitais: Obsolescência tecnológica e ausência de políticas e práticas de preservação digital. // Biblios. ISSN 1562-4730. 59 (2015).

Saracevic, Tefko (1995). Interdisciplinary nature of information science. // Ciência da Informação. e-ISSN 1518-8353. 24:1 (1995).

Seadle, Michael (2012). Archiving in the networked world: authenticity and integrity. // Library Hi Tech. ISSN 0737-8831. 30:3 (2012) 545-552. https://doi.org/10.1108/07378831211266654 (2019-04-25).

Stapleton, Richard (1983). Jenkinson and Schellenberg: A Comparison. // Archivaria. 17 (1983). https://archivaria.ca/index.php/archivaria/article/download/11021/11956 (2019-11-04).

Enviado: 2019-05-22. Segunda versión: 2020-05-06.
Aceptado: 2020-06-08.