RBPD Revista Brasileira de Preservação Digital
RBPD Brazilian Journal of Digital Preservation

Artigo Original

DOI: 10.20396/rebpred.v4i00.17355

RESEARCH DATA REPOSITORY

COMPARATION OF INTERNATIONAL RELIABILITY ASSESSMENT CRITERIA/REQUIREMENTS

Daiane Barrili dos Santos

Universidade Federal do Rio Grande do Sul
E-mail: dai.b.santos@hotmail.com
Porto Alegre – RS – Brasil

Samile Andrea de Souza Vanz

Universidade Federal do Rio Grande do Sul
E-mail: samilevanz@terra.com.br
Porto Alegre – RS – Brasil

Resumo

Introdução: O conhecimento acerca dos princípios e requisitos para dados e repositórios confiáveis, bem como de critérios para avaliação, pode auxiliar as instituições no planejamento e criação de repositórios confiáveis. Objetivo: A pesquisa visou comparar os principais critérios, requisitos e princípios de avaliação da confiabilidade de dados e repositórios de dados de pesquisa. Metodologia: Foram comparados o *CoreTrustSeal - Trustworthy Data Repositories Requirements* 2020–2022; o *Audit and Certification of Trustworthy Digital Repositories*; os FAIR Principles; e *The TRUST Principles for digital repositories*. Resultados: Apesar da dificuldade de realizar o trabalho de correspondência de quatro documentos de naturezas distintas, é possível estabelecer requisitos semelhantes entre eles. Conclusão: Conclui-se que os critérios, requisitos e princípios selecionados neste estudo apresentam as características almejadas para um repositório de dados confiável. A discussão destes critérios, requisitos e princípios é pertinente ao contexto brasileiro dada a incipiência dos repositórios de dados de pesquisa brasileiros.

Palavras-chave: Repositórios de dados de pesquisa. Avaliação de repositórios de dados de pesquisa. Critérios/Requisitos.

Abstract

Introduction: The knowledge about the principles and requirements for reliable data and repositories, as well as the criteria for evaluation, can support institutions in the planning and creation of trustworthy repositories. Objective: The research aimed to compare the main criteria, requirements and principles for evaluating the trustworthy of data and research data repositories. Methodology: Four documents were compared: CoreTrustSeal - Trustworthy Data Repositories Requirements 2020–2022; the Audit and Certification of Trustworthy Digital Repositories; the FAIR Principles; and The TRUST Principles for digital repositories. Results: Despite the difficulty of carrying out the correspondence work of four documents of different nature, it is possible to establish similar requirements between them. Conclusion: It concludes that the criteria, requirements and principles selected in this study present the desired characteristics for a reliable data repository. The discussion of these criteria, requirements and principles is pertinent to the Brazilian context given the incipience of Brazilian research data repositories.

Keywords: Research data repositories. Evaluation of research data repositories. Criteria/Requirements

PUBLISHERS
Universidade Estadual de Campinas – Sistema de Bibliotecas / Instituto Brasileiro de Informação em Ciência e Tecnologia – Rede Brasileira de Serviços de Preservação Digital – Cariniana. As ideias expressadas neste artigo são de responsabilidade de seus autores, não representando, necessariamente, a opinião dos editores ou da universidade.

EDITORES
Gildenir Carolino Santos, Miguel Angel Márdero Arellano.

CRediT

- Reconhecimentos: Não aplicável.
- Financiamento: Conselho Nacional de Desenvolvimento Científico e Tecnológico(CNPq), Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), Fundação de Apoio a Pesquisa no Estado do Rio Grande do Sul (FAPERGS).
- Conflitos de interesse: Os autores certificam que não têm interesse comercial ou associativo que represente um conflito de interesses em relação ao manuscrito.
- Aprovação ética: Não aplicável.
- Disponibilidade de dados e material: Não aplicável.
- Contribuições dos autores: Conceituação, Curadoria de Dados, Análise Formal, Aquisição de Financiamento, Investigação, Metodologia, Administração de Projetos, Recursos, Software, Supervisão, Validação, Visualização, Redação – rascunho original: SANTOS, D.B.; VANZ, S.; Redação – revisão & edição: VANZ, S.

Submetido em: 30/09/2022 – Aceito em: 02/02/2023 – Publicado em: 04/03/2023

1 Introdução

O desenvolvimento das tecnologias de informação e comunicação impulsionou a colaboração científica entre pesquisadores no final do século XX (VANZ; STUMPF, 2010). Mais recentemente, o movimento da Ciência Aberta acrescentou outros elementos que tornaram a ciência ainda mais colaborativa (ALBAGLI; CLINIO; RAYCHTOCK, 2014). Um dos pilares da Ciência Aberta, os dados abertos de pesquisa também adicionaram transparência, agilizaram o processo de pesquisa e reduziram custos.

O tema dados abertos de pesquisa vêm sendo estudado desde 2004, quando os ministros de Ciência e Tecnologia dos países membros da *Organization for Economic Co-operation and Development* (OECD) se reuniram em Paris, para discutir a necessidade de um guia internacional voltado para o acesso aos dados de pesquisa (HENNING *et al*., 2019). Tendo em vista o reconhecimento dos benefícios advindos do compartilhamento de dados, instituições governamentais passaram a estimular essa prática. A maior parte dessas iniciativas são conduzidas por órgãos de fomento à atividade científica, que solicitam de seus beneficiários adequações que vão desde o requerimento de um plano de gestão de dados associado ao projeto de pesquisa, até a definição do repositório no qual os dados serão depositados (RAUEN, 2018).

De modo a atender às exigências impostas, os pesquisadores necessitam repositórios para depósito de seus dados de pesquisa. Nesse contexto, as bibliotecas universitárias, os centros de pesquisa e as associações científicas que atuam no apoio ao pesquisador começaram a avaliar e qualificar os repositórios confiáveis (CURTY, 2018). Entre as características que creditam confiabilidade ao repositório estão recursos de descoberta e acesso, serviços de suporte ao usuário, sustentabilidade e reputação, definição de disciplinas e comunidades atendidas, políticas de dados, custos de depósito e preservação (DOWNS, 2021).

Organizações internacionais como, por exemplo, a *Research Data Alliance* (RDA) e a *The Future of Research Communications and e-Scholarship* (FORCE11) estão se empenhando para a consolidação de políticas globais que estimulem as melhores práticas de compartilhamento e reuso dos dados de pesquisa. No Brasil, organizações como o Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) e a Rede Nacional de Pesquisa (RNP) têm contribuído para a identificação de práticas, mapeamento de requisitos e prototipação de repositórios.

Considerados o alicerce do conhecimento científico e tecnológico, dados de pesquisa não são fáceis de estruturar, organizar, descrever e disponibilizar, para que sejam compreensíveis agora e no futuro (DUDZIAK, 2016). Wilkinson *et al.* (2016) argumentam que além da coleta, registro e arquivamento adequados, a gestão de dados inclui o 'cuidado a longo prazo', possibilitando que eles sejam descobertos e reutilizados para investigações posteriores, isoladamente ou em combinação com dados gerados.

A partir das reflexões referentes às infraestruturas específicas, e para que haja o compartilhamento, uso e reuso dos dados de pesquisa, Medeiros (2015), evidencia que é necessário que os dados sejam compartilhados em repositórios próprios para este fim, buscando o máximo de alcance possível no seu reuso. O desenvolvimento de uma infraestrutura e manutenção de repositórios de dados de pesquisa apresenta-se como um desafio tanto em termos de gestão quanto da representação e disponibilização dos conjuntos de dados que estão contidos nesses sistemas. Os repositórios precisam operar em infraestruturas confiáveis e estáveis que maximizam os serviços, devem ganhar a confiança das comunidades que pretendem servir e demonstrar que são confiáveis e capazes de gerenciar adequadamente os dados que custodiam (LIN, 2020).

A confiabilidade deve ser avaliada desde a construção dos repositórios digitais, a fim de garantir que os materiais armazenados permanecerão autênticos em longo prazo (MÁRDERO ARELLANO, 2008). Um repositório confiável aceita a responsabilidade pela manutenção dos recursos digitais, projeta seus sistemas de acordo com as convenções e os padrões comumente aceitos, estabelece metodologias para avaliação de sistemas que atendem às expectativas de confiabilidade da comunidade, cumpre suas responsabilidades com depositantes e usuários de forma aberta e explícita, e permite que sejam auditadas e medidas suas políticas, práticas e desempenho (JANTZ; GIARLO, 2006). Um repositório digital confiável é aquele cuja missão é fornecer acesso confiável, por longo prazo, a recursos digitais administrados à sua comunidade-alvo, agora e no futuro (RLG/OCLC WORKING GROUP ON DIGITAL ARCHIVE ATTRIBUTES, 2002).

Para manter o status de confiança, o repositório pode realizar autoavaliações e um ciclo regular de auditoria e/ou certificação permitindo que sejam auditadas e medidas suas políticas, práticas e desempenho. A avaliação de repositórios é uma etapa fundamental na construção e no desenvolvimento dos mesmos, pois permite quantificar a eficiência do sistema de modo que ele acompanhe o dinamismo dos objetos digitais e dos usuários (LAMEIRA, 2016). O processo de avaliação também é importante para verificar se os dados atendem a todos os critérios de seleção e para assegurar um manejo adequado para sua preservação. É a avaliação que garante que os dados permanecem relevantes e compreensíveis para a comunidade designada.

A sustentabilidade dos repositórios levanta uma série de questões desafiadoras em diferentes setores: organizacional, técnica, financeira e jurídica. A avaliação dos repositórios pode ser uma contribuição importante para garantir a confiabilidade e a durabilidade dos repositórios de dados. Ao passar por uma avaliação, os repositórios podem demonstrar para seus usuários e financiadores que uma autoridade os avaliou e endossou sua confiabilidade (CORETRUSTSEAL, 2020). Neste contexto, avaliar o desenvolvimento dos repositórios é de suma importância, pois possibilita a evolução de novas práticas e maior domínio sobre este novo campo de atuação. A realização de avaliações permite identificar os pontos fortes e fracos, trazendo mais confiabilidade ao repositório, como também ajudam as comunidades de dados - produtores, repositórios e consumidores - a melhorar a qualidade e a transparência

de seus processos e a aumentar a conscientização e a conformidade com os padrões estabelecidos (CORETRUSTSEAL, 2020).

No Brasil, diversas instituições encontram-se em fase de planejamento ou implantação de repositórios de dados de pesquisa. Desta forma, é necessário ampliar os estudos referentes aos critérios, requisitos e princípios de confiabilidade para repositórios de dados de pesquisa. Neste sentido, este artigo objetiva comparar e reunir princípios, critérios e requisitos presentes em quatro instrumentos internacionais, a saber: *CoreTrustSeal - Trustworthy Data Repositories Requirements 2020–2022; o ACTDR - Audit and Certification of Trustworthy Digital Repositories; os FAIR Principles; e The TRUST Principles for digital repositories*. A escolha destes instrumentos fundamentou-se na ideia de reunir princípios importantes para o dado em si, bem como requisitos de confiabilidade referentes ao repositório, em uma tentativa de sintetizar algumas recomendações aos gestores de repositórios. Percebe-se a natureza distinta dos quatro instrumentos, no entanto, considerou-se relevante reunir recomendações advindas de várias fontes, a fim de subsidiar um processo de aprendizado e amadurecimento da comunidade brasileira.

O *CoreTrustSeal* reúne 16 requisitos e divide-se em seções contemplando uma parte introdutória, algumas orientações gerais e, posteriormente, os requisitos com suas respectivas subdivisões. Cada um dos requisitos descritos no instrumento é acompanhado por um texto de orientação que descreve as informações que os candidatos à certificação devem fornecer para permitir uma revisão objetiva. O instrumento solicita o nível de conformidade para cada um dos requisitos. A mais recente edição (2023-2025) ainda não existia no momento da coleta de dados deste estudo, por esse motivo utilizou-se a edição disponível à época (2020-2022).

O ACTDR possui como propósito definir a Prática Recomendada CCSDS com base no processo de auditoria e certificação para avaliar a confiabilidade de repositórios digitais. Destina-se principalmente aos responsáveis pela auditoria de repositórios digitais e para aqueles que trabalham ou são responsáveis por repositórios e almejam medir a confiabilidade. Este documento possui 13 requisitos e está dividido em seções informativas, normativas e anexos que fornecem uma visão da justificativa, algumas questões importantes de design e uma introdução à terminologia e conceitos. Essas seções fornecem métricas agrupadas da seguinte forma: infraestrutura organizacional; gerenciamento de objetos digitais; infraestrutura e gerenciamento de riscos de segurança. Cada seção agrupa métricas em uma ou mais subseções.

Os Princípios TRUST caracterizam-se por ser um conjunto de cinco princípios orientadores para demonstrar a confiabilidade de um repositório digital: *Transparency, Responsibility, User Focus, Sustainability and Technology*. Esses princípios fornecem uma estrutura comum para facilitar a discussão e implementação das melhores práticas em preservação digital.

Os princípios FAIR têm como objetivo enfatizar a ação da máquina, ou seja, a capacidade dos sistemas computacionais de encontrar, acessar, interoperar e reutilizar dados com nenhuma ou mínima intervenção humana e referem-se a três tipos de entidades: dados (ou qualquer objeto digital); metadados (informações sobre

aquele objeto digital); e infraestrutura. É constituído por quatro princípios: *Findable* (localizável); *Accessible* (Acessível); *Interoperable* (Interoperável); e *Reusable* (Reutilizável). Diferentemente dos demais documentos, os Princípios FAIR atuam na perspectiva da localização, acesso, interoperabilidade e reuso de dados. Assim, nos Princípios FAIR não há qualquer requisito diretamente atrelado à confiabilidade, muito embora haja outras características extremamente relevantes no processo de gestão de dados de pesquisa e, por isso, entende-se que os Princípios FAIR auxiliam na confiabilidade.

Entende-se que as avaliações realizadas tanto em repositórios de dados de pesquisa em funcionamento quanto em processo de implementação, podem auxiliar no desenvolvimento de melhores práticas, proporcionando qualidade a estes repositórios. Algumas decisões tomadas na etapa de planejamento são cruciais para implementação e acompanhamento desse tipo de sistema de informação, especialmente no que diz respeito a certificação futura destes repositórios. Neste sentido, pretende-se que a comparação e síntese apresentada neste trabalho possam auxiliar gestores de repositórios de dados brasileiros. As seções a seguir apresentam os materiais e métodos utilizados, resultados da análise e considerações finais.

2 MATERIAIS E MÉTODOS

Esta pesquisa constitui-se num levantamento documental cujo objeto de estudo são os critérios, requisitos e princípios de confiabilidade para repositórios de dados de pesquisa. O universo para a aplicação da técnica de pesquisa se restringiu aos documentos disponíveis na web, em fontes de informação confiáveis como sites de organizações e instituições internacionais. A seleção do *CoreTrustSeal Trustworthy Data Repositories Requirements 2020–2022*[1]*; ACTDR - Audit and Certification of Trustworthy Digital Repositories*[2]*; Principles FAIR*[3]*;* e *The TRUST Principles for digital repositories*[4] guiou-se pelas seguintes características: referem-se ao principal assunto da pesquisa; possuem um reconhecimento internacional e as metodologias a eles aplicadas foram tratadas com aprofundamento podendo ser relacionadas a avaliação de confiabilidade de repositórios de dados de pesquisa.

O modelo de análise deste estudo partiu da averiguação manual dos instrumentos internacionais e posterior comparação dos itens que compõem cada um dos documentos. Foram realizadas as análises para a identificação de critérios semelhantes, que foram organizados por infraestruturas/áreas, conforme a ordem dos requisitos do *CoreTrustSeal.* A próxima seção apresenta o resultado da análise.

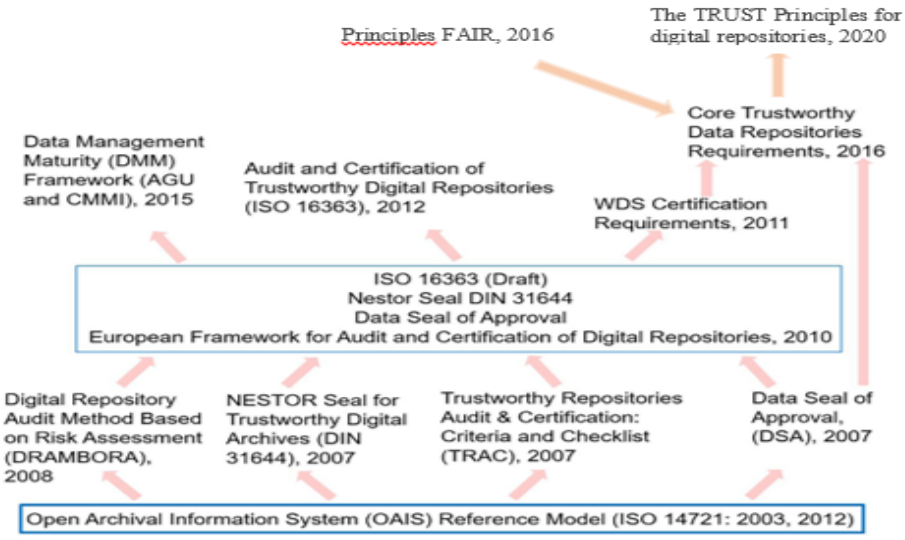
[1]https://www.coretrustseal.org/why-certification/requirements/
[2]https://public.ccsds.org/review/CCSDS%20652.0-P-1.1/652x0p11.pdf
[3]https://www.go-fair.org/fair-principles/
[4]https://www.nature.com/articles/s41597-020-0486-7.pdf

3 RESULTADOS E DISCUSSÃO

Esta seção apresenta a comparação dos instrumentos selecionados. Os princípios FAIR, já mencionados, destacam a necessidade de adotar boas práticas definindo características essenciais de objetos de dados para garantir que sejam reutilizáveis por humanos e máquinas. Para sustentar a implantação dos princípios FAIR, é necessário definir os elementos centrais dos objetos de dados envolvidos e, a partir dessa definição, desenvolver um ecossistema que inclua os serviços necessários para criar, gerir e partilhar os objetos de maneira FAIR (HODSON *et al*., 2018).

Percebe-se que os requisitos do *CoreTrustSeal* possuem uma terminologia baseada no modelo OAIS e os princípios FAIR estão implícitos nos requisitos. O *CoreTrustSeal* também serve para garantir que os repositórios atinjam as propriedades dos Princípios TRUST, os quais constituem outro conjunto de orientações que objetivam assegurar confiabilidade aos repositórios de dados digitais. Baseada nessas relações apresenta-se a seguir uma adaptação da publicação de Downs (2019) onde foram inseridos entre os instrumentos, os princípios FAIR e TRUST.

Figura 1. Esquema relacional dos instrumentos de avaliação e confiabilidade de repositórios



Fonte: Adaptado de Downs (2019).

Foram realizadas as análises para a identificação de critérios semelhantes e resolveu-se organizá-los por infraestruturas/áreas, conforme a ordem dos requisitos do *CoreTrustSeal*. Os dados mostraram similaridades entre alguns requisitos.

O primeiro requisito do *CoreTrustSeal* abrange a missão e o escopo. Nota-se que o instrumento ACTDR também possui essa subdivisão e, dentro da infraestrutura organizacional, trata sobre a governança e a viabilidade organizacional. Ambos abordam a declaração da missão como requisito e garantia da preservação. Da mesma forma, os princípios TRUST apresentam em seu primeiro requisito, '*transparency*', a mesma abordagem. Estes requisitos relatam que o repositório é

responsável pela administração dos objetos digitais e por garantir que os materiais sejam mantidos no ambiente apropriado por períodos específicos. Em conformidade com este princípio, os repositórios devem garantir que, no mínimo, a declaração de missão e o escopo do repositório sejam claramente indicados.

O segundo requisito do *CoreTrustSeal* refere-se às 'licenças', equivalente ao requisito 'contratos, licenças e responsabilidades' do instrumento ACTDR. Ambos os requisitos assemelham-se ao requisito '*Responsibility*' dos princípios TRUST. O Princípio FAIR R1.1 também possui relação com estes requisitos. Este requisito refere-se aos regulamentos de acesso e licenças aplicáveis estabelecidas pelo próprio repositório de dados, bem como quaisquer códigos de conduta que são geralmente aceitos no setor relevante para o intercâmbio e uso adequado de conhecimento e informação. Este requisito é importante para garantir que o repositório tenha os direitos e autorizações necessários para permitir que ele colete e preserve conteúdo digital ao longo do tempo, faça com que essas informações estejam disponíveis para sua comunidade designada, e para defender esses direitos quando questionados.

De acordo Tartarotti, Dal'Evedove e Fujita (2019), o gerenciamento de acesso é uma questão de grande importância. Ele contempla as decisões a serem tomadas pelo bibliotecário quanto aos tipos de acesso em um repositório de dados de pesquisa, ou seja, pode ter o acesso aberto. Neste caso, qualquer usuário com acesso à Internet pode acessar os dados de pesquisa, que podem ter termos de uso específicos ou indicar o uso apropriado ou impróprio por meio de uma licença padrão, por exemplo, a *Creative Commons*. Normalmente, é fornecido acesso anônimo aos dados, mas em alguns casos, um nome e endereço de e-mail podem ser solicitados antes que o acesso seja concedido. O acesso pode ser gerenciado a partir de regras aplicadas ao uso dos dados. Por exemplo, os usuários podem não apenas precisar se registrar, mas também serem aprovados antes que o acesso seja concedido. A aprovação pode depender do status do usuário, por exemplo, membro de instituição acadêmica, ou de suas respostas a determinadas perguntas, por exemplo, sobre seu objetivo da pesquisa; ou de acesso seguro. Os dados são liberados somente por meio de mecanismos seguros. Isso pode envolver o acesso a um servidor remoto para executar análises, em vez de baixar dados diretamente; ter a saída verificada pela equipe do repositório de dados de pesquisa para garantir a não divulgação.

O terceiro requisito do *CoreTrustSeal*, 'continuidade de acesso', se assemelha ao requisito do ACTDR 'governança e a viabilidade organizacional' destacando que o repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório terá no suporte de longo prazo. Os princípios TRUST tratam sobre esta questão por meio do princípio '*Sustainability*'. O requisito do *CoreTrustSeal* cobre a governança relacionada à operação contínua do repositório ao longo do tempo e durante desastres, bem como evidências em relação ao planejamento de sucessão, e as medidas em vigor para garantir o acesso e a disponibilidade dos acervos de dados, atualmente e no futuro.

O quarto requisito do *CoreTrustSeal*, 'Confidencialidade/Ética', menciona que o repositório deve garantir, na medida do possível, que os dados sejam criados, com curadoria, acessados e usados em conformidade com as normas disciplinares e

éticas. Da mesma forma, o requisito 'sustentabilidade financeira" do ACTDR, trata em parte do assunto confidencialidade. Os princípios TRUST, no item '*Responsibility*' aborda as informações confidenciais. O *CoreTrustSeal* relata que este requisito se refere às disposições éticas e de privacidade que afetam a criação, curadoria e uso dos dados. Contudo, o ACTDR menciona que é necessário se proteger contra má conduta ou outra atividade desagradável que possa ameaçar a viabilidade econômica do repositório. O repositório não pode apenas reivindicar transparência, mas deve mostrar que ajusta seus negócios para mantê-los transparentes, compatíveis e auditáveis. Os princípios TRUST mencionam que a responsabilidade é demonstrada com o gerenciamento dos direitos de propriedade intelectual dos produtores de dados, proteção de recursos de informações confidenciais, e a segurança do sistema e seu conteúdo.

O quinto requisito do *CoreTrustSeal,* 'Infraestrutura organizacional', menciona que o repositório deve ter financiamento adequado e número suficiente de funcionários qualificados gerenciados por meio de um sistema claro de governança. O ACTDR possui um requisito semelhante, 'estrutura organizacional e pessoal', e relata que o repositório deve ter identificado e estabelecido as funções de que necessita para executar e deve nomear equipe com habilidades e experiência adequadas para cumprir essas funções. Os princípios TRUST relatam que um repositório depende da interação das pessoas, processos e tecnologias para oferecer suporte seguro, persistente e serviços confiáveis.

Cabe ressaltar que a infraestrutura organizacional também é mencionada pelo Modelo OAIS, haja vista que afeta o desempenho, a prestação de contas e a sustentabilidade do repositório. Infraestrutura abrange elementos de governança; estrutura organizacional; mandato ou finalidade; escopo; papéis e responsabilidades; estrutura de políticas; sistema de financiamento; questões financeiras, incluindo ativos; contratos, licenças e passivos, e transparência (RLG/NARA, 2007).

O sexto requisito do *CoreTrustSeal*, 'Orientação de especialista' assemelha-se a um dos requisitos do ACTDR, 'contratos, licenças e responsabilidades'. Segundo o *CoreTrustSeal,* um repositório eficaz se esforça para realizar evoluções e adotar novas tecnologias mais eficazes a fim de permanecer valioso para sua comunidade designada. Da mesma forma, o ACTDR orienta que as Políticas de Preservação e Planos de Implementação de Preservação do repositório e mecanismos devem ser examinados por autoridades institucionais apropriadas e/ou especialistas jurídicos para garantir que as respostas aos desafios cumpram as leis e requisitos relevantes. Os princípios TRUST não mencionam este requisito.

O sétimo requisito do *CoreTrustSeal* corresponde a 'Integridade e autenticidade dos dados'. O ACTDR possui requisitos análogos: responsabilidade processual e política de preservação. Nos requisito 'preservação de AIP' e 'gestão de informações' também há especificações referentes a integridade. Na subdivisão: 'Gestão de risco de infraestrutura e segurança', requisito 'gestão de risco de infraestrutura técnica' do ACTDR, informa que o repositório deve identificar e gerenciar os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema como também, gerenciar o número e localização de cópias de todos os objetos digitais. O

Princípio FAIR R1.2 possui relação com estes requisitos. Nos princípios TRUST não foram encontrados requisitos relacionados a integridade e autenticidade.

O oitavo requisito do *CoreTrustSeal*, 'Avaliação', orienta o repositório a aceitar dados e metadados com base em critérios definidos para garantir relevância e compreensibilidade para os usuários de dados. O ACTDR possui alguns requisitos relacionados à avaliação: 'O repositório deve se comprometer com um cronograma regular de autoavaliação e certificação externa'; 'O repositório deve fornecer evidências da eficácia de sua preservação'; 'O repositório deve manter uma análise sistemática dos fatores de risco de segurança associados a dados, sistemas, pessoal e planta física'; 'O repositório deve ter uma Política de Coleta ou outro documento que especifique o tipo de informação que irá preservar, reter, gerenciar e fornecer acesso. Percebe-se que nos Princípios TRUST não há abordagem deste requisito. De acordo com o *CoreTrustSeal*, a função da avaliação é fundamental para avaliar se os dados atendem a todos os critérios de seleção e para garantir o manejo adequado para a sua preservação. A avaliação e a reavaliação ao longo do tempo garantem que os dados permaneçam relevantes e compreensíveis para a comunidade designada. Contudo, o ACTDR menciona que o repositório deve ser capaz de demonstrar a preservação contínua, incluindo compreensibilidade de suas participações. Isso pode ser avaliado em vários graus e depende da especificidade da comunidade designada.

O nono requisito do *CoreTrustSeal* trata sobre 'Procedimentos de armazenamento documentados', ou seja, em que medida o repositório aplica processos e procedimentos documentados durante o gerenciamento do armazenamento de arquivos de dados. O instrumento ACTDR possui requisito semelhante: 'o repositório deve ter processos documentados para aquisição de *Preservation Description Information* (PDI)'. Os princípios TRUST não abordam este requisito. De acordo com o *CoreTrustSeal*, os repositórios precisam armazenar dados e metadados desde o ponto de depósito até o ponto de acesso. O ACTDR orienta que o repositório deve executar seus processos documentados para aquisição de PDI como também deve garantir que o PDI esteja persistentemente associado às informações de conteúdo relevantes.

O décimo requisito do *CoreTrustSeal,* 'Plano de preservação', pontua que o repositório assume a responsabilidade pela preservação a longo prazo e gerencia essa função de forma planejada e documentada. O ACTDR possui entre seus requisitos, o seguinte critério: o repositório deve ter estratégias de preservação documentadas relevantes. O Princípio FAIR A2 trata sobre estratégias de preservação e possui relação com estes requisitos. De acordo com o *CoreTrustSeal,* o repositório, os depositantes de dados e a comunidade designada precisam entender o nível de responsabilidade assumido para cada arquivo depositado. O ACTDR menciona a necessidade do repositório registrar como planeja garantir que a informação permanecerá disponível e utilizável para as gerações futuras e fornecer um meio de verificar e validar o trabalho de preservação do repositório. O Princípio FAIR A2 menciona que quando necessário, dependendo das restrições ao acesso aos dados e/ou metadados, um mecanismo para autenticação e autorização para o acesso deve ser permitido pelo protocolo de comunicação.

Sayão e Sales (2018) reiteram a ideia de que um repositório confiável deve dispor de uma política explicita de preservação digital, que considere parâmetros arquivísticos tais como proveniência e autenticidade dos dados que não podem ser regerados e estejam conectadas à sistemas confiáveis de preservação fundamentados no modelo de referência ISO/OAIS. Os autores afirmam que a preservação digital de longo prazo é um dos principais requisitos para um repositório confiável.

O requisito 11 do *CoreTrustSeal*, 'Qualidade dos dados', refere-se a experiência apropriada para lidar com dados técnicos e qualidade de metadados e a garantia que informações suficientes estejam disponíveis para os usuários finais fazerem avaliações relacionadas à qualidade. O requisito do ACTDR, 'gestão de risco de segurança' orienta a manutenção de uma análise sistemática dos fatores de risco de segurança associado a dados, sistemas, pessoal e planta física descrevendo alguns aspectos relacionados a qualidade. Os princípios TRUST abordam este requisito qualidade no item '*Responsibility*', informando que a responsabilidade é demonstrada aderindo aos padrões de metadados e curadoria, juntamente com o gerenciamento dos acervos de dados, por exemplo, validação técnica, documentação e controle de qualidade. Os Princípios FAIR I3 e R1 estão implícitos neste requisito.

De acordo com o *CoreTrustSeal*, os repositórios devem garantir que haja informações suficientes sobre os dados para que a comunidade designada avalie a sua qualidade. A avaliação da qualidade torna-se cada vez mais relevante quando a comunidade designada é multidisciplinar, onde os usuários podem não ter experiência pessoal para fazer uma avaliação da qualidade apenas a partir dos dados. O ACTDR orienta que um curso interno e avaliação externa deve ser realizada para avaliar a qualidade do serviço e a relevância para o usuário.

O direito de propriedade intelectual também deve ser revisado regularmente, bem como a responsabilidade do repositório para regulamentar a não conformidade. O repositório deve avaliar as habilidades de sua equipe e garantir a aquisição de novos funcionários ou reciclagem do pessoal existente, conforme necessário. A avaliação de risco regular também deve abordar ameaças e ataques de negação de serviço e perda ou qualidade inaceitável de serviços terceirizados. O Princípio FAIR I3 menciona que (Meta)dados devem incluir referências qualificadas para outros (Meta)dados, ou seja, deve-se referenciar os conjuntos de dados devidamente, possibilitando que conjuntos de dados gerados, a partir de outros conjuntos de dados, sejam ligados. O R1 estabelece que os (Meta)dados devem ser descritos com uma pluralidade de atributos precisos e relevantes.

Conforme Aventurier (2017) e Assis (2019), o conjunto de dados deve ser descrito por metadados ricos o suficiente para que, uma vez indexados em um mecanismo de busca, possam ser encontrados mesmo sem o seu identificador único persistente. Tendo em vista que não se pode prever que os dados e seus metadados estejam sempre juntos, a associação entre eles deve ocorrer pela inclusão do identificador persistente dos dados nos metadados. Para que os dados sejam encontrados, seus metadados devem ser indexados em mecanismos de busca

(*search engine*), que possibilitem aos computadores e usuários encontrá-los com facilidade.

O requisito 12 do *CoreTrustSeal* corresponde a 'Fluxos de trabalho', ou seja, o arquivamento deve ocorrer de acordo com fluxos de trabalho definidos, desde o armazenamento até a disseminação. No ACTDR as questões relacionadas a fluxos de trabalho estão presentes em três requisitos: o repositório deve ter 'Políticas de Preservação em vigor para garantir que o seu Plano Estratégico de Preservação seja cumprido'; 'o repositório deve ter um processo de *ingest* que verifica cada *Submission Information Package* (SIP) para integridade e correção'; e 'o repositório deve gerenciar o número e localização de cópias de todos os objetos digitais'. Não foram identificadas questões relacionadas a fluxo de trabalho nos princípios TRUST e FAIR. Segundo o *CoreTrustSeal*, para garantir a consistência das práticas entre conjunto de dados e serviços, os fluxos de trabalho devem ser documentados e definidos de acordo com as atividades do repositório. O ACTDR indica utilizar fluxos de trabalho nos mecanismos para revisão, nas atualizações e desenvolvimento de suas políticas de preservação à medida que o repositório cresce e à medida que a tecnologia e a prática da comunidade evoluem.

O requisito 13 do *CoreTrustSeal*, 'Descoberta e identificação de dados', orienta que o repositório deve permitir que os usuários descubram os dados e os consultem de forma persistente por meio de citações adequadas. O ACTDR possui um requisito semelhante ao *CoreTrustSeal*: 'Gestão de informações', onde o repositório deve especificar os requisitos mínimos de informação para permitir a descoberta e identificação de materiais de interesse. Segundo o *CoreTrustSeal*, a descoberta de dados eficaz é a chave para o compartilhamento de dados. Uma vez descobertos, os conjuntos de dados devem ser referenciados por meio de citações completas, incluindo identificadores persistentes para garantia de acesso futuro. Os princípios FAIR F1, F2, F3, F4 estão de certa forma, implícitos neste requisito ao mencionar que os (meta)dados devem ter identificadores globais, persistentes e identificáveis como, por exemplo, DOI ou ARK. Para que os dados sejam encontrados, os metadados devem ser indexados por mecanismos de busca que, por sua vez, permitem aos usuários encontrá-los.

O requisito 14 do *CoreTrustSeal,* 'Reutilização de dados', menciona que o repositório deve permitir a reutilização dos dados ao longo do tempo, garantindo que os metadados apropriados estejam disponíveis para apoiar a compreensão e o uso dos dados. O requisito do ACTDR 'O repositório deve rastrear e gerenciar os direitos de propriedade intelectual e restrições ao uso do conteúdo do repositório, conforme exigido pelo acordo de depósito, contrato ou licença' também trata sobre a questão da reutilização de dados. Observou-se que os princípios TRUST também abordam a questão através do critério '*User Focus* (Foco no usuário)'. O *CoreTrustSeal* orienta que os repositórios devem garantir que os dados continuem a ser compreendidos e usados de forma eficaz no futuro, apesar das mudanças na tecnologia e na base de conhecimento da comunidade designada. O ACTDR relata que isso é necessário para permitir que o repositório rastreie, atue e verifique os direitos e restrições relacionadas ao uso dos objetos digitais dentro do repositório. Os Princípios TRUST mencionam

que os repositórios têm um papel vital na aplicação e reforço das normas e padrões, o que inclui os esquemas de metadados, formatos de arquivos de dados, vocabulários controlados, ontologias e outras semânticas. Também mencionam que um repositório confiável precisa se concentrar em servir sua comunidade de usuários-alvo.

O requisito 15 do *CoreTrustSeal* corresponde a 'Infraestrutura técnica' e orienta que o repositório funcione em sistemas operacionais bem suportados e em outro software de infraestrutura central, e use tecnologias de hardware e software apropriadas para os serviços que fornece à sua comunidade. O ACTDR possui uma subdivisão 'Gestão de risco de infraestrutura e segurança' e o requisito 'gestão de risco de infraestrutura técnica', indicando que o repositório deve identificar e gerenciar os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema. Os Princípios FAIR A1, A1.1, I1, I2 e R1.3 possuem relação com este requisito e tratam sobre os dados serem acessíveis. Não foram encontrados estes requisitos entre os princípios TRUST. O *CoreTrustSeal* orienta que os repositórios precisam operar em infraestruturas centrais confiáveis e estáveis que maximizam a disponibilidade do serviço. Ademais, o hardware e o software usados devem ser relevantes e apropriados para a comunidade e para as funções que o repositório desempenha. De acordo com ACTDR este requisito é necessário para garantir uma infraestrutura segura e confiável. Os Princípios FAIR A1, A1.1 mencionam que os (Meta)dados devem ser recuperáveis pelos seus identificadores usando um protocolo de comunicação padronizado aberto, gratuito e universalmente implementável. Já os Princípios FAIR I1 e I2 mencionam que os (Meta)dados devem ser representados por meio de uma linguagem formal, acessível, compartilhada e amplamente aplicável para a representação do conhecimento. Como os dados e metadados devem possuir referências aos vocabulários que contenham os conceitos utilizados, devemos garantir que sejam utilizados vocabulários que também sigam os princípios FAIR. Já o Princípio R1.3, diz que os (Meta)dados devem estar alinhados com padrões relevantes ao seu domínio, ou seja, deve atender os padrões específicos da comunidade da área e às boas práticas de arquivamento e ao compartilhamento do campo de pesquisa específico.

O requisito 16 do *CoreTrustSeal* refere-se a 'Segurança', ou seja, a infraestrutura técnica do repositório deve oferecer proteção para as instalações e seus dados, produtos, serviços e usuários. O instrumento ACTDR possui alguns requisitos relacionados à segurança: Gestão de acesso (o repositório deve obedecer às Políticas de Acesso); subdivisão 'Gestão de risco de infraestrutura e segurança', requisito 'gestão de risco de infraestrutura técnica' (o repositório deve identificar e gerenciar os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema), requisito 'gestão de risco de segurança' (o repositório deve manter uma análise sistemática dos fatores de risco de segurança associado a dados, sistemas, pessoal e planta física). Entre os princípios TRUST, nos itens *Responsibility* e *Technology* foram encontradas menções sobre segurança. O Princípio FAIR A1.2 está implícito neste requisito.

Conforme consta no *CoreTrustSeal*, o repositório deve analisar ameaças potenciais, avaliar riscos e criar um sistema de segurança consistente. Conforme os

requisitos citados e encontrados no ACTDR, o termo "acesso" tem vários sentidos diferentes, incluindo o acesso dos usuários ao sistema de repositório, por exemplo, segurança física e autenticação de usuário, e os diferentes estágios de acesso aos registros. Entre os princípios TRUST existem especificações para gerenciar os direitos de propriedade intelectual dos produtores de dados, proteção de recursos de informações confidenciais, e a segurança do sistema e seu conteúdo; como também ter planos e mecanismos em vigor para prevenir, detectar e responder à ameaças à segurança física ou cibernética. De acordo com o Princípio FAIR A1.2, quando necessário, dependendo das restrições ao acesso aos dados e/ou metadados, um mecanismo para autenticação e autorização para o acesso deve ser permitido pelo protocolo de comunicação.

A partir da análise documental minuciosa sobre os critérios/requisitos presentes no *CoreTrustSeal Trustworthy Data Repositories Requirements 2020–2022; ACTDR - Audit and Certification of Trustworthy Digital Repositories; Principles FAIR;* e *The TRUST Principles for digital repositories*, elaborou-se um conjunto de critérios/requisitos, conforme descritos no Quadro 1 a seguir.

Quadro 1. Síntese e agrupamento do conjunto de critérios/requisitos para repositórios de dados de pesquisa confiáveis

INFRAESTRUTURA ORGANIZACIONAL/TRANSPARÊNCIA
Requisitos/Princípios: - Missão/escopo (*CoreTrustSeal*) - Governança e viabilidade organizacional (ACTDR) - *Transparency* (TRUST)
Estratégias a serem utilizadas pelos repositórios
1 Descrever na missão da organização a missão em preservar e fornecer acesso aos dados.
2 Declarar de forma transparente o prazo mínimo de preservação digital para os acervos de dados.
Requisitos/Princípios: - Licenças (*CoreTrustSeal*) - Contratos, licenças e responsabilidades(ACTDR) - *Responsibility* (TRUST) - *Reusable* (FAIR)
Estratégias a serem utilizadas pelos repositórios
1 Possuir regulamentos de acesso e licenças aplicáveis cobrindo o uso de dados.
2 Possuir descrito as condições de uso e a proteção de dados confidenciais.
3 Possuir uma política pública em vigor para o descumprimento no caso de divulgação de dados pessoais.

4 Possuir contratos de depósitos devidamente assinados e executados de acordo com as normas locais, leis e regulamentos nacionais e internacionais.
5 Possuir políticas sobre acordos de depósitos de terceiros e usos permitidos.
Requisitos/Princípios: - Continuidade de acesso (*CoreTrustSeal*) - Governança e viabilidade organizacional (ACTDR) - *Sustainability* (TRUST)
Estratégias a serem utilizadas pelos repositórios
1 Possuir um plano de continuidade para garantir o acesso contínuo e a preservação de seus acervos.
2 Possuir descrito a governança relacionada à operação contínua do repositório ao longo do tempo e durante desastres, bem como evidências em relação ao planejamento de sucessão, designadamente, as medidas em vigor para garantir o acesso e a disponibilidade dos acervos de dados, atualmente e no futuro.
3 Ter acordo formal para garantir quem assumirá a responsabilidade em caso de descontinuidade do serviço.
4 Possuir um plano estratégico de preservação com definições administrativas que defina a abordagem que o repositório terá no suporte de longo prazo.
5 Possuir um plano de sucessão adequado, planos de contingência, e/ou acordos de custódia em vigor no caso do repositório deixar de operar ou a instituição governamental ou de financiamento alterar substancialmente seu escopo.
Requisitos/Princípios: - Confidencialidade/Ética (*CoreTrustSeal*) - *Responsibility* (TRUST)
Estratégias a serem utilizadas pelos repositórios
1 Garantir que os dados sejam tratados com curadoria, usados e acessados em conformidade com as normas.
2 Garantir que a coleta e criação de dados seja realizada com os critérios legais e éticos.
3 Gerenciar de maneira adequada os dados com risco de divulgação para limitar acesso.
4 Treinar os funcionários do repositório em relação ao gerenciamento de dados com risco de divulgação.
5 Possuir medidas em vigor caso as condições não sejam cumpridas.
6 Possuir os procedimentos em vigor documentados para garantir a conformidade.

7 Gerenciar os direitos de propriedade intelectual dos produtores de dados, proteger os recursos de informações confidenciais, a segurança do sistema e o seu conteúdo.
Requisitos/Princípios: - Infraestrutura organizacional (*CoreTrustSeal*) - Estrutura organizacional e pessoal (ACTDR) - *Technology* (TRUST)
Estratégias a serem utilizadas pelos repositórios
1 Possuir financiamento adequado e número suficiente de funcionários.
2 Ser hospedado por uma instituição reconhecida para a garantia da estabilidade e sustentabilidade de longo prazo.
3 Ter financiamento suficiente incluindo recursos de equipe e TI.
4 Possuir um plano de pessoal, definições de competência, e desenvolvimento profissional de equipe.
Requisitos/Princípios: - Orientação de especialista (*CoreTrustSeal*) - Contratos, licenças e responsabilidades (ACTDR)
Estratégias a serem utilizadas pelos repositórios
1 Possuir um aconselhamento e feedback de especialistas para garantir sua relevância e melhorias contínuas.
2 Possuir consultores internos ou um comitê consultivo (especialistas técnicos).
3 Examinar por meio de especialistas as políticas de preservação e planos de implementação do repositório.
GERENCIAMENTO DE OBJETOS DIGITAIS
Requisitos/Princípios: - Integridade e autenticidade dos dados (*CoreTrustSeal*) - Preservação de AIP (ACTDR) - Gestão de informações (ACTDR) - *Reusable* (FAIR)
Estratégias a serem utilizadas pelos repositórios
1 Fornecer evidências mostrando que opera um sistema de gerenciamento de dados e metadados adequado para garantir integridade e autenticidade durante o processo de armazenamento e acesso a dados.

2 Descrever a documentação da integridade em detalhes, assim como todas as alterações e descrições de controle de versões.
3 Possuir especificações de como os AIPs (*Archival Information Package*) – conjunto de informações contendo qualidades referente a preservação de determinado objeto de informação - são armazenados.
4 Disponibilizar a representação da informação para cada AIP.
5 Utilizar metadados descritivos e identificadores únicos persistentes associado ao AIP.
Requisitos/Princípios: - Avaliação (*CoreTrustSeal*) - Responsabilidade processual e política de preservação (ACTDR)
Estratégias a serem utilizadas pelos repositórios
1 Revisar os critérios de seleção ao longo do tempo e os ativos digitais devem ser reavaliados adequadamente.
2 Possuir uma política de desenvolvimento de coleção para orientar a seleção de dados.
3 Realizar uma avaliação automatizada da aderência dos metadados aos esquemas relevantes.
4 Possuir algum cronograma regular de autoavaliação e certificação externa.
5 Possuir listas de verificação preenchidas e datadas de autoavaliações e/ou auditorias.
Requisitos/Princípios: - Procedimentos de armazenamento documentados (*CoreTrustSeal*) - *Ingest*: criação do *Archival Information Package* (AIP). (ACTDR)
Estratégias a serem utilizadas pelos repositórios
1 Documentar os procedimentos e padronizar de forma que diferentes gerenciadores de dados, embora realizem as mesmas tarefas separadamente, cheguem ao mesmo resultado.
Requisitos/Princípios: - Plano de preservação (*CoreTrustSeal*) - Planejamento de preservação (ACTDR) - *Accessible* (FAIR)
Estratégias a serem utilizadas pelos repositórios
1 Especificar na documentação as ações relevantes para a preservação, incluindo a transferência de custódia, padrões de informações de envio e padrões de informações de arquivo.

2 Desenvolver alguma documentação que identifique os riscos de preservação e as estratégias para lidar com esses riscos.
3As estratégias de preservação e o plano estratégico de preservação deve abordar a degradação da mídia de armazenamento, a obsolescência das unidades de mídia e a obsolescência ou inadequação da representação das informações (incluindo formatos) como a base no conhecimento da comunidade designada.
Requisitos/Princípios: - Qualidade dos dados (*CoreTrustSeal)* - *Responsibility* (TRUST) *Interoperable/Reusable* (FAIR)
Estratégias a serem utilizadas pelos repositórios
1 Possuir verificações de controle de qualidade para garantir a integridade e a compreensibilidade dos dados depositados.
2 Possibilitar que a comunidade designada comente ou classifique dados e metadados.
3 Fornecer citações de trabalhos relacionados aos dados ou links para índices de citações.
4 Possuir validação técnica e controle de qualidade.
Requisitos/Princípios: - Fluxos de trabalho (*CoreTrustSeal*) - ACTDR
Estratégias a serem utilizadas pelos repositórios
1 Definir os fluxos de trabalho (descrições de processos de negócios) e a comunicação clara para depositantes e usuários sobre o manuseio de dados.
2 Definir os níveis de segurança e impacto nos fluxos de trabalho (proteção da privacidade dos sujeitos).
3 Adotar uma abordagem consistente, rigorosa e documentada para gerenciar todas as atividades em seus processos.
Requisitos/Princípios: - Descoberta e identificação de dados (*CoreTrustSeal*) - Gestão de informações (ACTDR) *Findable* (FAIR)
Estratégias a serem utilizadas pelos repositórios

1 Oferecer recursos de pesquisa e manter um catálogo de metadados pesquisável para padrões apropriados.
2 Facilitar a coleta automática dos metadados e oferecer recomendação de citação de dados.
3 Fornecer evidências de que toda a curadoria de dados e metadados apoia a descoberta de objetos digitais claramente definidos e identificados e permitir sua vinculação com objetos digitais relacionados de acordo com os padrões de domínio.
4 Esclarecer para a comunidade como os dados são citados, de modo que o crédito e a atribuição apropriado seja dado aos indivíduos/organizações que contribuíram para sua criação.
5 Especificar os requisitos mínimos de informação para permitir a comunidade designada a descobrir e identificar materiais de interesse.
Requisitos/Princípios: - Reutilização de dados (*CoreTrustSeal*) - *User focus* (TRUST)
Estratégias a serem utilizadas pelos repositórios
1 Garantir que os dados continuem a ser compreendidos e usados de forma eficaz no futuro, apesar das mudanças na tecnologia e na base de conhecimento da comunidade designada.
2 Fornecer catálogos para facilitar a descoberta de dados.
TECNOLOGIA/GESTÃO DE RISCO DE INFRAESTRUTURA E SEGURANÇA/*SUSTAINABILITY*
Requisitos/Princípios: - Infraestrutura técnica (*CoreTrustSeal*) - Gestão de risco de infraestrutura técnica (ACTDR) - *Reusable* (FAIR)
Estratégias a serem utilizadas pelos repositórios
1 Operar em infraestruturas centrais confiáveis e estáveis que maximizam a disponibilidade do serviço.
2 Descrever quais padrões o repositório usa para referência (se são padrões internacionais ou comunitários) e com que frequência são revisados.
3 Possuir um plano de desenvolvimento de infraestrutura.
4 Desenvolver um inventário de software e a documentação do sistema deve estar disponível.

5 Elaborar procedimentos e arranjos para fornecer recuperação rápida ou backup de serviços essenciais no caso de uma interrupção.
6 Realizar avaliações periódicas de tecnologia e fazer estimativas da vida útil dos componentes do sistema.
7 O repositório deve realizar ou contratar avaliações dos riscos relacionados ao hardware e infraestrutura de software e procedimentos operacionais.
Requisitos/Princípios: - Segurança (*CoreTrustSeal*) - Gestão de risco de segurança (ACTDR) - *Technology* (TRUST) - *Accessible* (FAIR)
Estratégias a serem utilizadas pelos repositórios
1 Analisar ameaças potenciais, avaliar riscos e criar um sistema de segurança consistente.
2 Possuir mecanismos para prevenir, detectar e responder a um incidente de segurança, ou seja, demonstrar de que forma a segurança da infraestrutura técnica é controlada pelo repositório e por sua instituição hospedeira/terceirizada e quem está no comando.
3 Realizar avaliações de risco regulares e manter a segurança adequada a fim de fornecer os níveis de serviço previstos e contratados.
4 Manter uma análise sistemática dos fatores de risco de segurança associado a dados, sistemas, pessoal e planta física.
5 Ter planos e mecanismos em vigor para prevenir, detectar e responder à ameaças à segurança física ou cibernética.

Foi observado que alguns requisitos que constavam no ACTDR não estavam contemplados de forma clara nos instrumentos *CoreTrustSeal*, TRUST e FAIR. Comparando os instrumentos relacionados nesta pesquisa nota-se que o ACTDR apresenta seus requisitos de forma mais extensa e detalhada, o que pode dificultar a compreensão e aplicação. Assim sendo, esta pesquisa forneceu *insights* sobre questões metodológicas e evidenciou a necessidade de ampliação das investigações sobre o tema para promover e consolidar iniciativas no Brasil.

4 CONSIDERAÇÕES FINAIS

Instituições brasileiras estão em busca do desenvolvimento e implementação de repositórios de dados de pesquisa e observa-se a grande necessidade de ampliar

os estudos referentes à avaliação, pois trata-se de uma etapa de extrema importância na implementação e acompanhamento de sistemas de informação. Internacionalmente, existem instituições que avaliam e oferecem certificações para repositórios de dados, no entanto, no Brasil, os estudos estão em fases iniciais, com falta de padronização e clareza na definição de critérios avaliativos.

O estudo de repositórios confiáveis é uma das linhas de pesquisa em preservação digital mais trabalhadas em nível internacional. Busca-se definir metodologias e ferramentas de avaliação de acordo com padrões. Avaliações e autoavaliações podem ser uma contribuição importante para garantir a confiabilidade dos repositórios de dados de pesquisa.

Propõe-se a aplicação dos requisitos apresentados no Quadro 1 em um processo de autoavaliação interna realizada pela equipe do próprio repositório, que é então revisada pelos colegas da comunidade. Essa abordagem da comunidade garante uma atmosfera inclusiva na qual o repositório candidato e os revisores interagem estreitamente. Além dos benefícios externos, como o fortalecimento da confiança das partes interessadas, o aprimoramento da reputação do repositório e a demonstração de que o repositório está seguindo as boas práticas, a certificação principal fornece vários benefícios internos ao repositório.

Pode-se perceber, a partir da literatura abordada nesta pesquisa, que as publicações sobre repositórios de dados de pesquisa confiáveis ainda são incipientes no contexto brasileiro. Neste sentido, considera-se fundamental ampliar a discussão sobre o assunto. A leitura e comparação dos documentos *CoreTrustSeal - Trustworthy Data Repositories Requirements* 2020–2022; ACTDR - *Audit and Certification of Trustworthy Digital Repositories*; FAIR Principles; e *The TRUST Principles for digital repositories* permitiu uma análise profunda de critérios e requisitos que vem sendo utilizados internacionalmente. Apesar de constituírem documentos de natureza distinta, todos eles indicam requisitos que vão na mesma direção, qual seja, compor o conjunto de características de repositórios confiáveis. Nesse sentido, a ampla divulgação e conhecimento acerca destes documentos no Brasil é fundamental para garantir o planejamento de repositórios confiáveis desde sua fase inicial.

REFERÊNCIAS

ALBAGLI, S.; CLINIO, A.; RAYCHTOCK, S. Ciência Aberta: correntes interpretativas e tipos de ação. **Liinc Em Revista**, Rio de Janeiro, v. 10, n. 2, 2014. Disponível em: https://doi.org/10.18617/liinc.v10i2.749 . Acesso em: 16 fev. 2022.

ASSIS, Tainá Batista de. Rede brasileira de repositórios e o impacto dos trabalhos das subredes. I Encontro Rede Sudeste de Repositórios Institucionais. **Anais.** 2019. Disponível em:https://www.arca.fiocruz.br/bitstream/icict/33642/2/Anais_I_Encontro_Sudeste_RIAA_2019.pdf. Acesso em: 13 set. 2020.

AVENTURIER, Pascal. **Princípios FAIR:** critérios de qualidade para dados de pesquisa. A publicação científica, 2017. Disponível em: https://publicient.hypotheses.org/1456. Acesso em: 25 jul. 2020.

CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS- CCSDS. **Audit and Certification of Trustworthy Digital Repositories - ACTDR**. Magenta Book, 2011.

CORETRUSTSEAL. **The World Data System of the International Science Council (WDS) and the Data Seal of Approval (DSA) are pleased to announce the launch of a new certification organization:** CoreTrustSeal. 2020a. Disponível em: https://www.coretrustseal.org/about/. Acesso em: 26 abr. 2020.

CORETRUSTSEAL. **Coretrustseal Trustworthy Data Repositories Requirements 2020-2022**. 2020b. Disponível em: https://www.coretrustseal.org/wp-content/uploads/2017/01/Core_Trustworthy_Data_Repositories_Requirements_01_00.pdf. Acesso em: 17 jun. 2020.

CORETRUSTSEAL. **Update: Draft Requirements 2023-2025.** Disponível em: https://www.coretrustseal.org/why-certification/meeting-community-needs/trustworthy-data-repository-requirements-review-2023-2025/. Acesso em: 16 jul. 2022.

CURTY, Renata. Para onde os dados devem ir afinal? **Dados de pesquisa abertos.** 2018. Disponível em: https://dadosdepesquisa.rnp.br/para-onde-os-dados-devem-ir-afinal. Acesso em: 9 jan. 2020.

DOWNS, Robert R. **Improving Opportunities for New Value of Open Data:** Assessing and Certifying Research Data Repositories. Data Science Journal, 2021. Disponível em: https://datascience.codata.org/article/10.5334/dsj-2021-001. Acesso em: 4 fev. 2021.

DUDZIAK, Elisabeth. Dados de Pesquisa agora devem ser armazenados e citados. **SIBIUSP**, 2016. Disponível em: http://www.sibi.usp.br/noticias/dados-materiais-metodos-revistas-exigem-dados-pesquisa-estejam-disponiveis. Acesso em: 5 jan. 2020.

HODSON, S. et al. **Turning FAIR into reality**. Interim report of the European Commission Expert Group on FAIR data. 2018. Disponível em: https://ec.europa.eu/info/sites/default/files/turning_fair_into_reality_1.pdf. Acesso em: 31, jul. 2018.

JANTZ, Ronald; GIARLO, Mike. **Digital Preservation:** Architecture and Technology for Trusted Digital Repositories. 2006. Disponível em: http://www.dlib.org/dlib/june05/jantz/06jantz.html. Acesso em: 4 maio. 2021.

LAMEIRA, Ana Kelly Alves. Avaliação de repositórios institucionais brasileiros: uma proposta de método de avaliação. **Cadernos BAD**, 2016. Disponível em: https://bad.pt/publicacoes/index.php/cadernos/article/view/1594. Acesso em: 17 abr. 2020.

MÁRDERO ARELLANO, Miguel Ángel. Critérios para a preservação digital da informação científica. 354f. **Tese** (Doutorado em Ciência da Informação) - Universidade Federal de Brasília, Departamento de Ciência da Informação, 2008. Disponível em: https://core.ac.uk/download/pdf/11884842.pdf. Acesso em: 27 maio. 2021.

MEDEIROS, Jackson da Silva. **Uma investigação sobre a autoria de dados científicos: teias de uma rede em construção.** 2015. Tese (doutorado) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2015. Disponível em: https://lume.ufrgs.br/handle/10183/116504. Acesso em: 3 abr. 2020.

RAUEN, Cristiane Vianna. A relevância de uma política nacional de acesso aberto a dados de pesquisa. **Revista Construção**, 2018. Disponível em: http://revistaconstrucao.org/ciencia-e-tecnologia/relevancia-de-uma-politica-nacional-de-acesso-aberto-dados-de-pesquisa/. Acesso em 14 maio. 2020.

RLG/OCLC WORKING GROUP ON DIGITAL ARCHIVE ATTRIBUTES. **Trusted digital repositories:** attributes and responsibilities. May 2002. Disponível em: https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf. Acesso em: 24 mar. 2021.

SAYÃO, Luis Fernando; SALES, Luana Farias. Subsídios para a construção de um modelo de avaliação de sistemas de gestão de dados de pesquisa. **Ponto de Acesso**, Salvador, v.12, n.3, p.80-108, dez. 2018. Disponível em: http://www.brapci.inf.br/index.php/res/download/119953. Acesso em: 3 abr. 2020.

TARTAROTTI, Roberta Cristina Dal´Evedove; DAL´EVEDOVE, P. R.; FUJITA, Mariângela Spotti Lopes. Biblioteconomia de dados em repositórios de pesquisa: perspectivas para a atuação bibliotecária. **Informação & Informação**, v. 24, n. 3, p. 207-226, 2019. Disponível em: https://www.brapci.inf.br/index.php/res/v/134221. Acesso em: 27 mar. 2020.

WILKINSON, Mark D. *et al*. The FAIR Guiding Principles for scientific data management and stewardship. **Scientific Data,** 2016**.** Disponível em: https://www.nature.com/articles/sdata201618. Acesso em: 23 jan. 2020.

VANZ, Samile Andrea de Souza; STUMPF, Ida Regina Chittó. Colaboração científica: revisão teórico conceitual. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 15, n. 2, Ago. 2010. Disponível em: https://doi.org/10.1590/S1413-99362010000200004 Acesso em: 16 fev. 2023.