Disponível em www.bad.pt/publicacoes

PAPER

12º CONGRESSO NACIONAL BAD

Estudo comparativo de referenciais normativos para avaliação da confiabilidade e certificação de repositórios digitais

Luis Corujo[a], *Miguel Ferreira*[b]

[a]*Faculdade de Letras da Universidade de Lisboa, Portugal, luiscorujo@campus.ul.pt*
[b]*KEEP SOLUTIONS, Portugal, mferreira@keep.pt*

Resumo

Neste trabalho toma-se como base os referenciais normativos relacionados com a temática da confiabilidade e certificação de repositórios e digitais. Partindo da premissa de que os repositórios digitais são elementos essenciais das instituições com funções de preservação do património digital, pretendeu-se analisar como podem ser considerados dignos de confiança por parte dos seus utilizadores. Tal análise permitiu considerar que elementos promovem e reforçam a confiabilidade através do cumprimento de normas, recomendações, e processos de auditoria e de certificação. Nesse sentido foram estudados vários referenciais normativos que visam aferir e certificar a confiabilidade de repositórios digitais. Nesta proposta de comunicação iremos apresentar uma comparação entre o TRAC, a ISO 16363:2012 e o NESTOR.

Palavras-chave: Repositório Digital, Confiança, Certificação; Auditoria; Normalização, ISO 16363, TRAC, NESTOR

Introdução

É do conhecimento geral que os conteúdos digitais são constituídos por uma sequência de dígitos binários que para serem interpretados necessitam de um sistema intermediário constituído por software e hardware. Verifica-se, no entanto, a existência de um conjunto de potenciais problemas associados a este tipo de material que incluem a perda de informação, perda de valor evidencial, dificuldades de gestão, rápida obsolescência tecnológica e instabilidade dos suportes. Não obstante, uma grande maioria dos ativos de informação produzidos atualmente nascem codificados em formatos digitais, e.g. fotografias, bases de dados, documentos, vídeo, áudio, registos da atividade pública e privada, etc.

Num mundo em rápido desenvolvimento tecnológico terão as instituições responsáveis pelo património informacional a capacidade de assegurar a preservação dos ativos digitais e fornecer acesso continuado a esta documentação? Conseguirão estas instituições assegurar que documentos digitais mantêm as mesmas características de fidedignidade, integridade e autenticidade dos tradicionais documentos em papel? Poderão os produtores e consumidores de informação digital, as entidades financiadoras e a comunidade em geral confiar na capacidade das instituições para gerir e preservar a documentação digital?

Estas são algumas questões que se têm vindo a colocar ao longo das últimas três décadas desde que várias organizações assumiram definitivamente a sua adesão aos formatos digitais para a produção, gestão e salvaguarda dos seus registos e documentos. Neste contexto, a questão da confiança é central quando se trata de informação em suporte digital. A tentativa de responder a questões como as anteriores trouxe para o debate científico a necessidade de assegurar a confiabilidade dos repositórios digitais.

Neste trabalho pretendeu-se analisar os desenvolvimentos registados ao longo das últimas décadas na área da Preservação Digital e demonstrar que os repositórios digitais confiáveis são o corolário sistémico que pretende dar resposta ao conjunto de problemas cada vez mais complexos referentes à ingestão, gestão, manutenção, preservação e garantia de acesso à informação digital a longo prazo. Considera-se, assim, necessário a existência de um plano de gestão sistematizado com processos específicos, a definição de políticas, gestão de recursos, estratégias, a aplicação de métodos e atividades definidas através de um compromisso de investimento continuado que aumente as perspetivas da preservação e a redução dos seus custos.

Verifica-se a necessidade de uma abordagem sistémica e não apenas tecnológica para a preservação do património digital, com um modelo integrado em instituições com responsabilidades na sua manutenção e que garanta o seu acesso e utilização. Considerando os Repositórios Digitais, sistemicamente, como um conjunto de pessoas, sistemas e tecnologias que têm como responsabilidade preservar informação e disponibilizá-la à sua comunidade de interesse, as finalidades e objetivos das entidades que gerem o Património Digital são comparáveis com as dos Repositórios Digitais.

Neste âmbito assume papel magistral o modelo de referência OAIS (Open Archival Information System, ISO 14721:2003)[1] cujo espectro de aplicação extravasou o objeto de informação de arquivo. Podemos considerar que tal se deveu ao facto do trabalho desenvolvido em torno deste modelo de referência, em termos de metainformação estrutural e de preservação, e também de especificação das interfaces, têm como finalidade o desenvolvimento de toda uma estrutura de normalização com o fito de aumentar a confiabilidade nos repositórios digitais.

Esta necessidade de afirmar que o repositório digital é de confiança surge como tentativa de fazer o contraponto aos riscos derivados da especificidade da informação digital. Implica portanto anteceder-se a estes, identificá-los e medi-los, para que não haja desvios face aos resultados expectados .

No caso específico dos repositórios digitais aplicam-se três níveis de confiança, referentes à forma como conquistam a confiança das suas comunidades de interesse, como confiam nos fornecedores externos, e como os consumidores confiam na informação fornecida pelo repositório. Assim, para atingir os seus objetivos, um repositório digital deve corresponder a um conjunto de expectativas que passam pela sua existência no âmbito de um sistema organizacional que viabilize a preservação da informação e o próprio repositório a longo prazo, e que aceite a responsabilidade pela manutenção dos recursos digitais ao longo do tempo de acordo com os interesses dos depositantes, dos atuais e futuros utilizadores.

---

[1] ISO 14721:2012, Space data and information transfer systems: Open archival information system (OAIS) - Reference model. Geneva. ISO.

O repositório deve também demonstrar responsabilidade quanto à sua sustentabilidade financeira, agir de acordo com as recomendações e normas internacionais referentes à gestão, acesso e segurança dos recursos digitais, definir metodologias para avaliação da qualidade dos sistemas de acordo com as expectativas de confiabilidade da comunidade, e que mantenha políticas, práticas e desempenhos auditáveis (por entidades independentes).

Não menos importante são as questões relacionadas com a tecnologia, nomeadamente o software, o hardware e segurança da infraestrutura que os suporta.

Tudo isto desemboca num processo de auditoria e certificação, baseado num qualquer referencial normativo. Para concretizar estes processos de auditoria e certificação têm concorrido uma série de referenciais, que em geral, enquadram as funções expectáveis dos repositórios digitais nas seguintes categorias:

- Conformidade com o modelo de referência OAIS;
- Responsabilidade administrativa;
- Viabilidade organizacional;
- Sustentabilidade financeira;
- Adequação tecnológica e procedimental;
- Segurança do sistema
- Registo de evidências do cumprimento dos procedimentos implementados[2].

São exemplos destes referenciais normativos a ISO 16363:2012[3], o NESTOR[4], o Data Seal of Approval[5] e o European Framework for Audit and Certification of Digital Repositories[6], todos estes no âmbito da certificação.

O DRAMBORA enquadra-se no mesmo contexto, porém foca-se mais na avaliação de risco, e o PLATTER trata-se de uma ferramenta para planeamento de repositórios digitais confiáveis.

Alinhamento de referenciais normativos

Constata-se que no âmbito da certificação emergem tantos referenciais normativos com vista à certificação, que as entidades dos quais emanam acabam por ser concorrenciais. Daí termos considerado importante aventurarmo-nos numa comparação entre os vários referenciais normativos que ponderámos serem os mais utilizados, ou mais amplamente disseminados: o TRAC e o referencial que o sucedeu, ou seja, a ISO 16363:2012 e o NESTOR[7].

Esta comparação permitiu apurar que o TRAC sistematizou as recomendações mais significativas fornecidas pelos estudos académicos produzidos até então, e conta com um conjunto de requisitos a serem usados no âmbito de auditorias internas e externas. Pode ser usado para o estabelecimento de metas, planeamento, construção de políticas, e avaliação. Foca-se nos repositórios de preservação.

---

[2] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development. Archival science.
[3] ISO 16363:2012, Space data and information transfer systems: Audit and certification of trustworthy digital. Geneva. ISO
[4] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories.
[5] http://datasealofapproval.org/en/
[6] http://www.trusteddigitalrepository.eu/Welcome.html
[7] CORUJO, Luis – Repositórios Digitais e Confiança – Um exemplo de repositório de Preservação Digital: o RODA. Lisboa: FLUL, 2014

A ISO 16363:2012 sucede ao TRAC, tendo sido desenvolvido por meio de auditorias técnicas realizadas a repositórios nos anos que antecederam a elaboração do TRAC. Este documento foi produzido como norma internacional a ser utilizada para obtenção de certificação por parte das organizações detentoras de repositórios digitais, requerendo a existência de mecanismos independentes de verificação e de prova documental de todos os procedimentos. Com o estabelecimento desta nova norma, as instituições detentoras de repositórios digitais passam a ter objetivos mensuráveis para determinar a confiança nos seus repositórios, permitindo aos seus utilizadores aferir se uma instituição detentora de arquivos digitais é capaz de satisfazer as suas necessidades.

Por seu lado, o NESTOR é um catálogo com referências e notas derivados do contexto alemão em termos de restrições legais, funcionamento das instituições públicas, decisões organizacionais, principalmente no âmbito explícito da gestão da qualidade e da segurança de TI. Pode ser usado para o planeamento, construção e avaliação, mas não fornecem detalhes quanto à implementação.

A tabela que se segue apresenta o conjunto global de requisitos normativos incluídos no ISO 16363:2012, TRAC e NESTOR. Para cada um dos requisitos é indicado o identificador que esse requisito assume em cada um dos referenciais normativos. Os vários requisitos estão agrupados de acordo com as seguintes secções:

- Estrutura organizacional
- Gestão de objetos digitais
- Infraestrutura e gestão da segurança

Requisitos	**ISO 16363**	**TRAC**	**NESTOR**
ORGANIZATIONAL INFRASTRUCTURE **Estrutura organizacional**			
GOVERNANCE AND ORGANIZATIONAL VIABILITY	3.1	A1.	-
The repository shall have a mission statement that reflects a commitment to the preservation of, long term retention of, management of, and access to digital information.	3.11	A1.1	1.2
The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission.	3.12	-	8
The repository shall have an appropriate succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.	3.1.2.1	A1.2.	4.6
The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.	3.1.2.2	A4.5. parcialmente	4.6
The repository shall have a Collection Policy or other document that specifies the type of information it will preserve, retain, manage, and provide access to.	3.1.3	-	1.1
ORGANIZATIONAL STRUCTURE AND STAFFING	3.2	A2.	-
The repository shall have identified and established the duties that it needs to perform and shall have appointed staff with adequate skills and experience to fulfill these duties.	3.2.1	A2.1. A2.2.	4.3 5.1 4.2
The repository shall have identified and established the duties that it needs to perform.	3.2.1.1	A2.1.	4.3 5.1
The repository shall have the appropriate number of staff to support all functions and services.	3.2.1.2	A2.2.	4.2
The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.	3.2.1.3	A2.3.	-
PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK	3.3	A3	-
The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.	3.3.1	A3.1.	1.3
The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.	3.3.2	-	-
The repository shall have mechanisms for review, update, and ongoing development of its Preservation Policies as the repository grows and as technology and community practice evolve.	3.3.2.1	A3.2.	-
The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.	3.3.3	A3.6.	-
The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time	3.3.4	A3.7.	-
The repository shall define, collect, track, and appropriately provide its information integrity measurements.	3.3.5	A3.8	-

Requisitos	ISO 16363	TRAC	NESTOR
The repository shall commit to a regular schedule of self-assessment and external certification.	3.3.6	A3.9	-
Repository has policies and procedures to ensure that feedback from producers and users is sought and addressed over time	-	A3.5	-
FINANCIAL SUSTAINABILITY	3.4	A4	-
The repository shall have short- and long-term business planning processes in place to sustain the repository over time.	3.4.1	A4.1.	4.1
The repository shall have financial practices and procedures which are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.	3.4.2	A4.3.	-
The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).	3.4.3	A4.4.	-
Repository has in place processes to review and adjust business plans at least annually	-	A4.2	-
CONTRACTS, LICENSES, AND LIABILITIES	3.5	A5	-
The repository shall have and maintain appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.	3.5.1	A5.1	3.1
The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred shall be documented.	3.5.1.1	A5.2	
The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	3.5.1.2	A5.3	3.2
The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.	3.5.1.3	A3.3. B1.7	1.1
The repository shall have policies in place to address liability and challenges to ownership/rights.	3.5.1.4	A5.5	
The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	3.5.2	A5.4	12.6
With regard to use, the repository acts on the basis of legal arrangements	-	-	3.3
DIGITAL OBJECT MANAGEMENT **Gestão de objetos digitais**			
INGEST: ACQUISITION OF CONTENT	4.1	B1	-
The repository shall identify the Content Information and the Information Properties that the repository will preserve.	4.1.1	B1.1.	9.2
The repository shall have a procedure(s) for identifying those Information Properties that it will preserve.	4.1.1.1	-	-
The repository shall have a record of the Content Information and the Information Properties that it will preserve.	4.1.1.2	-	-
The repository shall clearly specify the information that needs to be associated with specific Content Information at the time of its deposit.	4.1.2	B1.2.	9.1
The repository shall have adequate specifications enabling recognition and parsing of the SIPs.	4.1.3	-	-
The repository shall have mechanisms to appropriately verify the identity of the Producer of all materials.	4.1.4	B1.3	7.1
The repository shall have an ingest process which verifies each SIP for completeness and correctness.	4.1.5	B1.4	6.1
The repository shall obtain sufficient control over the Digital Objects to preserve them.	4.1.6	B1.5	9.3
The repository shall provide the producer/depositor with appropriate responses at agreed points during the ingest processes.	4.1.7	B1.6	-
The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.	4.1.8	B1.8	-
INGEST: CREATION OF THE AIP	4.2	B2	-
The repository shall have for each AIP or class of AIPs preserved by the repository an associated definition that is adequate for parsing the AIP and fit for long term preservation needs.	4.2.1	-	-
The repository shall be able to identify which definition applies to which AIP.	4.2.1.1	B2.1	10.1
The repository shall have a definition of each AIP that is adequate for long-term preservation, enabling the identification and parsing of all the required components within that AIP.	4.2.1.2	B2.2	10.1
The repository shall have a description of how AIPs are constructed from SIPs.	4.2.2	B2.3	10.2
The repository shall document the final disposition of all SIPs.	4.2.3	-	-
The repository shall follow documented procedures if a SIP is not incorporated into an AIP or discarded and shall indicate why the SIP was not incorporated or discarded.	4.2.3.1	B2.4	-
The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs.	4.2.4	B2.5	12.1
The repository shall uniquely identify each AIP within the repository.	4.2.4.1	B2.5	12.1
The repository shall have unique identifiers.	4.2.4.1.1	B2.5	12.1
The repository shall assign and maintain persistent identifiers of the AIP and its components so as to be unique within the context of the repository.	4.2.4.1.2	B2.5	12.1
Documentation shall describe any processes used for changes to such identifiers.	4.2.4.1.3	-	--
The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.	4.2.4.1.4	-	-
The system of identifiers shall be adequate to fit the repository's current and foreseeable future requirements such as numbers of objects.	4.2.4.1.5	-	-
The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location.	4.2.4.2	-	-
The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.	4.2.5	B2.7	-
The repository shall have tools or methods to identify the file type of all submitted Data Objects.	4.2.5.1	B2.8	12.3 12.5
The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.	4.2.5.2	B2.8	-
The repository shall have access to the requisite Representation Information.	4.2.5.3	-	-
The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects.	4.2.5.4	-	-
The repository shall have documented processes for acquiring Preservation Description Information (PDI) for its associated Content Information and acquire PDI in accordance with the documented processes.	4.2.6	B2.9	12.4 12.6.
The repository shall have documented processes for acquiring PDI.	4.2.6.1	B2.9	12.4 12.6
The repository shall execute its documented processes for acquiring PDI.	4.2.6.2	B2.9	12.4 12.6

Requisitos	ISO 16363	TRAC	NESTOR
The repository shall ensure that the PDI is persistently associated with the relevant Content Information.	4.2.6.3	B2.9	12.4 12.6
The repository shall ensure that the Content Information of the AIPs is understandable for their Designated Community at the time of creation of the AIP.	4.2.7	B2.10	2.2
Repository shall have a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation.	4.2.7.1	B2.10	2.2
The repository shall execute the testing process for each class of Content Information of the AIPs.	4.2.7.2	B2.10	2.2
The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.	4.2.7.3	B2.10	2.2
The repository shall verify each AIP for completeness and correctness at the point it is created.	4.2.8	B2.11	-
The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.	4.2.9	B2.12	6.1
The repository shall have contemporaneous records of actions and administration processes that are relevant to AIP creation.	4.2.10	B2.13	-
If unique identifiers are associated with SIPs before ingest, the repository preserves the identifiers in a way that maintains a persistent association with the resultant archived object (e.g., AIP).	B2.6	-	-
PRESERVATION PLANNING	4.3	B3	
The repository shall have documented preservation strategies relevant to its holdings.	4.3.1	B3.1	4.4. 8
The repository shall have mechanisms in place for monitoring its preservation environment.	4.3.2	B3.2 B3.3	-
The repository shall have mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings.	4.3.2.1	B3.2	-
The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.	4.3.3	B3.3	4.5
The repository shall have mechanisms for creating, identifying or gathering any extra Representation Information required.	4.3.3.1	-	-
The repository shall provide evidence of the effectiveness of its preservation activities	4.3.4	B3.4	-
AIP PRESERVATION	4.4	B4	-
The repository shall have specifications for how the AIPs are stored down to the bit level.	4.4.1	B4.2	10.4
The repository shall preserve the Content Information of AIPs.	4.4.1.1	B4.3	-
The repository shall actively monitor the integrity of AIPs.	4.4.1.2	B4.4	6.2 7.2
The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.	4.4.2	B4.5	-
The repository shall have procedures for all actions taken on AIPs.	4.4.2.1	-	-
The repository shall be able to demonstrate that any actions taken on AIPs were compliant with the specification of those actions.	4.4.2.2	-	-
Repository employs documented preservation strategies.	-	B4.1	-
INFORMATION MANAGEMENT	4.5	B5	-
The repository shall specify minimum information requirements to enable the Designated Community to discover and identify material of interest.	4.5.1	B5.1	-
The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.	4.5.2	B5.2	12.2
The repository shall maintain bi-directional linkage between each AIP and its descriptive information.	4.5.3	B5.3	12.7
The repository shall maintain the associations between its AIPs and their descriptive information over time.	4.5.3.1	B5.4	12.7
ACCESS MANAGEMENT	4.6	B.6	2.1 11.1 11.2
The repository shall comply with Access Policies.	4.6.1	B6.1 B6.5	6.3
The repository shall log and review all access management failures and anomalies.	4.6.1.1	B6.6	-
The repository shall follow policies and procedures that enable the dissemination of digital objects that are traceable to the originals, with evidence supporting their authenticity.	4.6.2	B6.10	7.3
The repository shall record and act upon problem reports about errors in data or responses from users.	4.6.2.1	B6.7 B6.8 B6.9	-
Repository has implemented a policy for recording all access actions (includes requests, orders etc.) that meet the requirements of the repository and information producers/depositors	-	B6.2	-
Repository ensures that agreements applicable to access conditions are adhered to.	-	B6.3	3.3
Repository has documented and implemented access policies (authorization rules, authentication requirements) consistent with deposit agreements for stored objects.	-	B6.4	-
INFRASTRUCTURE AND SECURITY RISK MANAGEMENT **Infraestrutura e gestão da segurança**			
TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	5.1	C1 C.2	5.2 13.1
The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure.	5.1.1	C1.1	-
The repository shall employ technology watches or other technology monitoring notification systems.	5.1.1.1	C2.1 C2.2	4.5
The repository shall have hardware technologies appropriate to the services it provides to its designated communities.	5.1.1.1.1	C2.1	4.5
The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.	5.1.1.1.2	C2.1	4.5
The repository shall have procedures in place to evaluate when changes are needed to current hardware.	5.1.1.1.3	C2.1	4.5
The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.	5.1.1.1.4	C2.1	4.5
The repository shall have software technologies appropriate to the services it provides to its designated communities.	5.1.1.1.5	C2.2	4.5
The repository shall have procedures in place to monitor and receive notifications when software changes are	5.1.1.1.6	C2.2	4.5

Requisitos	ISO 16363	TRAC	NESTOR
needed.			
The repository shall have procedures in place to evaluate when changes are needed to current software.	5.1.1.1.7	C2.2	4.5
The repository shall have procedures, commitment, and funding to replace software when evaluation indicates the need to do so.	5.1.1.1.8	C2.2	4.5
The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.	5.1.1.2	C1.2	-
The repository shall have effective mechanisms to detect bit corruption or loss.	5.1.1.3	C1.5	6.2
The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.	5.1.1.3.1	C1.6	-
The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.	5.1.1.4	C1.10	-
The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).	5.1.1.5	C1.7	-
The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.	5.1.1.6	-	-
The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.	5.1.1.6.1	C1.8	4.5
The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.	5.1.1.6.2	C1.9	4.5
The repository shall manage the number and location of copies of all digital objects.	5.1.2	C1.3	-
The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized.	5.1.2.1	C1.4	-
SECURITY RISK MANAGEMENT	5.2	C.3	-
The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.	5.2.1	C3.1	14
The repository shall have implemented controls to adequately address each of the defined security risks.	5.2.2	C3.2	13.2
The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.	5.2.3	C3.3	-
The repository shall have suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an offsite copy of the recovery plan(s).	5.2.4	C3.4	-

Tabela 1: Comparativo entre os referenciais normativos ISO 16363, TRAC e NESTOR.

Resultados e discussão

Na análise realizada verificou-se que, dos 85 requisitos do TRAC, 7 não passaram para a ISO 16363:2012 e que 44 não se verificam no NESTOR. A ISO 16363:2012 apresenta 109 requisitos, 18 dos quais não se verificam no TRAC e 50 dos quais não se verificam no NESTOR. O NESTOR apresenta 42 critérios, em que somente um não se verifica no TRAC (critério 8) e um outro não se verifica na ISO 16363:2012 (critério 3.3). Esta discrepância reflete um maior foco, por parte da ISO 16363:2012, em consolidar os termos adoptados de modo a corresponder aos critérios de uma norma ISO. Assim, alguns indicadores foram englobados dentro de outros ou expandidos (e.g. o indicador TRAC A2 é expandido na ISO 16363:2012 em mais dois indicadores: 3.1.2.1 e 3.1.2.2.); suprimidos (e.g. o indicador TRAC A4.2) e acrescentados (e.g. a ISO 16363:2012 acrescenta o indicador 4.3.4).

Constatou-se também que os referenciais partilham a mesma divisão em três secções, referentes à estrutura organizacional, à gestão dos objetos e à infraestrutura e gestão da segurança, sendo que tanto o TRAC como a ISO 16363:2012 se dividem ainda em subsecções, o que se justifica pelo maior nível de granularidade, quando comparados com o NESTOR. Tal permitiu identificar que, no que se refere ao TRAC, no âmbito da primeira secção (24 requisitos), a ISO 16363:2012 não transpõe 2 requisitos referentes à prestação de contas, enquadramento de política e à sustentabilidade financeira (subsecções A.3 e A.4), mais especificamente no que diz respeito à formalização de políticas e procedimentos que assegurem a solicitação e utilização do *feedback* de produtores e utilizadores (critério A3.5) e também sobre a revisão e ajustamento anuais do plano de negócio (critério A4.2). Por seu lado, ainda na primeira secção, o NESTOR não contém 14 requisitos, 1 relativo à estrutura organizacional e recursos humanos (subsecção A.2) e que requer a existência de programas de desenvolvimento profissional que forneçam aos funcionários as habilitações e competências necessárias (A2.3 do TRAC), e 7 critérios relativos à prestação de contas e enquadramento de política (subsecção A.3) que especificam a necessidade da existência de procedimentos e políticas em vigor, e os mecanismos para a sua

revisão e atualização, em que se incluem políticas escritas que especificam os direitos legais necessários para preservar os conteúdos digitais ao longo do tempo e que comprovem a aquisição desses direitos, para garantir a solicitação e utilização do feedback de produtores e utilizadores (critérios A3.2, A3.3 e A3.5), prevendo ainda a existência de um histórico que relate todas as alterações ao funcionamento e tecnologia do repositório, referindo as implicações dessas alterações na preservação do conteúdo digital, e um compromisso com a transparência, responsabilidade e responsabilização, que se verifica em termos de definição, recolha e apresentação de análises à integridade da informação, em sede de programas de autoavaliação e certificação periódica (critérios A3.6, A3.7, A3.8, A3.9).

Quanto à sustentabilidade financeira (subsecção A.4) foram referenciados 4 critérios que requerem planos de negócios analisados e ajustados periodicamente, numa perspectiva de transparência e conformidade com normas e práticas de *accountability* e auditoria, o que inclui análise de riscos, benefícios, investimentos e despesas, para monitorizar e colmatar falhas de financiamento (critérios A4.2, A4.3, A4.4, A4.5), e 2 ligados aos contratos, licenças e compromissos (subsecção A.5) e que requerem que os contratos especifiquem, documentem e transfiram todos os direitos de preservação necessários, caso contrário terá que definir políticas que abordem possíveis questões e perdas ligadas a conteúdo cujos direitos não estejam clarificados (A5.2, A5.5). Um elemento a ressalvar no NESTOR é a existência do requisito de gestão de qualidade (ponto 5), que não aparece explicitado nos outros documentos. Isto significa que se detetou uma equivalência de 91% dos requisitos da ISO 16363:2012 e cerca de 42% do NESTOR relativamente à primeira secção do TRAC.

No âmbito da segunda secção do TRAC (44 requisitos), a ISO 16363:2012 não transpõe 5 requisitos ligados à criação de pacotes para ingestão, armazenamento, preservação e manutenção de AIPs e à gestão do acesso (subsecções B.2, B.4 e B.6) que se referem à preservação de quaisquer identificadores únicos associados aos objetos digitais antes da ingestão (B2.6), a aplicação de estratégias de preservação documentadas (critério B4.1), a implementação de políticas de acesso documentadas que incluem o registo de todas as ações de acesso que se enquadram nos requisitos do repositório e dos produtores/responsáveis pelo depósito da informação, e que devem ser coerentes com os acordos de depósito estabelecidos para os objetos armazenados (critérios B6.2, B6.3, B6.4). Quanto a esta secção do TRAC, o NESTOR não contém 21 requisitos, 3 referentes à aquisição de conteúdo para ingestão (subsecção B.1) que requerem especificamente respostas adequadas ao produtor/depositador em pontos predefinidos do processo de ingestão, provas de quando a responsabilidade de preservação do conteúdo dos SIPs é formalmente aceite, tendo para isso que existir registos das ações e processos relevantes para a preservação (B1.6, B1.7 e B1.8), e 5 critérios ligados à criação de pacotes para ingestão (subsecção B.2), e que requerem registos que comprovem a aceitação do conteúdo do SIP como integrante em AIPs ou a sua eliminação, devendo preservar a ligação entre os AIPs e os identificadores únicos que os conteúdos dos SIP tenham previamente à ingestão, garantindo a existência de recursos para o acesso à informação de representação de autoridade adequada e sistemas de registo de formatos (critérios B2.4, B2.6, B2.7). Para tal é necessário verificar a integralidade e exatidão do AIP quando é gerado, registando todos os procedimentos ligados à criação do AIP que possam influenciar a preservação (critérios B2.11 e B2.13). De igual forma o NESTOR não transporta 2 critérios relativos ao planeamento de preservação (subsecção B.3) que requerem mecanismos de monitorização e notificação de obsolescência ou inviabilidade da Informação de Representação (incluindo formatos), e ainda a prova da eficácia do seu plano de preservação. (B3.2, B3.4)., 3

critérios referentes ao armazenamento e preservação/manutenção dos pacotes de informação de arquivo (subsecção B.4), 1 ligado à gestão da informação (subsecção B.5) para definição de requisitos mínimos de metainformação que permitam à comunidade de interesse recuperar e identificar os recursos que pretendam (B5.1), e 7 relativos à gestão do acesso (subsecção B.6) abordam a necessidade de documentar e informar a comunidade de interesse do repositório acerca das opções de acesso disponíveis, de registo de todas ações de acesso, e da definição e implementação de políticas de acesso consistentes com os contratos de depósito e exigências dos produtores/depositantes e do repositório (B6.1, B6.2, B6.4). Ainda neste âmbito, o TRAC requer o registo das falhas de acesso e que os recursos humanos verifiquem episódios de "negação de acesso" incorretos, comprovativos de que o processo que gera o DIP está completo e correto em relação ao pedido, e que todos os pedidos de acesso resultam numa resposta de aceitação ou rejeição. (B6.6, B6.7, B6.8, B6.9). Para esta secção apurou-se assim, uma equivalência de cerca de 89% da ISO 16363:2012 e de 52% do NESTOR relativamente ao TRAC.

A última secção do TRAC (16 requisitos) é totalmente transposta pela ISO 16363:2012, enquanto que o NESTOR não inclui 8 requisitos, 6 referentes à infraestrutura do sistema (subsecção C.1) ligados à garantia de funcionamento dos sistemas operativos e restante software infraestrutural, garantia essa que se estende para o hardware e software que garante controlo de funcionalidade de backups para os serviços e recursos geridos pelo repositório (C1.1 e C1.2), que tem que gerir o número e localização de cópias de todos os objetos digitais, garantindo a sincronização dessas cópias, tem que reportar todos os casos de corrupção ou perda de dados, e as medidas tomadas de correção/substituição, e definir processos para mudança de suportes de armazenamento e / ou de hardware (C1.3, C1.4, C1.6 e C1.7). O NESTOR não abarca 2 critérios do TRAC relativos à segurança (subsecção C.3), que requerem a definição de funções, responsabilidades e autorizações relacionadas com a gestão de mudança no sistema, e documentação para gestão de risco e planos de recuperação de desastre, que incluam no mínimo, cópias fora do sistema (C3.3 e C3.4). Nesta secção, a equivalência da ISO 16363:2012 é de 100%, contra 50% do NESTOR.

A comparação baseada no NESTOR, identificou que a ISO 16363:2012 somente não inclui um critério referente à primeira secção (16 critérios), sendo esse relativo ao desempenho das funções de arquivo do repositório com base em acordos legais (critério 3.3), e o TRAC não inclui um critério da segunda secção (22 critérios) referente à existência de um plano estratégico para as medidas de preservação técnica (critério 8). Os três critérios da última secção do NESTOR encontram correspondência nos outros referenciais analisados. Estes resultados permitem detetar equivalências a 100% a todas as secções do NESTOR, com exceção da primeira secção com a ISO 16363:2012, cuja equivalência é de cerca de 94% e da segunda secção com o TRAC, cuja equivalência é de 96%.

Finalmente, a análise comparativa da ISO 16363:2012 permitiu identificar 25 critérios na primeira secção, sendo que 3 não se encontram no TRAC, 2 relativos à governação e viabilidade organizacional (subsecção 3.1) que se prendem com a existência de um documento de Plano de Estratégia de Preservação que estipule uma abordagem a longo prazo para o desenvolvimento da sua missão (critério 3.1.2) e um documento de política que especifica o tipo de informação que a entidade detentora do repositório pretende preservar, manter, gerir e fornecer o acesso (3.1.3). Curiosamente, o primeiro critério abordado contém subcritérios que já constam no TRAC, mesmo que só em parte, como é o caso do requisito relativo à monitorização e

colmatação das falhas de financiamento (A4.5), que consideramos estar incluído no requisito referente à monitorização do ambiente organizacional para verificar a necessidade de executar planos de sucessão, de contingência e/ou acordos de garantia (3.1.2.2). O critério referente à prestação de contas e enquadramento de política de preservação (subsecção 3.3) diz respeito à existência de políticas de preservação que estejam em consonância com o cumprimento do Plano de Estratégia de Preservação (3.3.2).

Por seu lado, o NESTOR não contém 11 critérios, sendo 1 relativo à estrutura organizacional e recursos humanos (subsecção 3.2) que requer a existência de programas de desenvolvimento profissional que forneçam aos funcionários as habilitações e competências necessárias (3.2.1.3), e 6 referentes à subsecção 3.3, que especificam a necessidade da existência de políticas de preservação, de procedimentos e políticas em vigor, e os mecanismos para a sua revisão e atualização para garantir o cumprimento do plano estratégico de preservação (critérios 3.3.2, 3.3.2.1). Ainda nesta linha a ISO 16363:2012 prevê a existência de um histórico que relate todas as alterações ao funcionamento e tecnologia do repositório, referindo as implicações dessas alterações na preservação do conteúdo digital, e um compromisso com a transparência, responsabilidade e responsabilização, que se verifica em termos de definição, recolha e apresentação de análises à integridade da informação, em sede de programas de autoavaliação e certificação periódica (critérios 3.3.3, 3.3.4, 3.3.5, 3.36).

Não surgem no NESTOR 2 critérios da ISO 16363:2012 acerca da sustentabilidade financeira (subsecção 3.4) que requerem procedimentos de acordo com uma perspectiva de transparência e conformidade com normas e práticas de *accountability* e auditoria, o que inclui análise de riscos, benefícios, investimentos e despesas, para monitorizar e colmatar falhas de financiamento (critérios 3.4.2, 3.4.3), e outros 2 critérios dizem respeito aos contratos, licenças e compromissos (subsecção 3.5), que requerem que os contratos especifiquem, documentem e transfiram todos os direitos de preservação necessários, caso contrário terá que definir políticas que abordem possíveis questões e perdas ligadas a conteúdo cujos direitos não estejam clarificados (3.5.1.1, 3.5.1.4). Estes resultados permitem detetar uma equivalência do TRAC de 88% e do NESTOR de 56% relativamente à primeira secção da ISO 16363:2012.

Dos 60 critérios da segunda secção, o TRAC não contem 14, 3 referentes à aquisição de conteúdo para ingestão (subsecção 4.1) que requerem que o repositório tenha procedimentos para identificar e registar as características (propriedades) da informação, em conjunto com a informação de conteúdo (ou conteúdo da informação) a preservar (4.1.1.1 e 4.1.1.2) e especificações para reconhecer e analisar os SIPs (4.1.3), e 8 critérios relativos à criação de pacotes de informação de arquivo no âmbito da ingestão (subsecção 4.2), que requerem que o repositório tenha uma definição adequada para a análise e preservação a longo prazo dos AIPs (4.2.1) e ainda a documentação do processo de eliminação final dos SIPs (4.2.3).

Acerca dos identificadores únicos dos AIPs, e no que respeita a regras para a sua geração, requer-se a existência de documentação sobre os processos ligados à alteração, listagem e verificação de duplicação desses identificadores (critérios 4.2.4.1.3 e 4.2.4.1.4), e adequação do sistema de identificadores às necessidades presentes e futuras (critério 4.2.4.1.5). Ainda sobre os identificadores únicos, o serviço de ligação/resolução deve permitir encontrar o objeto digital independentemente da sua localização física (4.2.4.2). Ainda no âmbito da qualidade da Informação de Representação, requer-se a garantia de acesso à informação de representação necessária e que ela está persistentemente associada aos objetos de dados relevantes (critérios

4.2.5.3 e 4.2.5.4).

O TRAC também não contém 1 critério respeitante ao planeamento de preservação (subsecção 4.3) referente a mecanismos para criação, identificação e angariação de Informação Representação adicional em situações de alterações de planos de preservação derivado de monitorização (4.3.3.1), e ainda 2 critérios ligados à preservação dos de pacotes de informação de arquivo (subsecção 4.4) e que requerem a existência de procedimentos (documentados) para todas as ações tomadas sobre os AIPs, e demonstração de que tais ações estão de acordo com as especificações definidas para essas ações (4.4.2.1 e 4.4.2.2).

Por seu lado, o NESTOR não inclui equivalência a 29 critérios da segunda secção da ISO 16363:2012, 5 referentes à subsecção 4.1, e que requerem procedimentos de identificação das propriedades da informação que irá preservar, por forma a garantir um histórico do conteúdo da informação (informação de conteúdo) e das propriedades de Informação a preservar (4.1.1.1, 4.1.1.2). De igual forma devem existir especificações adequadas para o reconhecimento e análise dos SIPs, e respostas adequadas ao produtor/depositador em pontos predefinidos do processo de ingestão e registos das ações e processos de administração relevantes para a aquisição de conteúdo (4.1.3, 4.1.7, 4.1.8).

O NESTOR não contém 13 critérios relativos à subsecção 4.2, que requerem uma definição associada de cada AIP preservado, que seja apropriada para analisar o AIP e apto para as necessidades de preservação a longo prazo, devendo o repositório ter que documentar a eliminação final dos SIPs, e procedimentos documentados para situações em que o SIP não é incorporado no AIP ou rejeitado, referindo o que ocasionou tal situação (4.2.1, 4.2.3, 4.2.3.1). Ainda nesta linha é requerido um sistema de identificadores únicos e persistentes, adequado para atender às necessidades acuais e previstas, com documentação que descreva todos os processos utilizados para possíveis alterações a esses identificadores, listas completas de todos esses identificadores e fazer verificações pontuais para duplicações, e um sistema de serviços de ligação/resolução confiável, de forma a encontrar o objeto independentemente da sua localização física (4.2.4.1.3, 4.2.4.1.4, 4.2.4.1.5, 4.2.4.2). De igual modo, são necessários recursos para garantir a existência de Informação de Representação com qualidade de autoridade dos objetos digitais, por forma a determinar a informação de Representação necessária para tornar os dados do objeto compreensíveis por parte da Comunidade Designada, garantir o acesso à informação de representação necessária, e que esta esteja persistentemente associada aos objetos de dados (4.2.5, 4.2.5.2, 4.2.5.3, 4.2.5.4).

Requer-se ainda a verificação da integralidade e exatidão dos AIPs aquando da sua criação, e o histórico das ações e processos administrativos relevantes para a criação dos AIPs (4.2.8 e 4.2.10). Existem ainda 4 critérios respeitantes à subsecção 4.3 que não surgem no NESTOR e que requerem mecanismos de monitorização e notificação relativos ao seu ambiente de preservação, que alertem para a inadequação da Informação de Representação quando a informação custodiada deixe de ser compreendida por parte da Comunidade Designada, para criar, identificar ou angariar Informação de Representação adicional quando necessário, e ainda prova da eficácia do seu plano de preservação (critérios 4.3.2, 4.3.2.1, 4.3.3.1 e 4.3.4).

A subsecção 4.4 conta com 4 critérios que não transparecem no NESTOR e que requerem a preservação da informação de conteúdo dos AIPs, o registo de todas ações e processos administrativos que sejam relevantes para o armazenamento e preservação dos AIPs, devendo especificar os procedimentos referentes a essas ações, e comprovativos de que tais ações vão ao

encontro dessas especificações (4.4.1.1, 4.4.2, 4.4.2.1 e 4.4.2.2), 1 critério que diz respeito à gestão de informação (subsecção 4.5) para definição de requisitos mínimos de metainformação que permitam à Comunidade Designada recuperar e identificar os recursos que pretendam (4.5.1), e finalmente 2 critérios acerca da gestão do acesso (subsecção 4.6) que abordam a necessidade do registo das falhas de acessos e verificação de episódios de anomalias, e registar e agir sobre indicações de erros nos dados ou nas respostas aos pedidos dos utilizadores. (4.6.1.1, 4.6.2.1).

Arriscando uma perspectiva mais abrangente, poderíamos englobar o conjunto dos requisitos desta subsecção da ISO 16363:2012 em três requisitos do NESTOR, relativos à garantia de acesso aos objetos digitais por parte da Comunidade Designada, na definição dos DIPs e na garantia da transformação dos AIPs em DIPs (2.1, 11.1, 11.2). Para esta secção apurou-se assim, uma equivalência de cerca de 77% do TRAC e de 52% do NESTOR relativamente à ISO 16363:2012.

Quanto aos 24 critérios da última secção da ISO 16363.2012, o TRAC somente não inclui 1 relativo à gestão de risco da infraestrutura técnica (subsecção 5.1) que obriga à identificação e documentação dos processos críticos que afectam o cumprimento das responsabilidades obrigatórias no âmbito da gestão dos riscos das operações e objetivos de preservação associados à infraestrutura do sistema do repositório (5.1.1.6), enquanto o NESTOR não inclui 10 requisitos, 8 na subsecção 5.1 e que requerem a identificação e gestão dos riscos decorrentes das operações e metas de preservação associadas à infraestrutura do sistema, suporte para o hardware e software que garanta controlo de funcionalidade de backups para os serviços e recursos geridos pelo repositório (5.1.1, 5.1.1.2). Assim, o repositório tem que reportar todos os casos de corrupção ou perda de dados, e as medidas tomadas para a sua correção/substituição, processos para registar e agir, com base numa avaliação do risco-benefício, à disponibilidade de novas atualizações de segurança, devendo identificar e documentar os processos críticos que afectam sua capacidade de cumprir com as suas responsabilidades, tem que definir processos para mudança de suportes de armazenamento e / ou de hardware, e gerir o número e localização de cópias de todos os objetos digitais, garantindo a sincronização dessas cópias (5.1.1.3.1, 5.1.1.4, 5.1.1.5, 5.1.1.6, 5.1.2, 5.1.2.1).

Quanto aos 2 critérios não existentes no NESTOR relativos à gestão de risco de segurança (subsecção 5.2) prendem-se com a definição de funções, responsabilidades e autorizações relacionadas com a gestão de mudança no sistema, e documentação para gestão de riscos e planos de recuperação de desastres, que incluam no mínimo, cópias fora do sistema (5.2.3 e 5.2.4). Nesta secção, a equivalência do TRAC é cerca de 96%, contra 58% do NESTOR.

Resumidamente, no âmbito do TRAC, a ISO 16363:2012 e o NESTOR contêm, respectivamente, 24 e 10 critérios da secção acerca do quadro organizacional, 39 e 23 critérios referentes à gestão de objetos, e 16 e 8 critérios ligados à infraestrutura e segurança. No que respeita ao NESTOR, o TRAC e a ISO 16363:2012 contêm, respectivamente, 16 e 15 critérios da secção acerca do quadro organizacional, 16 e 15 critérios referentes à gestão de objetos, e 3 e 3 critérios ligados à infraestrutura e segurança. Em termos de ISO 16363:2012, o TRAC e o NESTOR contêm, respectivamente, 22 e 14 critérios da secção acerca do quadro organizacional, 46 e 31 critérios referentes à gestão de objetos, e 23 e 14 critérios ligados à infraestrutura e segurança.

Julgamos que este estudo comparativo e a tabela que dele resultou permitirão a todas as partes

interessadas em repositórios digitais aferir destes referenciais normativos os critérios que consideram indispensáveis para a sua avaliação, e/ou se eles são suficientes para garantir a confiabilidade dos mesmos.

Pretende-se no futuro avançar para a comparação de outros referenciais, tais como:

- Data Seal of Approval
- European Framework for Audit and Certification of Digital Repositories no âmbito dos repositórios digitais,
- ISO/IEC 15504 Information technology — Process assessment, COBIT's Process Assessment Model,
- MoREQ 2010: Model Requirements for the Management of Electronic Records
- ISO 16175: Information and documentation – Principles and functional requirements for records in electronic office environments
- ISO 18128: Information and documentation – Risk assessment for records processes and systems
- ISO 30301: Information and documentation – Management systems for records – Requirements
- ISO 38500: Corporate governance of information technology
- ISO 27001: Information security management, relativos à questões da tecnologia, da gestão documental e dos processos de negócio.

Referências

BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories [Em linha]. v.2. Frankfurt am Main: Network of Expertise for Long-Term STORage and Long-Term Accessibility of Digital Resources in Germany (NESTOR) Working Group Trusted Repositories - Certification, 2009. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://files.d-nb.de/nestor/materialien/nestor_mat_08_eng.pdf>.

CORUJO, Luis – Repositórios Digitais e Confiança – Um exemplo de repositório de Preservação Digital: o RODA. Lisboa: FLUL, 2014. Tese de Mestrado em Ciências da Documentação e Informação da Faculdade de Letras da Universidade de Lisboa.

ISO 14721:2012, Space data and information transfer systems: Open archival information system (OAIS) - Reference model. Geneva. ISO

ISO 16363:2012, Space data and information transfer systems: Audit and certification of trustworthy digital. Geneva. ISO

YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development. Archival science. [Em linha]. Vol. 14, nº 1 (2014), p. 17-34 [Consult. 6 Abril. 2014]. Disponível na Internet: <URL: http://link.springer.com/article/10.1007%2Fs10502-013-9207-8>. ISSN 1573-7519.