UNIVERSIDADE DE LISBOA
FACULDADE DE LETRAS

Repositórios Digitais e Confiança

Um exemplo de repositório de Preservação Digital: o RODA

Luis Miguel Nunes Corujo

Dissertação
Mestrado em Ciências da Documentação e Informação
Área de Especialização: Arquivística

2014

UNIVERSIDADE DE LISBOA
FACULDADE DE LETRAS

Repositórios Digitais e Confiança

Um exemplo de repositório de Preservação Digital: o RODA

Luis Miguel Nunes Corujo

Dissertação orientada
pelo Professor Doutor Paulo Alberto Farmhouse e
pelo Professor António Gil Matos

Mestrado em Ciências da Documentação e Informação
Área de Especialização: Arquivística

2014

“There are 10 kinds of people. Those who understand
binary notation, and those who do not.”

Sumário

Índice de Ilustrações

Dedicatória

Em homenagem à minha família, particularmente ao meu pai e à minha mãe, pelo carinho, amparo absoluto e valores que continuamente me passaram, e que continuam a ser pilares estruturantes da minha vida.

Ao meu irmão, amigo, conselheiro confidente e companheiro, um verdadeiro *alter-Ego* da minha pessoa.

Um tributo muito especial à minha mulher, aquela molécula de carbono indispensável à sobrevivência do meu Ser. Pelo Amor, apoio, e pela sua jovialidade contagiante e forma de ver a Vida, e que me desafia a abrir-me ao Mundo.

A todos os meus amigos, colegas, companheiros e conhecidos que passaram pela minha vida, estejam ou não presentes nela, pela marca que deixaram não só na minha memória, mas também na minha vida.

Agradecimentos

Aos meus professores, verdadeiros Mestres do Conhecimento, muito particularmente ao Mestre Francisco Barbedo, pelos desafios e apoio que me tem concedido, desde o curso de especialização, passando pelo Arquivo Distrital do Porto e pela Direcção-Geral de Arquivos. Um verdadeiro exemplo de competência e profissionalismo descomprometido.

Aos meus amigos e colegas da Torre do Tombo (independentemente do nome do organismo ou instituição que alberga o edifício!) e Arquivos Distritais (especialmente no do Porto e o de Braga), pelos ensinamentos e pela forma como me ensinaram a vivenciar a prática arquivística, bem longe de "academismos empoeirados". A lista é longa, mas estão bem presentes na minha lembrança. Foi uma regalia a oportunidade de ter trabalhado convosco. Estes organismos foram e continuam a ser a minha *Alma Mater*.

Aos meus amigos e colegas da Comunidade do RODA, Miguel Ferreira, Luis Faria e Rui Castro, por suportarem as minhas infindáveis questões e pedidos.

Aos meus amigos e colegas da Faculdade de Letras da Universidade de Lisboa, especialmente aos Professores António Gil Matos, Carlos Guardado da Silva, Jorge Revez e Paulo Alberto Farmhouse, pela força e incentivo.

Às minhas amigas e colegas de trabalho da Biblioteca da Faculdade de Ciências da Universidade de Lisboa, nomeadamente a Margarida Pino, a Ana Fraga e Teresa Boa, pelo cuidado e atenção que tiveram a escutar as minhas dúvidas.

Aos meus amigos e familiares que tiveram a paciência de me acompanhar na produção deste trabalho, e de todas as incertezas, apreensões e anseios ao longo desta lide, manifesto o meu mais sincero e profundo reconhecimento.

Resumo

Este trabalho pretende situar os repositórios digitais no seio da Preservação Digital e analisar como estes podem ser considerados dignos de confiança por parte dos seus utilizadores. Nesse sentido são abordadas normas e outros documentos com requisitos que têm como fim a certificação, como elementos que promovem e reforçam a confiança nos repositórios digitais, sendo proposta uma comparação entre o TRAC, a ISO 16363:2012 e o NESTOR. Neste âmbito é igualmente apresentado o RODA, repositório orientado para a preservação digital a longo prazo, aventando-se a sua avaliação com base nos requisitos propostos pelos referidos documentos.

PALAVRAS-CHAVE:

Preservação Digital; Repositório Digital; Objecto Digital; Confiança; Certificação; OAIS; TRAC; ISO 16363:2012; NESTOR; RODA; Informação Electrónica

Abstract

This work aims to place the digital repositories within the Digital Preservation subject, and analyze how these can be considered trustworthy by their users. In this sense, it addresses standards and other documents that present requirements as an end for certification, and as elements that promote and strengthen the trust in digital repositories, also including a comparison proposal between the TRAC, the ISO 16363:2012, and the NESTOR standards. Also in this context is presented the RODA, a long-term preservation-oriented digital repository, venturing its assessment based on the requirements proposed by the said documents.

KEYWORDS :

Digital preservation; Digital Repository; Digital Object; Trust ; Certification; OAIS; TRAC; ISO6363:2012; NESTOR; RODA; Electronic Information

Siglas

AIP – Archival Information Package

ALA - American Library Association

APBAD – Associação Portuguesa de Bibliotecários, Arquivistas e Documentalistas

ASCII - American Standard Code for Information Interchange

BNF - Bibliothèque Nationale de France

CCSDS - Consultative Committee for Space Data Systems

CEDARS - CURL Exemplars in Digital Archives

CLIR - Council on Library and Information Resources

CNES - Centre National d'Études Spatiales

CPA - Commission on Preservation and Access

CRL - Center for Research Libraries

DAE - Documento de Arquivo Electrónico

DANS - Data Archiving and Networked Services

DGArq – Direcção-Geral de Arquivos

DGLAB – Direcção-Geral do Livro, Arquivo e Bibliotecas

DINI – Deutsche Initiative für NetzwerkInformation. (German Initiative for Network Information)

DIP - Dissemination Information Package

DCC - Digital Curation Centre

DLM Forum - Document Lifecycle Management (até 2002 era *Données Lisibles par Machine*)

DPC - Digital Preservation Coalition

DPE – Digital Preservation Europe

DSA - Digital Seal of Approval

DRAMBORA - Digital Repository Audit Method Based on Risk Assessment

EAD – Encoded Archival Description

EESSI - European Electronic Signature Standardization Initiative

GDFR - Global Digital Format Registry

HATII - Humanities Advanced Technology and Information Institute

HTML - HyperText Markup Language

IAN/TT – Instituto dos Arquivos Nacionais/Torre do Tombo

iARQ - informação de arquivo

ICA – International Council of Archives

ICPSR - Inter-University Consortium for Political and Social Research

IDA - Interchange of Data between Administrations

IFLA - International Federation of Library Associations

InterPARES - International Research on Permanent Authentic Records in Electronic Systems

JISC - Joint Information Systems Committee

KNAW - Netherlands Academy of Arts and Sciences

LOC – Library of Congress

MIT - Massachusetts Institute of Technology

METS - Metadata Encoding and Transmission Standard

MoReq - Modular Requirements for Records Systems (até 2010 era *Model Requirements for the Management of Electronic Records*)

NAA - National Archives of Australia

NARA - National Archives and Records Administration

NASA - National Aeronautics and Space Administration

NEDLIB - Networked European Deposit Library

NIST - National Institute of Standards and Technology

NLA - National Library of Australia

NWO - Netherlands Organization for Scientific Research

OAIS - Open Archival Information System

OCLC - Online Computer Library Center

OD – Objecto Digital

PDI - Preservation Description Information

PPD – Plano de Preservação Digital

PREMIS - Preservation Metadata: Implementation Strategies

PRO - Public Record Office

RAMP - Records and Archives Management Programme

RCAAP - Repositório Científico de Acesso Aberto de Portugal

RLG - Research Libraries Group

SI – Sistema da Informação

SIADE - Sistemas de Informação de Arquivo e Documentos Electrónicos

SIG - Sistemas de Informação Geográfica

SIP - Submission Information Package

SPARC - Scholarly Publishing & Academic Resources Coalition

TI – Tecnologia da Informação

UDFR - Unified Digital Format Registry

UML - Unified Modeling Language

UNESCO - United Nations Educational, Scientific and Cultural Organization

UTF - Unicode Transformation Format

UVC - Universal Virtual Computer

XML - eXtensible Markup Language

1 - Introdução

> *"Unfortunately, we cannot guarantee the continued preservation and accessibility of digital information generated in this context of rapid technological advances. Despite our information technology investments, there is a critical, cumulative weakness in our information infrastructure. Long-term preservation of digital information is plagued by short media life, obsolete hardware and software, slow read times of old media, and defunct Web sites. Indeed, the majority of products and services on the market today did not exist five years ago. More importantly, we lack proven methods to ensure that the information will continue to exist, that we will be able to access this information using the available technology tools, or that any accessible information is authentic and reliable."*[1]

Podemos constatar que os principais problemas decorrentes da produção, utilização e manutenção de informação electrónica passam pela ausência de percepção social/organizacional ou, pelo contrário, pelo excessivo sentido de individualização, perda de informação operacional, perda de informação-memória e perda de valor evidencial, o que compromete a responsabilização de conduta e actividades. Outros problemas passam pela dificuldade de gestão dessa informação, a nível do seu armazenamento, recuperação e localização, identificação e controlo. Do ponto de vista técnico, os problemas surgem em termos de obsolescência tecnológica, do *hardware*, do *software*, dos formatos, dos suportes de armazenamento, dos danos e desgaste físicos, e ainda do fenómeno do *bit rot,* ou corrupção de dados no suporte[2]. Estes problemas levam à ilegibilidade, impossibilidade de acesso e mesmo desaparecimento físico dos objectos digitais.

Sabendo que esta informação é operacionalmente necessária durante períodos mais ou menos longos, torna-se necessário empreender acções para manter a sua legibilidade. Verifica-se no caso dos formatos, que um formato de ficheiro pode ser ultrapassado por outro ou tornar-se mais complexo, que o formato não "pega" (não é utilizado pela possível comunidade de interesse) ou as empresas não criam *software* compatível, ou que o formato falha, estagna, ou já não é compatível com os sistemas actuais. No caso do *software*, este pode falhar comercialmente ou inclusivamente a empresa que o produz ser adquirida por um competidor que o retira do mercado. Entre os elementos que afectam os suportes e o *hardware* contam-se a instabilidade do material, as condições ambientais de armazenamento, os efeitos de manuseamento e utilização, desastres naturais, as falhas infra-estruturais e a manutenção inadequada. A obsolescência do *hardware* é uma constante desta indústria devido aos avanços tecnológicos a nível de velocidade do processador, densidade dos chips de memória, capacidade dos periféricos de armazenamento, velocidade de processamento de imagem e velocidade de transmissão. Tais alterações levam à rápida substituição dos suportes, não só devido à maior rapidez, capacidade e produtividade disponíveis, mas também devido ao cada vez maior número de funções oferecidas. Elementos como a diminuição do tamanho físico, o

[1] CHEN, Su-Shing - The paradox of digital preservation. p. 1.
[2] Cft. SALTER, Jim - Bitrot and atomic COWs; Wikipedia contributors – Bit rot; e RAYMOND, Eric - Bit rot.

aumento da capacidade e diminuição do custo por unidade de armazenamento, as tendências em termos de fragilidade, estabilidade, segurança e duração antes da obsolescência, levam a novas e melhores aplicações de *software*, que aumentam a probabilidade de obsolescência do equipamento anterior[3]. Enquanto os fabricantes de todas estas tecnologias competem, emergem, unem-se ou desaparecem, torna-se cada vez mais difícil a manutenção dos conteúdos digitais ao longo do tempo.

Num mundo em rápido desenvolvimento tecnológico terão as instituições responsáveis pelo património digital a capacidade de assegurar a sua preservação, fornecer o acesso e permitir a utilização da documentação a longo prazo? Conseguirão estas instituições assegurar aos documentos digitais as mesmas características de fidedignidade, integridade e autenticidade face aos tradicionais documentos em papel? Poderão os autores e utilizadores dos repositórios digitais, as entidades financiadoras de projectos digitais, e a comunidade em geral, confiar na capacidade das instituições para gerir e preservar a documentação digital?

Sendo estas características abordadas ao longo deste trabalho, impõe-se a definição de cada uma delas. Considera-se assim que, a integridade de um documento de arquivo refere-se a este permanecer completo e inalterado. No caso dos objectos digitais, esta inalterabilidade é percepcionada como inexistência de modificações não intencionais (humanas ou técnicas). A autenticidade diz respeito à garantia de prova de que o documento de arquivo é aquilo que pretende ser, de ter sido produzido ou enviado pelo alegado produtor ou remetente, e de ter sido produzido ou enviado no alegado momento de produção ou envio. Tal implica a possibilidade de confirmar a sua origem ou proveniência e percurso. A usabilidade ou disponibilidade prende-se com o facto de o documento ser utilizável, ou seja, que pode ser localizado, recuperado, apresentado e interpretado. A fidedignidade (ou confiabilidade) é a propriedade do documento que é digno de crédito enquanto representação completa e fiel das transacções, actividades ou factos que atesta. Esta característica está intimamente ligada com a confiança, assunto que será abordado mais profundamente em capítulo próprio.[4]

Estas são algumas questões que se têm vindo a colocar nas últimas três décadas, desde que várias organizações assumiram definitivamente a sua adesão aos formatos digitais para a produção, gestão e guarda dos seus documentos, sejam eles nado-digitais ou digitalizados. A questão da confiança é central quando se trata de informação em suporte digital, e a tentativa de responder a questões como as anteriores trouxe para o debate na comunidade científica a necessidade de assegurar a confiabilidade dos repositórios digitais.

Pretende-se neste trabalho:

- demonstrar que os repositórios digitais não são apenas um veículo de transmissão de informação, mas que também são uma solução de sistematização de preservação digital;
- demonstrar que a certificação pode ser uma solução possível para garantir a confiabilidade dos repositórios digitais;

[3] BARBEDO, Francisco; CORUJO, Luis; SANT'ANA, Mário – Recomendações para a produção de planos de preservação digital, p. 29-31.
[4] NP 4438-1:2005, Informação e Documentação - Gestão de documentos de arquivo, p. 14-15.

- apresentar a comparação entre alguns documentos normalizadores com critérios que pretendem ser veículo de certificação (TRAC; ISO 16363:2012; NESTOR);

- demonstrar qual o grau de cumprimento do RODA (Repositório de Objectos Digitais Autênticos) perante os critérios desses documentos.

A abordagem perspectivada para este trabalho foi de carácter essencialmente diacrónico, e do geral para o particular. Pretende-se assim inferir dos desenvolvimentos registados ao longo das últimas décadas na área da Preservação Digital, a demonstração 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. Por esse motivo se considera igualmente que a apresentação que parte da conservação em geral, passa pelas problemáticas da preservação digital, pelos repositórios digitais, e dentro destes o Modelo de Referência OAIS, como caminho e aprofundamento para a certificação de repositórios que se pretendem confiáveis, no âmbito dos quais surge o RODA, sistema em constante evolução, desenvolvimento e actualização como forma de cumprimento dos requisitos de certificação pelos quais é avaliado. Assim, a organização deste trabalho está configurada da seguinte forma: considerando o primeiro capítulo esta Introdução, o segundo capítulo aborda a problemática da preservação no âmbito digital e o objecto em que se foca a preservação digital. Nesse âmbito apresentam-se as estratégias e o quadro teórico de referência de preservação de objectos digitais, e finalmente com o Modelo de Informação de Preservação Digital. Este capítulo permite introduzir a preservação de objectos digitais, de forma que no terceiro capítulo se demonstre que a preservação sistematizada desses objectos só é verdadeiramente passível em repositórios digitais. Nesse sentido aborda-se a questão do conceito e definição dos repositórios. Sendo o termo repositório algo vago e, numa altura que estrangeiros avaliam a produção científica portuguesa (nalguns casos referentes a disciplinas do saber com características específicas, como é o exemplo da História), tendo por base critérios mais ligados à quantidade do que à qualidade das publicações, os repositórios de artigos científicos assumem real importância, devendo haver cuidado no que diz respeito aos atributos de descrição, usados para referenciação dos artigos científicos, como forma de atenuar de certa forma o problema de publicar sem ser em inglês. Este capítulo refere-se aos repositórios digitais, aos âmbitos de utilização, como repositórios/arquivos digitais (não deixando de lado a questão do Acesso Aberto), e as particularidades dos repositórios institucionais e temáticos e ainda das Bibliotecas Digitais. O quarto capítulo apresenta o Modelo de Referência OAIS, com os seus modelos de Ambiente Externo, de Informação, e o Funcional. De igual forma abordam-se áreas para desenvolvimento de normas relacionadas com o modelo OAIS, algumas das quais intimamente ligadas à Certificação, questão esta que é aprofundada no quinto capítulo relativo à Confiança. Este capítulo aborda conceptualmente a confiança, particularmente quando derivada de documentos normalizadores, com atributos, requisitos, critérios e métricas para auditoria, avaliação, planeamento e certificação de repositórios, sem esquecer o ponto de vista dos utilizadores dos repositórios digitais, na medida em que tais documentos devem ser reconhecidos pela(s) comunidade(s) de produtores e utilizadores. Factores como definição de estratégias e análise de riscos, monitorização, auditoria e certificação são aspectos que promovem a confiança, e que fazem parte da preservação digital, e, logo, dos repositórios digitais. Um dos possíveis cúmulos da

confiança nos repositórios digitais seria a gestão e manutenção a médio-longo prazo das propriedades arquivísticas de documentos de arquivo com assinatura electrónica. O sexto capítulo aborda o RODA, falando da sua origem, evolução e elementos constituintes. Este repositório digital teve como base o modelo de referência OAIS (abordado no quarto capítulo) e foi alvo de avaliação por parte de um documento normalizador para auditoria e certificação (TRAC), abordado no quinto capítulo. O conteúdo destes capítulos vai permitir apresentar uma comparação entre três documentos para certificação (TRAC, ISO 16363:2012 e NESTOR), e será acompanhada de um quadro comparativo anexo e que foi produzido no âmbito deste trabalho. Ainda neste capítulo proceder-se-á à apresentação dos resultados da avaliação do RODA com base nestes mesmos documentos.

2 - Preservação Digital

O assustador texto de Terry Kuny *A Digital Dark Ages? Challenges in the Preservation of Electronic Information*[5], de 1997, representa uma tomada de consciência, no início da eufórica expansão da Internet, símbolo da preponderância que as tecnologias electrónicas da informação e comunicação estavam a assumir nos vários domínios da vida das pessoas, das organizações, da sociedade. Contra a sedutora utopia anunciada pelos evangelistas e gurus informáticos, Kuny anunciava sensatamente que era necessário estudar o impacto destas tecnologias na Sociedade e garantir a preservação da História e do património criado nesta Era, sob o risco de se perder a sua memória. Afirmando que não existiam soluções sustentadas para os problemas da preservação digital, o autor apontava linhas de acção a seguir e que especialistas e profissionais estavam habilitados para garantir que não entraríamos numa Idade das Trevas Digital.

Precisamos então de saber o que significa preservação digital, qual o seu objecto, e de que forma opera sobre esse objecto.

Conway afirma que "*simply defining what preservation means in the digital imaging environment is a challenge*[6]". O conceito de preservação digital requer assim uma análise dos termos utilizados à luz da área científica. Esta abordagem assentará em normas e bibliografia indicada ao longo do texto. Não se insere no âmbito deste trabalho a pretensão de analisar a evolução dos modelos teóricos nem dos paradigmas ligados à preservação e conservação, uma vez que se considera que esse estudo, por si só, requer um trabalho dedicado e autónomo.

Preservação …

O conceito de Preservação é utilizado muitas vezes de maneira indiscriminada, gerando-se confusão com outros termos como Conservação e Restauro, sendo necessário a distinção destes três termos. Azevedo Pinto refere que, "*Relativamente à definição de preservação e conservação, é um facto a associação destes conceitos, sobretudo no último quartel do século XX*."[7] De acordo com Maria Luísa Cabral:

> "*Durante muito tempo, preservação significava o restauro das espécies correspondendo, portanto, a uma intervenção pontual, desarticulada do contexto mais geral, que tinha em vista a prossecução dos objectivos da biblioteca que são fundamentalmente facultar o acesso à informação*(...)"[8]

Verifica-se então que o tratamento era feito erraticamente e sem qualquer planeamento, sugerindo uma postura de "apagar os pequenos fogos diários" sem qualquer estratégia de

[5] KUNY, Terry - A digital dark ages?, 1999.
[6] CONWAY, Paul - Preservation in the digital world, 1996.
[7] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 33.
[8] CABRAL, Maria Luísa – Amanhã é sempre longe de mais, p. 17.

fundo. Adicionalmente, a conservação impunha-se à preservação, sendo mesmo sua parte integrante, como se atesta no *Traditional restoration techniques: a RAMP study*[9]*:*

> *"There are two types of action in the conservation of materials:*
> *(a) Preventing deterioration (preservation)*
> *(b) Repairing damage (restoration)"*

A publicação portuguesa, em 1992, dos *Princípios para a Preservação e Conservação de Espécies Bibliográficas* da IFLA[10] (original de 1986) já indica que a "*Preservação engloba todos os aspectos financeiros e de gestão incluindo a armazenagem em todos os aspectos, questões de pessoal, política, técnica e métodos envolvidos na preservação de espécies bibliográficas e a informação que elas contenham"*; a Conservação "*engloba políticas e práticas específicas necessárias à protecção das espécies bibliográficas relativamente à deterioração, destruição e envelhecimento, incluindo os métodos e as técnicas propostas pelo pessoal técnico"*; e o Restauro "*diz respeito às técnicas e critérios utilizados pelo pessoal técnico envolvido no processo de tratamento de espécies bibliográficas, deterioradas pelo tempo, uso ou outros factores"*. Constata-se assim, e de acordo com Maria Luísa Cabral, que "(...) *Aos poucos, foi-se compreendendo que esta intervenção, espécie a espécie, constituía uma corrida contra o tempo, corrida que os técnicos de biblioteca perdiam sempre.* (...)"[11]. Estes termos começam assim a ser tratados como problemáticas independentes mas que fazem parte de uma política específica da própria biblioteca e das preocupações de quem as gere.

Analogamente, no Dicionário de Terminologia Arquivística, publicação portuguesa de 1993 que visava ser o equivalente português do *Dictionary of Archival Terminology* do Conselho Internacional de Arquivos (ICA) de 1984 e 1988, a Conservação surge com duas definições: "*Função do arquivo que consiste em assegurar a custódia e preservação dos arquivos*, e como *Conjunto de medidas de intervenção sistemática e directa nos documentos com o objectivo de impedir a sua degradação, sem alterar as características físicas dos suportes"*[12]*. R*efere também que Preservação é o "*conjunto de medidas de gestão tendentes a neutralizar potenciais factores de degradação dos documentos"*[13], e que Restauro é o conjunto de técnicas utilizadas para a recuperação dos suportes e/ou eliminação dos danos causado na documentação pelo tempo, uso ou outros factores. Implica intervenção e tratamento do documento.

No âmbito destes dois documentos, Manuela Azevedo Pinto na sua obra *PRESERVMAP*, de 2009, identifica uma sintonia nas definições do termo Preservação[14], no que se refere à associação do termo gestão à preservação.

No quadro normativo nacional, já no século XXI, são dignas de menção a norma de Terminologia Arquivística NP 4041[15], de 2005, e a Norma de Gestão de Documentos de

[9] VIÑAS, Vicente; VIÑAS, Rute - Traditional restoration techniques, p. 2.
[10] DUREAU, J. M.; CLEMENTS, D. W. G. – Princípios para a preservação e conservação de espécies bibliográficas, 1992.
[11] CABRAL, Maria Luísa – Amanhã é sempre longe de mais, p. 17.
[12] ALVES, Ivone [*et al.*] – Dicionário de terminologia arquivística, p. 23-24.
[13] ALVES, Ivone [*et al.*] – Dicionário de terminologia arquivística, p. 76.
[14] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 31.

Arquivos NP 4438, de 2005, correspondente à norma ISO 15489:2001[16]. A NP 4041 apresenta a Preservação como sendo a "*aplicação de medidas e procedimentos tendentes a prevenir a degradação física dos documentos e a garantir a sua segurança contra acidentes e intrusões*"[17], o que é corroborado pela definição de preservação fornecida pela NP 4438, ou seja, "*processos e operações necessárias para assegurar a sobrevivência de documentos autênticos através do tempo*"[18]. No que se refere à Conservação, a NP 4041, define-a como "*função primordial do serviço de arquivo que tem por objectivo assegurar a manutenção das características essenciais dos arquivos/documentos de modo a garantir a sua eficácia através do tempo. Exerce-se mediante recurso à avaliação, recolha, custódia, preservação, conservação física, restauro e tratamento arquivístico*"[19]. A mesma Norma indica que o Restauro é o "*conjunto de técnicas utilizadas na recuperação e/ou consolidação dos suportes. Implica intervenção e tratamento do documento*"[20].

A publicação do *Dicionário do Livro* em 2008 apresenta a definição de Conservação como o "*conjunto de técnicas que, através de materiais de boa qualidade, têm como finalidade preservar o objecto*"[21], e liga-o à preservação e protecção. Esta definição é aprofundada na definição de Conservação de Documentos, "*nome dado ao conjunto de processos que visam a estabilização mecânica e química dos materiais constituintes do documento gráfico. Conjunto de medidas destinadas a manter em boas condições um acervo bibliográfico ou outro, com vista a garantir que se mantenha a sua forma original. Acções iniciais para conter o processo de degradação de um documento; centram-se em operações de protecção ao documento, como limpeza e manutenção de condições ideias de armazenamento que contribuam para garantir a sua integridade (…)*"[22]. O mesmo Dicionário definiu preservação como a "*função de providenciar cuidados adequados à protecção e manutenção do acervo bibliográfico e documental de qualquer espécie, com vista a manter a sua forma original. Medidas colectivas e individuais tomadas no respeita à reparação, restauro, protecção e manutenção do património bibliográfico*"[23]. Por sua vez o Restauro é definido como uma "*intervenção levada a cabo sobre um bem cultural degradado ou danificado, determinada pela necessidade de conservar a informação histórica de que ele é veículo e de lhe restituir a funcionalidade no todo ou em parte. No caso dos materiais gráficos, consiste em eliminar de um livro ou documento os estragos causados pelo tempo, manuseamento e incúria do homem; é um trabalho complexo e delicado, que vai do simples desmanchar, lavar, desacidificar, remendar, reforçar o papel e fortalecer as folhas ao refazer da encadernação; o respeito crescente dos bibliófilos pelo estado original da obra, torna-os cada vez mais reticentes em relação à reparação dos livros antigos e prudentes na aquisição de espécies restauradas, cujo resultado final não teve êxito*"[24]. Remete ainda para a Substituição de partes danificadas, para a Reconstrução e Reparação.

---

[15] NP 4041:2005, Informação e Documentação - Terminologia arquivística: Conceitos básicos.
[16] ISO 15489-1: 2001, Information and documentation - Records management.
[17] NP 4041:2005, Informação e Documentação - Terminologia arquivística: Conceitos básicos, p. 14.
[18] NP 4438-1:2005, Informação e Documentação - Gestão de documentos de arquivo, p. 10.
[19] NP 4041:2005, Informação e Documentação - Terminologia arquivística: Conceitos básicos, p. 11.
[20] NP 4041:2005, Informação e Documentação - Terminologia arquivística: Conceitos básicos, p. 14.
[21] FARIA, Maria Isabel; PERICÃO, Maria da Graça - Dicionário do Livro, p. 303.
[22] FARIA, Maria Isabel; PERICÃO, Maria da Graça - Dicionário do Livro, p. 303-304.
[23] FARIA, Maria Isabel; PERICÃO, Maria da Graça - Dicionário do Livro, p. 997.
[24] FARIA, Maria Isabel; PERICÃO, Maria da Graça - Dicionário do Livro, p. 1081.

Nesta panorâmica podemos ver a evolução terminológica, tentando-se fazer uma destrinça conceptual. Para, Manuela Azevedo Pinto estas definições revelam um "*enfoque na custódia, na protecção física,* (…) *na manutenção da forma original, necessidade de controlo ambiental/ou tratamento físico e/ou químico*[25]*"*, sendo ainda necessário distinguir claramente o que é preservação e o que é conservação e a sua relação, uma vez que "(...) *esta relação caracterizou-se pela inexistência de contornos claros e objectivos"*[26]. Neste sentido a autora avança com uma definição de Preservação, que considera ser:

> *"intrínseca à função de Gestão, seja a nível institucional, seja a nível intermédio* (…), *devendo ser pensada no longo prazo e em termos de politicas, planos e programas, recursos e estrutura orgânica/funcional que os suporte, tendo, consequentemente, implicações quer na fixação da Missão da organização, quer nos objectivos (estratégicos e operacionais), quer nas metas fixadas, quer, ainda, nas acções/actividades e projectos planeados para os efectivar."*[27]

Ainda segundo a autora, após definida a estratégia de preservação, será a sua concretização ou operacionalização que vai contar com os contributos do domínio da componente técnica, da Conservação, com a aplicação de procedimentos, medidas e técnicas de protecção de cariz mais preventivo, e o Restauro, que, de forma complementar, lidaria com o tratamento e recuperação. Esta definição vai de encontro ao estipulado por Conway:

> "*Preservation is the acquisition, organization, and distribution of resources to prevent further deterioration or renew the usability of selected groups of materials. The essence of preservation management is resource allocation* (…) *Preservation management includes an ongoing, iterative process of planning and implementing prevention activities (e.g., maintaining a stable, safe, and secure environment, ensuring disaster preparedness, and building a basic collection-level maintenance program) and renewal activities (e.g., undertaking conservation treatments, replacing the content of library materials, or reformatting them on microfilm)."*[28]

Cremos que, independentemente de qualquer modelo empírico e/ou teórico ou de qualquer paradigma, estas definições especificam declaramente os termos em apreço.

… Digital

Por seu lado, o termo digital, assumido como adjectivo da preservação, afigura-se como de difícil concordância numa definição única por parte dos cientistas da computação. De acordo com Rothenberg, normalmente diz respeito a um conjunto de dispositivos de transmissão, processamento ou armazenamento de sinais digitais que usam valores discretos (descontínuos). No contexto em que nos apresentamos, geralmente significa qualquer meio de representação de sequências de valores simbólicos discretos - cada valor tem dois ou mais estados inequivocamente distintos - para que estas sequências possam, pelo menos em princípio, ser acedidos, manipulados, copiados, armazenados, e integralmente transmitidos

[25] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 32.
[26] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 33.
[27] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 34.
[28] CONWAY, Paul - Preservation in the digital world, 1996.

por meios mecânicos com elevado grau de fiabilidade.[29] Pelo contrário, os sistemas não-digitais (ou analógicos) utilizam um intervalo contínuo de valores para representarem informação. Embora as representações digitais sejam discretas, a informação representada pode ser discreta, como números, letras, ou ícones, ou contínua, como sons, imagens, outras medidas de sistemas contínuos.[30] Outros exemplos de sistemas digitais são, para além dos sistemas binários electrónicos que utilizam na computação e na electrónica, por exemplo, o ábaco, os faróis, os semáforos, o código de morse, o Braille…

Bannat-Berger dos *Archives de France*, afirma que o domínio do digital se caracteriza por:

> *"Évolutions d'une rapidité spectaculaire, capacité de traitement en constante augmentation, progression géométrique des capacités de stockage et de transport, obsolescence des technologies."*[31]

Esta definição não nos traz muito conforto para entender o que é a preservação digital, uma vez que parece ser oposta à pretensão do que a preservação se propõe fazer, mas serve de ponto de partida para encontrar a resposta para essa questão na literatura.

Encontramos tanto a nível internacional como nacional um conjunto de definições:

Margaret Hedstrom [1997] - planeamento, alocação de recursos e aplicação de métodos e tecnologias de preservação necessárias para garantir que a informação digital de valor, seja esta nadodigital ou produto de digitalização, se mantêm continuadamente acessível e utilizável, sendo que com o uso do termo continuadamente pretende afastar-se do idealismo e absolutismo do termo "permanente".[32]

BEAGRIE, Neil & GREENSTEIN, Daniel (1998) - processo distribuído que inclui um conjunto de diferentes partes interessadas que lidam com recursos digitais em determinadas fases do seu ciclo de vida. Para aumentar as probabilidades da preservação digital e reduzir custos, as diferentes partes interessadas necessitam de estar mais conscientes de como o seu envolvimento com um recurso digital influencia o seu ciclo de vida.[33]

CEDARS - RUSSEL, Kelly & SERGEANT, Derek (1999) - armazenamento, manutenção e acesso a longo prazo de um objecto digital, normalmente como consequência da aplicação de uma ou mais estratégias de preservação, incluindo a preservação de tecnologia, a emulação, ou a migração de dados.[34]

Rothenberg (2000) - a dificuldade da definição de uma estratégia de preservação viável prende-se em parte com a nossa falha de compreensão e avaliação das questões de autenticidade à volta das entidades informacionais digitais e a implicação dessas questões em possíveis soluções técnicas para o problema da preservação digital. O impacto da

[29] ROTHENBERG, Jeff - Preserving authentic digital information, p. 52.
[30] TOCCI, Ronald; WIDMER, Neal; MOSS, Gregory - Digital systems: principles and applications, 2007.
[31] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 23.
[32] HEDSTROM, Margaret - Digital preservation: a time bomb for digital libraries.
[33] BEAGRIE, Neil; GREENSTEIN, Daniel – A strategic policy for creating and preserving digital collections, p. 5.
[34] RUSSEL, Kelly; SERGEANT, Derek - The CEDARS project : implementing a model for distributed digital archives, 1999.

autenticidade na preservação manifesta-se em termos de usabilidade, nomeadamente quando uma entidade informacional preservada só pode ser usada nos âmbitos pretendidos ou requeridos somente se a sua autenticidade estiver preservada. Não existe uma definição de preservação digital que garanta a salvaguarda de todas as características de tais identidades.[35]

APBAD - Manifesto para a Preservação Digital, Cecília Henriques (2002) – "*capacidade do objecto preservado cumprir com as suas funções para que foi produzido, no âmbito da sua utilização, ou seja, a manutenção da autenticidade e acessibilidade do e ao objecto preservado, o que implica compromissos de investimento durante todo o ciclo de vida do documento, caso contrário redundará em perdas irremediáveis e inutilização do esforço anterior."*[36]

IFLA - H. Hofman (2002) - pode ser descrita de duas formas válidas, necessárias e complementares, porque identificam os aspectos ou requisitos a considerar na preservação de objectos digitais: uma definição abrangente que leva em conta os aspectos intelectuais e que pretende assegurar a autenticidade, usabilidade e acessibilidade dos objectos digitais durante o tempo necessário; e outra mais específica e referente a aspectos técnicos com o intuito de garantir a sobrevivência tecnológica dos objectos e informação digitais enquanto forem necessários.[37]

Research Libraries Group & Online Computer Library Center, Report (RLG/OCLC) Beagrie, M. Bellinger, R. Dale, M. Doerr, M. Hedstrom, M.Jones, A. Kenney, C. Lupovici, K. Russell, C. Webb and D. Woodyard, (2002) - gestão de actividades necessárias para garantir tanto a manutenção a longo prazo de dados digitais como o acesso continuado dos seus conteúdos. Se a discussão se refere a um destes em específico, deve utilizar um termo mais preciso.[38]

UNESCO - Webb, C. (2003) - Processos ligados à manutenção de informação e outros tipos de património digital. Neste âmbito não se refere a técnicas de cópia ou digitalização de itens não-digitais, mesmo que seja para fins de preservação. No entanto o produto destas digitalizações pode constituir-se em património a preservar.[39]

Maria Manuela Gomes de Azevedo Pinto (2005) – "*garantir os requisitos e objectivos referentes à produção, tendo em conta as várias partes interessadas e implicações de vária ordem que dela decorrem."*[40]

Miguel Ferreira (2006) – "*capacidade de garantir a acessibilidade e autenticidade suficiente da informação digital para que possa ser interpretada num plataforma tecnológica diferente daquela em que foi criada. Trata-se da actividade responsável pela garantia da comunicação entre emissor e receptor através do espaço e do tempo."*[41]

[35] ROTHENBERG, Jeff - Preserving authentic digital information, p. 54-55.
[36] HENRIQUES, Cecília - Preservação digital: uma perspectiva arquivística, p. 79-81.
[37] HOFMAN, Hans - Can bits and bytes be authentic? preserving the authenticity of digital objects, p. 1.
[38] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 3.
[39] WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage, p. 20.
[40] PINTO, Maria Manuela Gomes de Azevedo – Do «efémero» ao «sistema de informação», p. 55.
[41] FERREIRA, Miguel - Introdução à preservação digital, p. 24.

Digital Curation Centre (DCC) e *Digital Preservation Europe* (DPE) (2007) - define-se como um exercício de gestão de risco com o objectivo de converter a incerteza da manutenção da usabilidade de objectos digitais autênticos em riscos quantificáveis.[42]

ALA (2007 e 2009) - combina políticas, estratégias e acções que garantam a apresentação mais precisa do conteúdo autêntico ao longo do tempo, independentemente dos problemas de corrupção dos ficheiros, falha de suportes e avanço tecnológico, aplicando-se a conteúdo nadodigital ou digitalizado.[43]

Digital Preservation Coalition - BEAGRIE, Neil; JONES, Maggie (2008) - todas as acções necessárias para a manutenção do acesso aos materiais digitais para além dos limites da falha de suportes ou avanço tecnológico. Esses materiais podem ser documentos de arquivo produzidos no âmbito das actividades de negócio da organização, materiais nadodigitais criados para um fim específico, ou resultados de projectos de digitalização.[44]

Faria & Pericão (2008) - utiliza a definição de Webb que considera como "*o conjunto de actividades ou processos responsáveis pela garantia de acesso continuado a longo prazo à informação e património digitais, consistindo na capacidade de garantir a acessibilidade suficiente da informação, para que possa ser interpretada no futuro numa plataforma tecnológica diferente da que lhe deu origem.*"[45]

Rafael António (2008) – *"política, serviços e práticas que pretendem garantir o acesso fidedigno a longo prazo dos recursos digitais."*[46]

InterPARES 2 (2007?) - o processo específico de manutenção de materiais digitais durante e ao longo de várias gerações de tecnologia ao longo do tempo, independentemente de onde se encontram.[47]

Interpares 3 (2011?) - o processo específico de manutenção de materiais digitais durante e ao longo de várias gerações de tecnologia ao longo do tempo, independentemente de onde se encontram. Conjunto de acções de gestão e técnicas necessárias para ultrapassar as alterações tecnológicas e a fragilidade dos suportes garantindo o acesso e interpretação dos documentos digitais durante o tempo considerado necessário.[48]

DGARQ (2011) - e finalmente a definição apresentada no documento do qual partilhamos a autoria, segundo o qual a preservação digital assume três vectores: referentes a conjuntos de actividades cuja finalidade é, por um lado, aumentar a vida útil da informação de arquivo (iARQ), salvaguardando a utilização operacional e protegendo-os das falhas de suportes, perda física e obsolescência tecnológica, por outro, promover a acessibilidade continuada aos

[42] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 20.
[43] MARYNIAK, Cathy [et al.] - Definitions of digital preservation, p. 2.
[44] BEAGRIE, Neil; JONES, Maggie – Preservation management of digital materials: a handbook.
[45] FARIA, Maria Isabel; PERICÃO, Maria da Graça - Dicionário do livro, p. 997.
[46] ANTÓNIO, Júlio - O sistema de gestão documental, p. 187.
[47] - InterPARES 2 Project Glossary, p. 18.
[48] - InterPARES 3 Project Glossary.

conteúdos, e ainda assistir na preservação do conteúdo intelectual, forma, estilo, aparência e funcionalidade.[49]

A análise destas definições permite verificar que a maioria dos autores identifica a necessidade de um plano de gestão sistematizado, com processos específicos, e que inclua a definição de políticas, gestão de recursos, estratégias de aplicação de métodos e actividades definidas, com o objectivo de manter a autenticidade, usabilidade, e garantir acessibilidade fidedigna e continuidade da informação e/ou património digital, independentemente da evolução tecnológica, falhas de suporte, corrupção de ficheiros, tendo em conta os objectivos das partes interessadas e as implicações administrativas, legais, políticas e económico-financeiras. Tal requer que as partes interessadas, os diversos atores, desde o emissor até ao receptor, adquiram consciência de como o seu envolvimento, por muito particular que seja, com os objectos digitais se ramifica ao longo do seu ciclo de vida, devendo esse envolvimento implicar um compromisso de investimento continuado que aumente as perspectivas da preservação e a redução dos seus custos.

Para além disso estas definições:

- consideram como digna de preservação não só os materiais nado-digitais mas também os produtos de projectos de digitalização, estabelecendo o objecto da preservação digital;
- referem os objectivos que se pretendem atingir com a preservação digital, que indicamos como manter a autenticidade, usabilidade, e garantir acessibilidade fidedigna e continuidade da informação e/ou património digital, tendo em conta os objectivos das partes interessadas e as implicações administrativas, legais, políticas e económico-financeiras;
- identificam as razões na origem da necessidade de promover a preservação digital, como riscos decorrentes da evolução tecnológica, falhas de suporte, corrupção de ficheiros;
- inferem a necessidade de identificar os diversos envolvidos na comunidade de interesse e o seu papel no âmbito do ciclo de vida e, por consequência, no âmbito da preservação digital.

Ainda no que se refere a estas definições, elas evidenciam o que Chen já referia em 2001:

> *"Traditionally, preserving things meant keeping them unchanged; however, our digital environment has fundamentally changed our concept of preservation requirements. If we hold on to digital information without modifications, accessing the information will become increasingly more difficult, if not impossible. Even if we could find a physical medium to contain unaltered digital data permanently, formats for recording the information would change and the hardware and software needed to recover the information would become obsolete."*[50]

Thibodeau, em 2002, referia mesmo que:

[49] BARBEDO, Francisco; CORUJO, Luis; SANT'ANA, Mário – Recomendações para a produção de planos de preservação digital, p. 8.
[50] CHEN, Su-Shing - The paradox of digital preservation, p. 5.

> *"Digital preservation is not a simple process of preserving physical objects but one of preserving the ability to reproduce the objects. The process of digital preservation, then, is inseparable from accessing the object. You cannot prove that you have preserved the object until you have re-created it in some form that is appropriate for human use or for computer system applications."*[51]

Tal permite-nos corroborar a afirmação feita em 2011 por Carla Ferreira:

> "*o facto de serem necessárias plataformas tecnológicas diferentes daquelas utilizadas no momento da criação do documento original. Quer isto dizer que o objectivo da preservação digital não passa tanto pela preservação do suporte físico (como acontece com a preservação tradicional), mas sim por garantir que a informação nele contida permaneça acessível e autêntica ao longo do tempo.*" [52]

Existem ainda dois elementos a ter conta, em relação a estas definições: em primeiro lugar oferecem uma gama diversa de termos do que consideram material a preservar; em segundo lugar, algumas definições incluem estratégias específicas para a preservação desse material.

O Objecto da Preservação Digital

Definições e Características

No que concerne à existência dos termos, *documento, digital information, contents, records, digital resources, digital object, bytestream, digital materials*, ela reflecte a afirmação de Azevedo Pinto, referente ao enfoque na área de estudo e investigação que é a preservação digital, como consciencialização do desafio digital:

> *"Aos termos documento/livro sucedem-se agora termos como digital materials, digital object e digital resources*."[53]

Em 1997 o ICA publica o Estudo 8: *Guide for Managing electronic records from an archival perspective*[54] em que define um documento de arquivo como informação registada produzida ou recebida no início, condução ou conclusão de uma actividade institucional ou individual e que compreende conteúdo, contexto e estrutura suficientes para fornecer prova dessa actividade independentemente do formato ou suporte. A característica distintiva dos documentos de arquivo electrónicos é que o conteúdo é registado num suporte e em símbolos (dígitos binários) cuja leitura e compreensão requer um computador ou tecnologia similar.

[51] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 12.
[52] FERREIRA, Carla - Preservação da informação digital, p. 15.
[53] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 121.
[54] ICA Committee on Electronic Records - Guide for managing electronic records from an archival perspective.

Nesse mesmo ano o DLM Forum[55] publica *Guidelines on best practices for using electronic information*, onde define

> *"Electronic record A record where the information is recorded in a form that is suitable for retrieval, processing and communication by a digital computer."*[56]

Neste documento são também indicados os elementos constitutivos dos documentos electrónicos: o Conteúdo (que pode incluir vários tipos de dados, desde texto, tabelas, imagens, som, links), a Estrutura (lógica e física), o Contexto (que pode incluir metainformação técnica e descritiva), Apresentação (esta é cada vez mais abordada separadamente do documento de arquivo, na medida em que a informação é independente de como vai ser apresentada).

É digno de nota que no âmbito do Programa SIADE (Sistemas de Informação de Arquivo e Documentos Electrónicos) que decorreu entre 1997 e 2002, fruto de um protocolo de cooperação entre Instituto dos Arquivos Nacionais/ Torre do Tombo (IAN/TT) e o Instituto de Informática (II), são produzidos dois documentos. *As Recomendações para a Gestão de Documentos de Arquivo Electrónicos – 1:Contexto de Suporte*, de 2000 já definem:

> *"Documento de arquivo electrónico – Documento de arquivo produzido, transmitido e mantido com recurso a equipamentos electrónicos.*
> *Documento electrónico – Documento produzido, transmitido e mantido com recurso a equipamentos electrónicos."*[57]

Esta última definição é confirmada mais tarde, pelo Projecto InterPARES (*International Research on Permanent Authentic Records in Electronic Systems*)[58], que lança em 2001 o The InterPares Glossary[59], em que surgem definições como:

> *"Digital component - A digital object that is part of an electronic record, or of a reproduced electronic record, or that contains one or more electronic records, or reproduced electronic records, and that requires specific methods for preservation.*
> *Electronic record - A record that is created (made or received and set aside) in electronic form."*

[55] O DLM Forum foi fundado em 1994 pela Comissão Europeia. É uma associação que tem como membros os Arquivos Públicos e outros interessados em arquivos, documentos e gestão de informação de toda a União Europeia. A associação é aberta a todos. A sua sigla significava "*Données Lisibles par Machine*" até que, na sua Conferência de 2002 em Barcelona, se decidiu alterar o significado para *'Document Lifecycle Management'*. Cft. DLM Forum - European Commission Introduction: The DLM-Forum, MoReq and the European Commission, p. 1-2.

[56] UNIÃO EUROPEIA. Comissão - *Guidelines on best practices for using electronic information, p. 50.*

[57] BARBEDO, Francisco; GOMES, Eugénia; HENRIQUES, Cecília - Recomendações para a gestão de documentos de arquivo electrónicos, p. 47.

[58] O Projecto InterPARES desenrola-se entre 1999 e 2001 e estava focado em estabelecer requisitos de autenticidade de documentos inactivos produzidos e mantidos em grandes bases de dados e sistemas de gestão documental criados por organismos governamentais, cft. DURANTI, Luciana - The long-term preservation of authentic electronic records, 2001.

[59] INTERPARES Project. Glossary Task Force - The InterPARES glossary, 2001.

Ainda no mesmo ano é publicado o *MoReq (Model Requirements for the Management of Electronic Records) Specification*, no âmbito do programa IDA (*Interchange of Data between Administrations*) da Comissão Europeia, através do *DLM Forum* e corrobora as definições anteriormente indicadas:

> *"Electronic document - A document which is in electronic form. Note: use of the term electronic document is not limited to the text-based documents typically generated by word processors. It also includes e-mail messages, spreadsheets, graphics and images, HTML/XML documents, multimedia and compound documents, and other types of office document.*(…)
> *Electronic record - A record which is in electronic form. Note: it can be in electronic form as a result of having been created by application software or as a result of digitisation, e.g. by scanning paper or microform."*[60]

As fontes utilizadas pelo MoReq para estas definições são as *Functional Requirements for Electronic Records Management Systems*[61] do *Public Record Office*, actual *The National Archives.*

Em 2002 o Programa SIADE avança com as *Recomendações para a gestão de documentos de arquivo electrónicos - 2. Modelo de requisitos para a gestão de arquivos electrónicos*[62]. Este documento é a tradução e adaptação do MoReq à realidade portuguesa, incluindo as duas definições.

Nesse mesmo ano Kenneth Thibodeau define objecto digital como um objecto de informação, de qualquer tipo de informação ou qualquer formato, que está expresso em forma digital. Para o autor, os componentes digitais de um objecto são os objectos lógicos e físicos necessários à reconstituição do objecto conceptual, e esses componentes não se limitam necessariamente aos objectos que contêm o conteúdo de um documento, na medida em que os componentes digitais podem conter dados necessários para a estrutura ou apresentação do objecto conceptual.[63]

A *Digital Preservation Coalition* (DPC), com o seu *The Handbook*[64]*,* que vai actualizando desde 2002, apresenta definições para alguns destes termos:

> *"Digital Materials - A broad term encompassing digital surrogates created as a result of converting analogue materials to digital form (digitisation), and "born digital" for which there has never been and is never intended to be an analogue equivalent, and digital records."*
> *"Digital Publications - "Born digital" objects which have been released for public access and either made available or distributed free of charge or for a fee. They*

[60] UNIÃO EUROPEIA. Comissão – MoReq specification, p. 104.
[61] A última versão disponível é de 2002. cft REINO UNIDO. Public Record Office - Requirements for electronic records management systems: 1: Functional Requirements.
[62] HENRIQUES, Cecília [et al.] - Recomendações para a gestão de documentos de arquivo electrónicos: SIADE 2. Modelo de requisitos para a gestão de arquivos electrónicos.
[63] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 6.
[64] BEAGRIE, Neil ; JONES, Maggie – Preservation management of digital materials: a handbook.

may consist of networked publications, available over a communications network or physical format publications which are distributed on formats such as floppy or optical disks. They may also be either static or dynamic."
"Documentation - The information provided by a creator and the repository which provides enough information to establish provenance, history and context and to enable its use by others."
"Electronic Records - Records created digitally in the day-to-day business of the organisation and assigned formal status by the organisation. They may include for example, word processing documents, emails, databases, or intranet web pages."

A UNESCO lança em 2003 *Charter on the Preservation of the Digital Heritage*, e as *Guidelines for the Preservation of Digital Heritage*[65] que definem Herança Digital como recursos únicos do conhecimento e expressão humanos, e que engloba recursos culturais, educacionais, científicos e administrativos, assim como informação técnica, legal, médica ou outra, criada digitalmente ou digitalizada a partir de recursos analógicos. Quando os recursos são nadodigitais não existe outro formato que não seja o objecto digital. Os materiais digitais incluem textos, bases de dados, imagem estática e em movimento, sons, gráficos, *software* e páginas web, dentro de uma grande e crescente variedade de formatos. São frequentemente efémeros e necessitam de produção, manutenção e gestão premeditados para serem conservados.[66]

O ICA (*International Council on Archives*) apresenta o seu estudo *16 Documentos de Arquivo Electrónicos: Manual para Arquivistas* em 2005, cuja versão em português é uma tradução do original, adaptada à realidade portuguesa. A tradução foi efectuada em tempo recorde por um grupo de trabalho reunido pelo Instituto dos Arquivos Nacionais/Torre do Tombo, e do qual tivemos oportunidade de fazer parte. Nesse estudo, documento de arquivo é definido como "Informação registada, produzida ou recebida no início, condução ou conclusão de uma actividade de um individuo ou organização, e que compreende suficiente conteúdo, contexto e estrutura para fazer prova dessa actividade. Este amplo conceito cobre os vários tipos de documentos de arquivo produzidos em sistemas burocráticos. Os documentos de arquivo podem surgir sob formas e representações diferenciadas. Normalmente são representados como objectos de informação logicamente delimitados, ou seja, como objectos discretos. No entanto surgem cada vez mais documentos de arquivo sob a forma de objectos distribuídos, como sejam bases de dados relacionais e documentos *compostos."* [67]

No ano seguinte, tanto a IFLA (*International Federation of Library Association*), com *Networking for digital preservation: current practice*[68] *in 15 National Libraries*, como o projecto InterPARES 2[69] com o *The InterPARES 2 Project Glossary*[70]*,* apresentam definições de *digital objects, digital records, digital publications.*

[65] WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage, p. 13.
[66] ONU. UNESCO - Charter on the preservation of the digital heritage, p. 75.
[67] ICA Committee on Electronic Records - Documentos de arquivo electrónicos: manual para arquivistas, p. 11.
[68] VERHEUL, Ingeborg - Networking for digital preservation, p. 20-21.
[69] O InterPARES 2 (2002 – 2007) concentrou-se em questões de confiabilidade, exactidão e autenticidade dos documentos de arquivo durante todo o seu ciclo de vida, e examinou os documentos de arquivo produzidos em ambientes dinâmicos no decurso de actividades artísticas, científicas e

Apresentamos finalmente os conceitos definidos pela DGARQ (*Direcção-Geral de Arquivos*) nas *Recomendações para a Produção de Planos de Preservação Digital* em 2008, do qual partilhamos a autoria, em que o Documento de Arquivo Electrónico surge como uma entidade lógica detentora de conteúdo, contexto e estrutura que lhe garanta ter um significado específico, sendo o Objecto Digital a sua componente física, podendo assim um Documento de Arquivo Electrónico, independentemente do formato, ser composto por um ou mais Objectos Digitais. Assim, somente é possível preservar um documento de arquivo electrónico se forem realizadas acções sobre os objectos digitais que o compõem.[71]

A estas definições acrescentam-se as considerações emanadas da versão de 2011 do mesmo documento, do qual também fomos autor, referentes ao sistema de informação, considerado como uma estrutura aplicacional especializada na contenção e gestão de dados e/ou informação. Neste documento são apresentadas dois tipos de representação que a informação de arquivo (iARQ) pode assumir, uma referente ao sistema de informação, mediado tecnologicamente e habitualmente ligado à aplicação de metodologias e ferramentas de bases de dados, estando aqui incluídos os sistemas multimédia como sistemas de informação geográfica (SIG), sistemas de *webconference*, etc., e outro tipo de representação relativo aos Documentos de Arquivo Electrónicos (DAE), que são objectos discretos legíveis de forma equivalente aos seus análogos em suporte analógico, e que são documentos produzidos com recurso a aplicações de produtividade (MS Office, CAD/CAM, etc.). De notar que os sistemas de informação podem conter ou gerir documentos de arquivo electrónico, como é o caso dos sistemas electrónicos de gestão documental, habitualmente constituídos por um sistema baseado em bases de dados que gere, manipula e referencia documentos produzidos e recebidos pela organização.[72]

Assim é consensual o resumo que Manuela Azevedo Pinto apresenta em 2009, de que existem novos materiais que apelida de materiais digitais, que são produzidos no âmbito das actividades do dia-a-dia das organizações e indivíduos e fazem parte da sua memória, que podem ser nadodigitais ou resultado de digitalização mas não existem noutro meio que não o digital, que incluem qualquer tipo de informação e formato, conquanto seja em código binário, que envolvem um processo de codificação/descodificação entre código humano e código binário, sendo necessário um computador[73] para tal, que pode estar em linha ou fora de linha, que pode existir em diversos formatos e suportes, que necessita de elementos para a sua

governamentais on-line. Cft. DURANTI, Luciana; PRESTON, Randy, eds. - InterPARES 2: Experiential, interactive and dynamic records.

[70] - *InterPARES 2 Project glossary.*

[71] BARBEDO, Francisco [et al.] – Recomendações para a produção de planos de preservação digital, 2008, p. 4.

[72] BARBEDO, Francisco; CORUJO, Luis; SANT'ANA, Mário – Recomendações para a produção de planos de preservação digital, 2011, p. 5.

[73] Na nossa opinião trocaríamos aqui o termo computador pelo conceito Sistema Intermediário, isto é, o conjunto de dispositivos - *software* e *hardware* - que foram utilizados para criar o documento e que serão igualmente necessários para ler e apresentar esse mesmo documento. Este conceito é mais cómodo face à profusão de dispositivos que têm surgido no mercado, e que, seja por nomes puramente comerciais ou por categorias tecnológicas, não se assumem como computadores.

referenciação baseados no seu conteúdo, contexto, estrutura e apresentação, e que exigem requisitos de autenticidade, fidedignidade, integridade e usabilidade/inteligibilidade.[74]

Para além destas características, podemos ainda reconhecer a sua versatilidade e dinamismo, na medida em que neles podem ocorrer operações, muitas vezes sem intervenção humana[75], como por exemplo a data mudar automaticamente. Para além disso, podem ser complexos, na medida em que podem integrar diversas componentes digitais, como o caso de um ficheiro de texto com uma imagem embebida, sendo então composto por duas componentes: o texto (os dados de caracteres) e aquele que reproduz a imagem (mapa de bits). Estes componentes podem ou não estar armazenados no mesmo ficheiro físico, como é o caso dos sítios web. Outra característica prende-se com a sua linearidade/não linearidade. A linearidade verifica-se quando, ao ser transposto para suporte analógico, não perde informação significativa (na prática há sempre informação, como o nome do ficheiro, e metainformação perdidas). A não-linearidade verifica-se quando a transposição é impossível, como é o caso de imagens em movimento e sons.

Camadas constituintes do Objecto

Aludindo à definição de objecto digital, é irresistível a referência à abordagem multicamada de Thibodeau[76], um conceito que deu origem a várias adaptações, das quais apresentamos três. Assim, para este autor:

> *All digital objects are entities with multiple inheritance; that is, the properties of any digital object are inherited from three classes. Every digital object is a physical object, a logical object, and a conceptual object, and its properties at each of those levels can be significantly different. A physical object is simply an inscription of signs on some physical medium. A logical object is an object that is recognized and processed by software. The conceptual object is the object as it is recognized and understood by a person, or in some cases recognized and processed by a computer application capable of executing business transactions.*

Ou seja, como objectos físicos, são constituídos por "inscrições" (geralmente os estados binários "activo" ou "inactivo") no objecto que serve de suporte, sejam eles suportes ópticos ou suportes magnéticos. Mesmo os objectos digitais que se encontram em linha na “Nuvem” ou no "ciberespaço" têm que existir em suportes físicos localizáveis em algum sítio. De acordo com Miguel Ferreira, o objecto físico constitui aquilo que é passível de ser interpretado pelo *hardware*, que transforma os símbolos inscritos no suporte físico num conjunto de dados passíveis de serem manipulados pelo *software.*[77]

Como objectos lógicos, ou seja, um código processável pelo *software*, e a sua existência num dado momento depende das inscrições físicas, mas não está vinculada a um suporte em particular. Para Miguel Ferreira:

---

[74] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 125-126
[75] BARBEDO, Francisco - Arquivos digitais: da origem à maturidade, p. 7-8.
[76] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 6.
[77] FERREIRA, Miguel – Introdução à preservação digital, p. 22.

> *"Esse conjunto de dados encontra-se organizado segundo as regras decretadas pelo software utilizado na criação do objecto digital. Essas regras ou estruturas de dados constituem aquilo que vulgarmente se designa por formato de um objecto digital. "*[78]

Como objectos conceptuais que têm um significado para o ser humano, contrariamente aos objectos lógicos ou materiais que os codificam num determinado momento (os objectos conceptuais podem ser reconhecidos como o resultado apresentado ao utilizador). Para que isso aconteça é necessário que o *software* assuma a responsabilidade de preparar o objecto lógico para ser apresentado a uma pessoa, para que o computador converta os sinais digitais em sinais analógicos que serão apresentados ao utilizador através de periféricos de saída.[79]

Como já foi dito surgiram adaptações, das quais damos conta em seguida.

A UNESCO, pela mão da *National Library of Australia*, nas *Guidelines for the Preservation of Digital Heritage,* sugere ainda a existência de uma quarta camada a ter em conta para efeitos de preservação do objecto digital, e que é definida pelos grupos de elementos essenciais que contêm a mensagem, a finalidade ou as características pelas quais se decidiu preservar o material, referindo que a maioria dos objectos digitais contêm uma camada adicional a considerar, na medida em que muitos são composto por vários elementos, alguns dos quais são mais importantes do que outros em levar a essência da mensagem do objecto.[80]

Azevedo Pinto defende esta adaptação afirmando que as características, ou "*significant properties",* pelas quais se decidiu preservar o material podem incluir os aspectos relacionados com a autenticidade e o ciclo de vida, que garantem o acesso a futuros utilizadores à própria informação, ou essência, e a metainformação, que a descreve, representa e garante as condições da sua preservação a longo prazo.[81]

Também Miguel Ferreira, em 2006 sugere a existência de uma quarta camada, diferente da indicada pelo documento da UNESCO:

> *"Não obstante, cada ser humano acaba por fazer uma interpretação individual do objecto recebido. Essa interpretação será aqui designada por objecto experimentado."*[82]

Segundo o autor, apesar de ser teoricamente possível captar e preservar o objecto experimentado, as estratégias de preservação por ele apresentadas não abordam seriamente esta questão.

O modelo multicamadas apresentado pela *Direction des Archives de France*, com apoio da *Bibliothèque Nationale de France* e do *Centre National d'Études Spatiale*s (CNES) refere-se à

[78] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 15.
[79] FERREIRA, Miguel – Introdução à preservação digital, p. 22-23.
[80] WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage, p. 36.
[81] PINTO, Maria Manuela Azevedo – PRESERVMAP, p. 131.
[82] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 16.

informação digital e é composto por cinco camadas, a saber a camada física, a camada binária, a camada de codificação, a camada elemento, e a camada objecto.

Assim, a camada física é o tipo de suporte usado para registar os bits, e está frequentemente ligado a uma tecnologia de gravação que define também o formato de registo da informação.[83]

A camada binária descreve a organização dos bits (tamanho[84] e ordem de dados[85]), ligado ao nível léxico. Esta camada mascara as características específicas do suporte físico, tais como formatos de pacotes registados fisicamente, espaços entre os registos, códigos de correcção de erros.[86]

A camada de codificação permite passar de uma representação de dados para outra e descreve a estrutura do tamanho dos bits ou conjuntos de bits, estando ligado ao nível sintáctico. Esta camada permite transformar os bits de um ou vários bytes em informação básica que pode consistir num caractere alfabético[87], um sinal de pontuação, um algarismo, um nome, uma representação da cor de um *pixel* numa imagem.[88]

A camada elemento descreve o que significa um conjunto de bits, tendo então a ver com o significado da estrutura utilizada. O conhecimento do tipo de codificação não é suficiente, devendo saber também a correspondência na tabela "*código* ←→ *significado utilizado*".[89] Trata-se de um nível semântico básico, uma vez que se limita a dar um primeiro significado a uma estrutura.[90]

A camada objecto descreve como são reunidos os elementos e os seus significados, e a informação adquire aqui sentido. Para serem inteligíveis, os objectos, que normalmente são armazenados em ficheiros, necessitam de um conjunto de *software*s para poderem ser interpretados e de materiais para poderem ser representados. São aplicações que permitem as interacções possíveis entre objectos e informação: criação, manipulação, modificação, interpretação, destruição.[91] Por exemplo, para visualizar um objecto, um ficheiro no formato ".docx", precisamos da versão correcta da aplicação Word da Microsoft, das fontes (tipo de letra) utilizadas nesse ficheiro e um computador com um ecrã.

---

[83] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 28.

[84] Refere-se à sequência de bits de tamanho fixo que é processado em conjunto numa máquina. Esses tamanhos podem ser de 8 bits, 16 bits, 32 bits, 64 bits, dependendo do sistema intermediário utilizado.

[85] Refere-se à ordem utilizada para representar os dados ou os bits. Podem ser guardados por ordem crescente do seu "peso numérico", chamado *Little-Endian*, ou por ordem crescente do seu "peso numérico", chamado *Big-Endian*. Por exemplo, o número 12 é representado em código binário 1100 numa forma e 0011 noutra.

[86] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 29-30.

[87] Por exemplo, para a representação de caracteres, temos codificações simples, como o ASCII para os caracteres do alfabeto inglês, em que cada caracter está codificado em 7 bits, ou a ISO 8859-1:1998 para os caracteres do alfabeto latino, em que cada caracter está codificado em 8 bits (1 byte ou octeto), e temos codificações complexas, como o UTF-8 que é utilizado normalmente para codificar os caracteres das tabela UNICODE, e que pode utilizar 1 a 6 bytes ou octetos, isto é, de 8 a 48 bits.

[88] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 30-31.

[89] Por exemplo, no caso dos caracteres UNICODE, tem a ver com as várias tabelas que definem, para um valor numérico (a posição no código), tendo em conta como foi codificado, o sinal gráfico (o glifo) correspondente a representar.

[90] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 31.

[91] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 32.

Pode-se aventar a relação entre estas camadas com os três níveis de problemas de comunicação apresentados por Shannon[92] (1949):

- O problema técnico: Ligada ao grau de exactidão da transmissão da mensagem;
- O problema semântico: Ligada ao grau de precisão da "comunicação" do significado;
- O problema da eficácia: Ligada ao grau de sucesso com que o significado "comunicado" afecta o comportamento do destinatário.

Assim o problema técnico referia-se à passagem do objecto físico para o objecto lógico, na medida em que está ligado à exactidão da comunicação de um conjunto discreto de símbolos, inscritos ou registados num suporte, como um conjunto de dados codificado processável por um *software*. O problema semântico prender-se-ia com a passagem do objecto lógico ao objecto conceptual, na medida em que está relacionado com a identificação, ou aproximação suficientemente satisfatória, na interpretação do significado pelo receptor, em comparação com o significado pretendido do remetente, ou seja, que o *software* consegue apresentar o conjunto de dados por ele processado como algo devidamente reconhecível pelo receptor (humano). Finalmente, o problema da eficácia reportar-se-ia à passagem do objecto conceptual ao objecto experimentado (tal como referido por Ferreira[93]), ligado ao grau de sucesso com que o significado transmitido ao receptor resulta na conduta desejada de sua parte, ou seja, se o consumidor compreende a intenção da mensagem e consegue usufruir dela, utilizando-a e adaptando-a às suas intenções.

Estratégias de Preservação

Tendo como base esta perspectiva, Thibodeau considera que é necessário identificar quais os objectivos que se pretendem alcançar com a preservação digital, para podermos seleccionar a melhor estratégia de preservação digital. Esta selecção deve ter em conta quatro critérios, a exequibilidade, a sustentabilidade, a viabilidade e a pertinência. O primeiro critério requer *hardware* e *software* capazes de implementar a estratégia, o segundo critério significa que a estratégia pode ser utilizada a longo prazo ou que há garantias para considerar outra estratégia no futuro que substitua a utilizada actualmente. A sustentabilidade de cada estratégia tem componentes internos e externos em que os primeiros estão relacionados com a imunidade ou isolamento da estratégia face à obsolescência tecnológica, e os segundos com a capacidade de se relacionar com outras estratégias, em termos de pesquisa e disseminação, que continuará a evoluir. O terceiro critério tem a ver com a necessidade da implementação ser feita dentro de limites aceitáveis de dificuldade e custos, e o último critério prende-se com os tipos de objectos a preservar e os objectivos específicos da preservação. Relativamente aos tipos de objectos a preservar, pode-se definir um espectro de possibilidades que vai desde a preservação da tecnologia até à preservação dos objectos que são produzidos usando tecnologias da informação digitais.[94]

[92] SHANNON, Claude; WEAVER, Warren – The mathematical theory of communication, p. 4.
[93] Cft. FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 16.
[94] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 15-16.

Esta divisão entre estratégias de preservação da tecnologia, ligadas ao objecto físico e/ou lógico, e estratégias de preservação do objecto (objecto conceptual) é consentânea com a sistematização apresentada por Lee [*et al.*] em 2002 que classifica as estratégias de preservação de acordo com duas perspectivas, uma mais conservadora em que se preserva o ambiente tecnológico original para descodificar a informação digital no futuro, e outra ligada à superação do problema da obsolescência técnica dos formatos dos ficheiros."[95]

Na primeira abordagem estes autores incluem uma das técnicas de preservação identificadas em 1996 pela *Task Force on Archiving of Digital Information* da *Research Libraries Group (*RLG) e da *Commission on Preservation and Access* (CPA)[96], a Preservação de Tecnologia, e a Emulação, tal como referida por Rothenberg[97] em 2000. A segunda abordagem inclui a Migração, também referida pela *Task Force on Archiving of Digital Information* da RLG/CPA[98], e o Encapsulamento, referido por Waugh, [*et al.*][99] em 2000.

Thibodeau apresenta uma grelha em que mapeia as estratégias de preservação, tendo em conta em que um dos eixos representa, num dos extremos, a incidência da estratégia de preservação no objecto físico e/ou lógico, e no outro extremo a incidência da estratégia de preservação ou no objecto conceptual. No outro eixo, e de acordo com Ferreira:

> *"No eixo vertical as várias estratégias são dispostas mediante o seu grau de especificidade, i.e., se são estratégias apenas aplicáveis a uma dada classe de objectos digitais ou se se tratam de estratégias genéricas, passíveis de ser administradas a qualquer classe de objectos digitais."*[100]

Thibodeaux aduz assim várias metodologias de preservação digital, agrupadas em três grandes conjuntos[101], sendo o primeiro a preservação de tecnologia, que pretende manter os dados em formatos e suportes específicos e utilizar a tecnologia originalmente associada a esses formatos e suportes para aceder aos dados e reproduzir os objectos [Emulação, Chips programáveis, Manutenção da Tecnologia original]. No meio, as estratégias que migram formatos de dados à medida que a tecnologia evolui, permitindo o uso de tecnologia actual para a pesquisa, acesso e reprodução. [Computador Virtual Universal, Máquina Virtual, Reengenharia de *Software*, Visualizadores, Conversão para formatos do mesmo tipo de dados, Pedra de Rosetta, Normalização de formatos, Migração de versões]. E finalmente a preservação dos objectos, com estratégias focadas na preservação das características significativas dos objectos e que são definidas explicita e independentemente de qualquer

[95] LEE, Kyong-Ho [et al.] - The state of the art and practice in digital preservation, p. 95.
[96] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information.
[97] ROTHENBERG, Jeff - Preserving authentic digital information.
[98] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, http://www.dpconline.org/advice/preservationhandbook/organisational-activities/storage-and-preservation.
[99] WAUGH, Andrew [et al.] - Preserving digital information forever.
[100] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 16.
[101] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 19.

software ou *hardware* específico. [Arquivos Persistentes e Formatos de importação/exportação de objectos].

O autor enfatiza, no entanto, que os métodos que apresenta não incluem todos os que foram propostos ou testados para a preservação digital, nomeadamente métodos que se focam na metainformação. Por outro lado, para alguns ele apresenta métodos que ainda não foram mencionados como estratégias de preservação, como forma de demonstrar a robustez da grelha por ele apresentada, para demonstrar que é preciso estar aberto às possibilidades que o desenvolvimento tecnológico está constantemente a criar, e finalmente para se verificar que a preservação em ambiente digital não é somente para transmitir informação diacronicamente, mas também a nível de fronteiras no espaço, na tecnologia e instituições, pelo que os métodos a desenvolver como estratégia devem permitir a transmissão de informação confiável e com autenticidade de forma transversal a essas fronteiras.[102]

Por sua vez, a UNESCO[103] (2003) divide as estratégias em cinco tipos:

- Estratégias de investimento, que envolvem investimento de empenho no início: utilização de normas; extracção e estruturação de dados; encapsulamento; restringir o número de formatos a gerir; abordagem ligada à máquina virtual universal;
- Estratégias a curto prazo: preservação de tecnologia; retrocompatibilidade e migração de versões; migração (também funciona a longo prazo);
- Estratégias de médio-longo prazo: migração; visualizadores; emulação; máquina virtual universal;
- Estratégias alternativas: abordagens não-digitais, recuperação de dados;
- Combinação de estratégias.

O *Digital Preservation Coalition* (DPC) faz a sua divisão entre estratégias primárias (a Migração e a Emulação) e estratégias secundárias (Preservação de tecnologia, Adesão a Normas, Retrocompatibilidade, Encapsulamento, Conversão para Formato Analógico Estável, Arqueologia Digital):

> *"Primary preservation strategies as defined here are those which might be selected by an archiving repository for medium to long-term preservation of digital materials for which they have accepted preservation responsibility. Secondary preservation strategies are those which might be employed in the short to medium term either by the repository with long-term preservation responsibility and/or by those with a more transient interest in the materials."*[104]

[102] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 18.
[103] WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage, p. 122-123.
[104] BEAGRIE, Neil ; JONES, Maggie – Preservation management of digital materials: a handbook.

Miguel Ferreira apresenta[105] as seguintes estratégias de preservação: a Preservação da Tecnologia, o Refrescamento, a Emulação, a Migração/Conversão, que inclui Migração para Suportes Analógicos, Actualização de Versões, Conversão para Formatos Concorrentes, Normalização, Migração a-pedido e a Migração Distribuída, o Encapsulamento, e a Pedra de Rosetta Digital.

Face a toda esta panóplia de métodos e estratégias, e propostas de tipologias das mesmas, decidiu-se apresentar de forma mais aprofundada as estratégias identificadas pela DGARQ*[106]*, num documento do qual partilhamos a autoria:

- A preservação de tecnologia refere-se à conservação e manutenção de todo o *hardware* e *software* necessários à correta apresentação dos OD[107], focando-se então na preservação do objecto digital na sua forma original[108], e não no objecto conceptual. As desvantagens desta estratégia passam pela inevitabilidade da obsolescência acabar por afectar qualquer plataforma tecnológica[109], pelas dificuldades colocadas pela gestão do espaço físico, pela manutenção e custos de operação[110], e ainda porque o acesso à informação fica limitado ao local físico onde se encontra o *hardware* e *software*, com os condicionalismos acrescidos que daí advém no âmbito da reutilização da informação.[111]

- A emulação prende-se com a utilização de uma aplicação de *software* - o emulador - para reproduzir o comportamento de uma plataforma de *hardware* e/ou *software*, numa outra plataforma que, em condições habituais, seria incompatível.[112] Esta estratégia é vantajosa na medida em que permite a preservação fiel das características e funcionalidades do objecto digital original[113] e, apesar de estar centrada na preservação do objecto lógico no seu formato original, não padece dos principais problemas da estratégia de preservação de tecnologia (Ex.: envelhecimento do *hardware*).[114] As suas desvantagens passam pelo risco do emulador também se tornar obsoleto[115] e a sua utilização presume que, a médio-longo prazo, os utilizadores saibam operar adequadamente aplicações e sistemas operativos não

[105] FERREIRA, Miguel – Introdução à preservação digital, p.32-45 e FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 22-34.
[106] BARBEDO, Francisco; CORUJO, Luis; SANT'ANA, Mário – Recomendações para a produção de planos de preservação digital, 2011, p. 47 e 52-55.
[107] Cft. BEARMAN, David - Collecting *software*: a new challenge for archives & museums; WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information; SWADE, Doron - Preserving *software* in an object-centred culture; HENDLEY, Tony – Comparison of methods and costs of digital preservation.
[108] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 22.
[109] HENDLEY, Tony – Comparison of methods and costs of digital preservation.
[110] LEE, Kyong-Ho, [et al.] - The state of the art and practice in digital preservation.
[111] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years.
[112] ROTHENBERG, Jeff - Avoiding technological quicksand.
[113] LEE, Kyong-Ho, [et al.] - the state of the art and practice in digital preservation.
[114] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 22.
[115] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years.

existentes há muito. (Ex.: num futuro próximo será difícil conceber que os utilizadores estejam aptos a enfrentar as particularidades do sistema operativo MS-DOS).[116]

- A estratégia de monitorização pressupõe a existência de processos de verificação manual, semiautomática e automática dos objectos digitais, sendo as duas primeiras opções mais racionais por questões de custos. As principais questões em que se centram as preocupações da monitorização têm a ver com o tempo médio de prevalência de uma versão de aplicação informática (3 anos), tempo de vida estimado dos suportes de armazenamento; retrocompatibilidade do *software* assegurada pelos fabricantes (em média 3 versões anteriores).

- A estratégia de encapsulamento implica a preservação do objecto digital, juntamente com toda a informação considerada necessária e suficiente para garantir o desenvolvimento futuro de *software* aplicacional para conversão, visualização ou emulação (por exemplo, a descrição formal e detalhada do formato de ficheiro do objecto a preservar).[117] Esta estratégia está direccionada para os objectos que terão interesse apenas num futuro longínquo, permitindo o adiamento da responsabilidade de preservação, apesar de o nível de complexidade dos objectos obrigar à existência de especificações complexas, que, se incompletas, podem conduzir a um efeito desastroso para a preservação do objecto digital.

- A transferência de formatos e suportes diz respeito à passagem de documentos contidos num determinado suporte ou formato para outro suporte ou formato mais actualizado[118], num processo que reorganiza os elementos de informação que constituem os objectos digitais.[119] Esta estratégia tem essencialmente a ver com a preservação do conteúdo intelectual, isto é, com a preservação do objecto conceptual e a verificação frequente da integridade dos suportes físicos.[120] O objectivo desta estratégia é evitar a obsolescência tecnológica, mantendo os objectos digitais compatíveis com as tecnologias atuais, para garantir a sua interpretação sem ter de recorrer a artefactos menos convencionais.[121] Esta estratégia pressupõe processos de refrescamento a nível de suportes (por exemplo: de Disquete para CD-R ou de CD-R para DVD-R), nos casos em que existam e sejam utilizados estes suportes, a migração entre formatos (por exemplo: de Word 97 para Word 2000), e a transposição conjunta de formatos e suportes. As desvantagens apresentadas por esta estratégia derivam da probabilidade de algumas propriedades dos objectos digitais não serem correctamente transportadas para o formato de destino adoptado[122], da incompatibilidade que pode existir entre os formatos de origem e destino, da inadequação

[116] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 22.
[117] PAÍSES BAIXOS. Nationaal Archief - Digital preservation testbed white paper: migration: context and current status.
[118] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information.
[119] LAWRENCE, Gregory W. [et al.] - Risk management of digital information.
[120] RUSSELL, Kelly - Digital Preservation and the CEDARS project experience.
[121] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 26.
[122] Cft. HESLOP, Helen; DAVIS, Simon; WILSON, Andrew - An approach to the preservation of digital records; HEDSTROM, Margaret - Digital preservation: problems and prospects.

do *software* de conversão e da obsolescência de formatos.[123] Para além disso, este processo, no âmbito da transposição para novos formatos, acarreta sempre perda de informação em termos da estrutura, da metainformação e, por vezes, do conteúdo, pelo que se deve recorrer a estratégias que incluam a documentação exaustiva de todo o processo de migração (metainformação) que demonstre o que se perdeu, quando e como se perdeu. Este cuidado pretende evitar que as perdas não comprometem a autenticidade e fidedignidade do documento. No âmbito da transferência de formatos existem algumas variantes, que passam pela actualização de versões, caracterizada pela actualização dos formatos utilizando *software* retrocompatível (por exemplo, a utilização do Word 6 para actualizar um documento criado com o Word 5), a conversão para formatos concorrentes, que permite superar o risco de descontinuidade de formatos, convertendo o objecto digital para formatos semelhantes, independentemente da aplicação informática utilizada na sua criação (por exemplo, converter um documento Word para PDF), a normalização, que corresponde à migração para um número restrito de formatos compatíveis, o que poderá evitar futuras problemas a nível de direitos de autor ou pagamento de royalties, e, finalmente promove, também, a interoperabilidade entre sistemas distintos.

Ainda dentro das estratégias de preservação deve-se ter em atenção a elementos como a análise de riscos, o registo de formatos e a metainformação. A análise de riscos é um conjunto de actividades no âmbito da gestão de risco, e que pretende identificar as ameaças e o risco de ocorrências, para assim prever as mais prováveis e tomar decisões sobre a melhor forma de se precaver contra elas mediante a aplicação dos métodos mais adequados.[124] O DRAMBORA[125], que será aprofundado no capítulo 5, é um exemplo de metodologia e ferramenta para efectuar a análise de risco nos repositórios digitais. O registo de formatos pretende recolher informação relacionada com os formatos de ficheiro, nomeadamente a sua estrutura e ambiente de *hardware* e *software*, assim como outros componentes técnicos necessários para suportar o acesso de longo prazo aos documentos de arquivo electrónicos e outros objectos digitais de valor cultural, histórico ou de negócio, garantindo que no futuro, seja possível a existência de aplicações que interpretem os ficheiros e permitam aceder à informação neles contida. Exemplo disso é o PRONOM[126], um registro técnico de acesso via web para apoiar os serviços de preservação digital, desenvolvido pelo Arquivo Nacional do Reino Unido. Outros projectos são o *Global Digital Format Registry* (GDFR)[127] e, mais recentemente, o *Unified Digital Format Registry* (UDFR)[128], que pretende unificar as funções e recursos do PRONOM e do GDFR numa plataforma comum. No que respeita à metainformação, na sua acepção mais básica trata-se de informação sobre informação, mais concretamente, dados estruturados sobre informação capturada no sistema de arquivo, e que permite a descrição dos atributos do documento de arquivo electrónico, fornecendo-lhe significado, contexto e organização, o que

[123] Cft. FERREIRA, Miguel; BAPTISTA, Ana Alice; RAMALHO, José Carlos - A foundation for automatic digital preservation; LAWRENCE, Gregory W. [et al.] - Risk management of digital information; RAUBER, Andreas; ASCHENBRENNER, Andreas - Part of our culture is born digital: on efforts to preserve it for future generations.
[124] WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage, p. 52-53.
[125] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment.
[126] REINO UNIDO. National Archives – PRONOM: The technical registry.
[127] HARVARD UNIVERSITY. Harvard Library - Global Digital Format Registry.
[128] UNIVERSITY OF CALIFORNIA. Curation Center - Unified Digital Format Registry.

permite a produção, gestão e utilização de documentos de arquivo ao longo do tempo, assim como nos, e através dos, domínios em que são produzidos. Uma vez que os documentos electrónicos são dependentes do sistema intermediário, a metainformação permite a contextualização dos objectos digitais no âmbito da sua produção, gestão e preservação. Esta revela-se assim, importante para a preservação digital, na medida em que, ao estar associada aos objectos digitais, permite para cada um desses objectos digitais, a sua referenciação única e persistente, a sua localização e recuperação expedita, a criação do seu histórico, e o registo das transformações neles realizados.

A questão da metainformação será abordada mais adiante, principalmente no capítulo 4.

Quadro Teórico de Referência

No que se refere à preservação digital é preciso falar ainda do quadro teórico de referência, isto é, os fundamentos intelectuais que a sustentam.

A publicação, em 1996, do relatório "*Preserving digital information: Report of the task force on archiving of digital information*"[129] pela *Research Libraries Group* (RLG) e *Commission on Preservation and Access* (CPA), fruto de um grupo de trabalho constituído dois anos antes, com o objectivo de investigar o que era necessário para garantir a preservação a longo prazo e acesso continuado aos documentos electrónicos tornou-se um marco que ajudou a definir a conceitos-chave, requisitos e desafios.[130] Esse grupo de trabalho propôs o desenvolvimento de um sistema nacional de arquivos digitais que assumissem a responsabilidade do armazenamento e acesso de informação digital a longo prazo; apresentou o conceito de repositório digital confiável e definiu o seu papel e responsabilidades; identificou cinco características da integridade da informação digital (conteúdo, fixidez [inalterabilidade/estabilidade], referenciação, proveniência e contexto), que foram posteriormente incorporadas na definição de Informação de Descrição de Preservação do Modelo de Referência OAIS (*Open Archival Information System*)[131] e definiu a migração como uma função essencial nos arquivos electrónicos. Os conceitos e as recomendações descritas no relatório estabeleceram as bases para pesquisas e iniciativas de preservação digital posteriores.[132]

O *Modelo de Referência OAIS* foi desenvolvido em 2002 com a intenção de normalizar a prática da preservação digital e fornecer um conjunto de recomendações para implementação de programas de preservação. O OAIS diz respeito a todos os aspectos técnicos do ciclo de vida de um objecto digital, desde a Ingestão, Armazenamento, Gestão de Dados, Administração, Acesso e Planeamento de preservação. O modelo também aborda questões ligadas à metainformação, recomendando cinco tipos de metainformação para cada objecto digital: informação de referenciação (identificação); informação de proveniência (incluindo o histórico de preservação), o contexto, fixidez (indicadores de autenticidade), e de representação

[129] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information.
[130] MCGOVERN, Nancy - Principles and good practice for preserving data. p. 5–6.
[131] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS).
[132] CONWAY, Paul - Preservation in the age of google: digitization, digital preservation, and dilemmas, p.66–67.

(formatação, estrutura de ficheiro, e o que "confere sentido ao *bitstream* de um objecto").[133] Este modelo de referência vai ser aprofundado no capítulo 4.

A publicação de *Trusted Digital Repositories: Attributes and Responsibilities* em 2002, fruto da colaboração, iniciada dois anos antes, entre o *Research Libraries Group* (RLG) e Online *Computer Library Center* (OCLC), permitiu identificar as características para repositórios digitais para organizações de investigação, baseando-se e consolidando o Modelo OAIS. Este documento define Repositório Digital Confiável como aquele cuja missão é fornecer acesso a longo prazo de confiança de recursos digitais geridos, à sua Comunidade Designada, na actualidade e no futuro.

O Repositório Digital Confiável deve incluir sete atributos: conformidade com o modelo de referência OAIS, a responsabilidade administrativa, a viabilidade organizacional, sustentabilidade financeira, adequação tecnológica e de procedimentos, a segurança do sistema, a responsabilidade *(accountability*) de procedimentos. O Modelo de Repositório Digital Confiável descreve as relações entre esses atributos. O relatório também recomenda o desenvolvimento colaborativo da certificação de repositórios digitais, modelos de redes de cooperação e partilha de pesquisa e informação sobre a preservação digital referente aos direitos de propriedade intelectual.[134] Em 2004, H. Gladney propõe outra abordagem para a preservação de objectos digitais que prevê a criação de "Objectos digitais Confiáveis", que podem dar conta da sua própria autenticidade, uma vez que integram um registo do seu histórico de utilização e modificações, permitindo que futuros utilizadores possam verificar a validade do conteúdo do objecto.[135]

O *International Research on Permanent Authentic Records in Electronic Systems* (InterPARES) é uma iniciativa de pesquisa colaborativa liderada pela Universidade de British Columbia, que se foca nas questões de preservação de documentos digitais autênticos a longo prazo. A pesquisa está a ser realizada por grupos de discussão de várias instituições dos vários continentes, com o objectivo de desenvolver teorias e metodologias que sirvam como base para estratégias, normas, políticas e procedimentos necessários para garantir a *trustworthiness* [confiança][136], a *reliability* [credibilidade][137] e *accuracy* [precisão/exactidão] dos documentos de arquivo electrónicos a longo prazo.[138] O Projecto *InterPARES* desenrola-se numa primeira fase, entre 1999 e 2001, e estava focado em estabelecer requisitos de autenticidade de documentos inactivos produzidos e mantidos em grandes bases de dados e sistemas de gestão documental criados por organismos governamentais.[139] O *InterPARES 2* (2002 – 2007) concentrou-se em questões de confiabilidade, exactidão e autenticidade dos documentos de arquivo durante

[133] CORNELL UNIVERSITY; ICPSR; MIT - Digital preservation management: implementing short-term strategies for long-term problems.
[134] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities.
[135] GLADNEY, HENRY - Trustworthy 100-year digital objects: evidence after every witness is dead.
[136] trustworthy (adj) able to be trusted as being honest, safe, or reliable http://www.macmillandictionary.com/thesaurus-category/british/Reliable-and-trustworthy.
[137] Reliable (adj) a reliable person is someone who you can trust to behave well, work hard, or do what you expect them to do. http://www.macmillandictionary.com/thesaurus-category/british/Reliable-and-trustworthy.
[138] SUDERMAN, Jim - Principle-based concepts for the long-term preservation of digital records.
[139] DURANTI, Luciana - The long-term preservation of authentic electronic records, 2001.

todo o seu ciclo de vida, e examinou os documentos de arquivo produzidos em ambientes dinâmicos no decurso de actividades artísticas, científicas e governamentais *online.*[140] A terceira fase (*InterPARES 3*) foi iniciada em 2007. O seu objectivo é utilizar o conhecimento teórico e metodológico criado pelo *InterPARES* e outros projectos de investigação de preservação para desenvolver as orientações, planos de acção e programas de formação sobre preservação a longo prazo de documentos de arquivo autênticos para pequenas e médias organizações de gestão documental e arquivo.[141]

As *Recomendações para a Produção de Planos de Preservação Digital*[142], tem como objectivo a produção de um documento estratégico que contenha políticas, procedimentos e práticas/actividades para a constituição de uma estrutura técnica e organizacional que permita preservar e gerir de forma continuada os objectos digitais, por forma a mantê-los utilizáveis, do ponto de vista administrativo e eventualmente patrimonial durante o período de tempo considerado necessário. Tal passa pela identificação e caracterização da informação digital produzida pelo organismo, identificação dos procedimentos a realizar para evitar a obsolescência tecnológica e perda de informação, e definição das responsabilidades relativas à execução desses procedimentos dentro da organização. Isto implica a categorização dessa informação de acordo com necessidades operacionais e identificação dos prazos de conservação das classes de informação identificadas.

Esta análise incide sobre entidades como os Sistemas onde é produzida e/ou armazenada a informação digital, os actores que agem sobre esses sistemas e qual o seu papel. Também verificará o conteúdo informacional, a relação entre os vários sistemas do ponto de vista informacional e funcional, e finalmente informação sobre a plataforma tecnológica, nomeadamente o sistema intermediário, formatos, procedimentos e infrastruturas de segurança do sistema e da informação.

A implementação, execução e monitorização de um Plano de Preservação Digital passa pela atribuição de novas responsabilidades e tarefas num quadro de actividade transversal continuada da organização que se coadune com uma gestão da mudança.

O resultado implica a identificação, racionalização e melhor utilização continuada da informação digital no âmbito das actividades da organização, pelo conhecimento de entidades como os sistemas de informação, os agentes e os seus papéis, e as relações entre tais entidades no âmbito organizacional e funcional, pelo desenvolvimento e ampliação de competências, conhecimento e infrastruturas referentes à preservação digital e que permitam o desenvolvimento de outros projectos, racionalização de recursos derivada da eliminação da informação desnecessária.[143]

[140] DURANTI, Luciana; PRESTON, Randy, eds. - International research on permanent authentic records in electronic systems (InterPARES) 2: experiential, interactive and dynamic records.
[141] LASZLO, Krisztina; MCMILLAN, Timothy, YUHASZ, Jennifer - The InterPARES 3 project: implementing digital records preservation in a contemporary art gallery and ethnographic museum, p. 4.
[142] BARBEDO, CORUJO, SANT'ANA – Recomendações para a produção de planos de preservação digital, 2011.
[143] BARBEDO, Francisco; MARTINS, Sílvia – Preservação digital.

Para concluir o Estado da Arte da Preservação Digital?

Katia Thomaz[144] resume as preocupações e desafios identificados e abordados por vários autores, no que se refere à preservação de documentos de arquivo electrónico nas seguintes categorias[145]:

1. Falta de políticas de avaliação: O impacto causado pela definição dos critérios de selecção é muito importante no ambiente digital. O documento digital que não for seleccionado nas fases iniciais do seu ciclo de vida irá provavelmente perder-se ou tornar-se inútil no futuro;

2. Falta de políticas de descrição: A natureza complexa da tecnologia exige uma abordagem descritiva e detalhada, ou seja, metainformação de objectos digitais para a manutenção. A metainformação de elementos internos e externos dos documentos tornou-se crucial;

3. Vulnerabilidade física: O *Hardware* e os suportes de armazenamento são inerentemente instáveis e, sem a instalação e manutenção adequada, eles podem deteriorar-se rapidamente, mesmo que externamente não pareçam estar danificados;

4. Vulnerabilidade lógica: O ambiente digital é sensível a mudanças (algumas são derivadas das próprias necessidades de gestão) o que pode comprometer a integridade, a autenticidade e a história dos objectos digitais;

5. Elevada obsolescência tecnológica: O ciclo de renovação tecnológica é curto (3-5 anos) por oposição a décadas e séculos associados à preservação de objectos físicos;

6. Elevada dependência tecnológica: Todos os objectos digitais requerem *hardware* e *software* específicos para serem acedidos e cada um desses elementos geralmente requer contratos, que são geralmente difíceis de negociar;

7. Dificuldade no recrutamento de pessoal devidamente qualificado: A tecnologia envolvida no acesso a objectos digitais requer uma significativa diversidade de actividades que são realizadas por poucos especialistas.

No que se refere aos requisitos de preservação, a autora aponta o estudo de Bullock[146] acerca do modelo de referência OAIS, que identifica acções ou requisitos a cumprir no âmbito da preservação digital de documentos de arquivo:

---

[144] THOMAZ, Katia P - Critical factors for digital records preservation.

[145] Cft. BEAGRIE, Neil ; JONES, Maggie – Preservation management of digital materials: a handbook; BRAND, Stewart - Escaping the digital dark; BULLOCK, Alison - Preservation of digital information: issues and current status; CONWAY, Paul - Preservation in the digital world; UNIÃO EUROPEIA. Comissão – MoReq specification: Model Requirements for the Management of Electronic Records, 2001; HEDSTROM, Margaret - Digital preservation: a time bomb for digital libraries; ICA Committee on Electronic Records - Guide for managing electronic records from an archival perspective; LUSENET, Yola de - Digital heritage for the future; WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage; REINO UNIDO. Public Record Office - Management, appraisal and preservation of electronic records: principles; ROTHENBERG, Jeff - Ensuring the longevity of digital information; THIBODEAU, Kenneth - Building the archives of the future; WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information.

[146] BULLOCK, Alison - Preservation of digital information: Issues and current status.

1. A fixação do objecto como um todo discreto: Os limites de um objecto digital não são claros, especialmente um objecto composto criado pela reunião de diferentes suportes ou através da ligação a vários recursos existentes numa rede;

2. Preservar a presença física: Refere-se a manter o ficheiro de computador, a série de 1s e 0s que são a base de um objecto digital;

3. Preservar o conteúdo: Refere-se a manter a possibilidade de aceder o conteúdo no seu nível mais baixo (por exemplo, texto ASCII) sem os embelezamentos de variações de fontes e funções de *layout*;

4. Preservar a apresentação: Refere-se a manter a aparência original de um objecto digital. As especificações de *layout* também devem ser preservadas, especialmente quando contribuem significativamente para a compreensão e interpretação do conteúdo. Especificações de layout incluem os diferentes rostos de fontes e tamanhos, o uso do espaços em branco, colunas, notas marginais, cabeçalhos, rodapés, paginação, e assim por diante, por vezes separados do conteúdo;

5. Preservar a funcionalidade: Refere-se a manter os aspectos dinâmicos de um objecto digital (por exemplo, componentes de multimédia, o formato de hipertexto, a capacidade de gerar automaticamente conteúdo dinâmico a partir armazenamentos de dados, funções de navegação e tabelas de conteúdo interactivo);

6. Preservar a autenticidade: Refere-se a assegurar um objecto digital contra alterações não autorizadas e monitorizando o objecto digital através de múltiplos ciclos de "cópia" para garantir que cada cópia é uma versão aceitável do original;

7. Localizar e referenciar o objecto original ao longo do tempo: Trata-se de ser capaz de corresponder a uma citação a um objecto digital, e para distingui-lo de outras versões ou edições;

8. Preservar a proveniência: Refere-se a afirmar a origem e a cadeia de custódia de um objecto e contribui para defini-lo como um todo. Isto ajuda a confirmar que o trabalho é autêntico e o seu conteúdo está intacto;

9. Preservar contexto: Refere-se a descrever a dependência de *hardware* e *software* de um objecto digital, e seu modo de distribuição e ligações a outros objectos digitais.

A literatura aborda ainda, na perspectiva da autora, as funções de arquivo, tendo por base o modelo referência OAIS[147]:

1. Ingestão: A entidade OAIS que contém os serviços e funções para aceitar SIPs dos produtores, preparando AIPs para o armazenamento, e assegurando que os AIPs e a sua Informação Descritiva de apoio são integrados no OAIS;

2. Armazenamento de arquivo: A entidade OAIS que contém os serviços e funções de armazenamento e recuperação de AIPs;

[147] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS).

3. Gestão de dados: A entidade OAIS que contém os serviços e funções para preencher, efectuar a manutenção, e o acesso a uma ampla variedade de informação. Alguns exemplos desta informação são catálogos e inventários sobre o que pode ser recuperado a partir de armazenamento de arquivo, algoritmos de processamento que podem ser executados em dados recuperados, estatísticas de acesso ao consumo, facturação do consumidor, pedidos com base em eventos, controlos de segurança e cronogramas OAIS, políticas e procedimentos;

4. Administração: A entidade OAIS que contém os serviços e funções para o controlo do funcionamento do dia-a-dia das outras entidades funcionais do OAIS;

5. Planeamento de Preservação: A entidade OAIS que contém os serviços e funções para a monitorização da ambiente OAIS e para fornecer recomendações para garantir que as informações armazenadas permanecem acessíveis à Comunidade Designada, a longo prazo, mesmo que o ambiente computacional original se torne obsoleto;

6. Acesso: A entidade OAIS que contém os serviços e funções para aceder à informação arquivística custodiada e serviços relacionados.

Com base nestes dados[148], nas variáveis organizacionais definidas por Chiavenato[149] no Modelo de Referência OAIS[150] e outras teorias gerais da gestão[151], Katia Thomaz desenvolve um Modelo de Contextualização de Objectos digitais.

Este modelo de Contexto inclui 12 variáveis de organização.

1. Objecto Digital de Arquivo: objecto digital criado no âmbito de uma actividade, como fim e que faz prova do mesmo, e mantido para o acesso futuro;

2. Suporte de armazenamento: diferentes tipos de materiais físicos em que são gravados e armazenados os objectos digitais de arquivo, como disquetes, disco rígidos, fitas magnéticas e discos ópticos;

3. *Software* de Apresentação: *software* que é necessário para apresentar toda ou parte de um objecto digital de arquivo, de um modo que as pessoas possam compreender;

4. Equipamento de Processamento: *hardware* que é necessário para processar os suportes de armazenamento e executar o *software* de apresentação;

5. Actividade de Manutenção: acção da organização que visa a manter correctamente - em ordem, em execução, actualizado, etc. - o objecto de arquivo digital, o suporte de armazenamento, *software* de apresentação, o *hardware* de processamento e instalação;

[148] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS).
[149] CHIAVENATO, Idalberto – Teoria geral da administração.
[150] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS).
[151] Cft BLAU, Peter; SCOTT, W Richard - Formal organizations: a comparative approach; BOWDITCH, James; & BUONO, Anthony; STEWART, Marcus - A primer on organizational behavior; CHAMPION, Dean - Sociology of organizations; HALL, Richard; TOLBERT, Pamela - Organizations: structure, processes, and outcomes; MIRANDA, Geraldo – Organização e métodos.

6. Actividade de Negócio: uma acção da organização que visa o exercício do negócio da organização;

7. Funcionário: a pessoa, por vezes, um técnico ou um empregado menos qualificado, que realiza a actividade de manutenção;

8. Produtor: uma pessoa ou um sistema cliente que produz o objecto digital de arquivo a ser armazenado;

9. Consumidor: a pessoa ou sistema cliente interessado no objecto digital de arquivo;

10. Terceiros: a pessoa ou organização que faz os produtos, presta serviços, ou certifica (afirmar por declaração formal que é autêntico, preciso, genuíno) um objecto digital, tecnologia e instalações;

11. Instalações: um espaço físico onde está o *hardware* de processamento ou suportes de armazenamento;

12. Gestão: uma estrutura de organização necessária para executar as actividades de manutenção e de negócios;

13. Ambiente: todas as condições, circunstâncias e influências envolventes, e que afectam o desenvolvimento da organização.

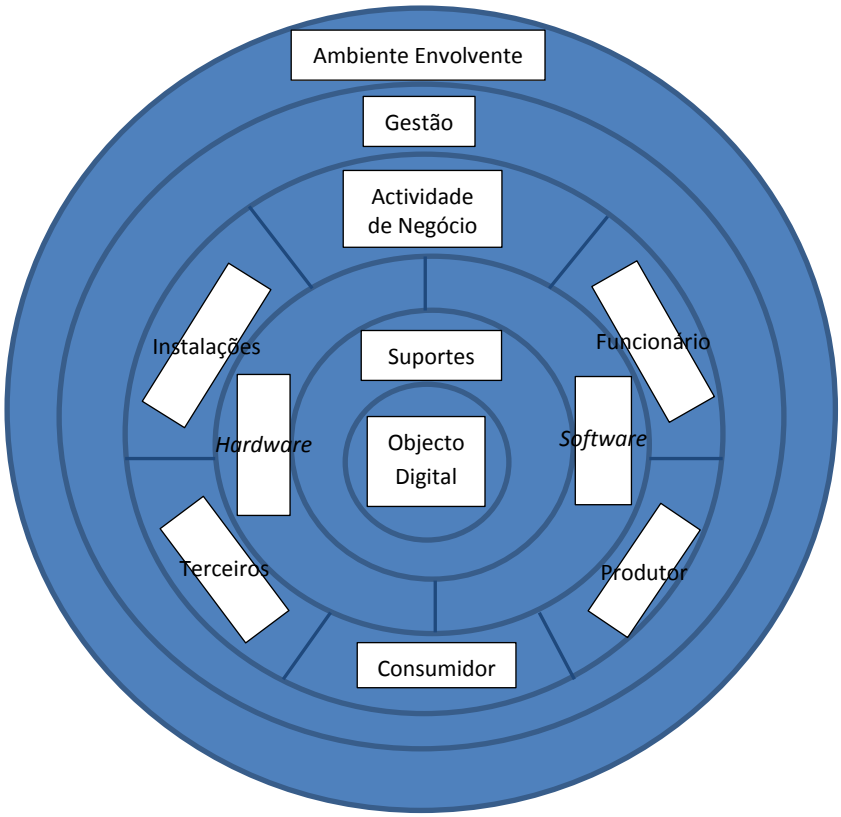

Figura 1 - Modelo de Contextualização de Objectos digitais (Thomaz, 2012)

As relações entre as variáveis da organização mostram como o centro depende da periferia. Na verdade, o objecto de arquivo digital depende do suporte de armazenamento, onde é registado, do *software* de apresentação que o interpreta, no *hardware* de processamento que o lê e processa, da interacção entre a actividade de Manutenção, Actividade de Negócios, funcionário, Produtor, Consumidor, terceiros e as Instalações que o gerem, da gestão para estabelecer políticas de preservação e, finalmente, do ambiente no qual ele é mantido.

O Modelo de Informação começa com a Gestão a gerir as diversas variáveis de organização interna. O Produtor realiza uma ou mais Actividades de Negócio que geram zero ou mais Grupos de Documentos de Arquivo, e alguns deles são definidos como Grupos de Preservação a Longo Prazo. Um Grupo de Preservação a Longo Prazo contém um ou mais Documentos de Arquivo, e alguns desses são Documentos de Arquivo Electrónicos. Um Documento de Arquivo Electrónico é composto de um ou mais Objectos Digitais que são registados em vários Suportes de Armazenamento e são apresentados por *Software* de Apresentação específico, ambos processados por *Hardware* de Processamento compatível. Este complexo tecnológico - Suportes de Armazenamento, *Software* de Apresentação e *Hardware* de Processamento - é mantido por uma ou mais Actividades de Manutenção realizadas por um ou mais Funcionários. Ele também suporta uma ou mais Actividades de Negócios que suportam um ou mais Consumidores. É possível verificar a influência do Ambiente sobre todas as variáveis de organização interna em termos de mudança / evolução, incluindo a própria Administração.

Existem alguns aspectos a destacar no Modelo de Informação:

- a transição de Grupos de Documentos de Arquivo para Grupos de Preservação a Longo Prazo, que envolveria uma tomada de decisão complexa;
- a multiplicidade do Documento de Arquivo e a delimitação dos Objectos Digitais que compõem o Documento de Arquivo;
- as actividades de manutenção, quando não reúnem informação suficiente sobre os componentes tecnológicos, podem levar ao colapso do modelo; e
- a dificuldade em avaliar a influência do Ambiente sobre as várias variáveis organizacionais.

Além disso, a associação do Modelo de Informação com os factores de preservação digital fornece uma ampla compreensão do que é necessário para garantir a preservação cuidadosa de Documentos de Arquivo Electrónicos a longo prazo, tendo em conta as três categorias funcionais de metainformação identificados pelo *Working Group on Preservation Metadata:* [152]

1. Descritiva: facilitar a descoberta da origem e a identificação;
2. Administrativa: apoio à gestão de origem dentro de uma colecção;
3. Estrutural: unir os componentes de objectos de informação complexos.

[152] DALE, Robin [et al.] - Preservation metadata for digital objects: a review of the state of the art : a white paper.

O Modelo de Informação da Preservação Digital e os factores associados oferecem uma visão holística do ambiente digital e fornecem ao profissional e / ou pesquisador da Informação uma análise mais precisa dos seus componentes. Qualquer instância específica de um arquivo digital encontra-se espelhada no modelo de informação, permitindo que cada aspecto mencionado seja objecto de implementação e estudo detalhado, de modo que o pesquisador ou profissional não omita qualquer componente ou perca o sentido do todo.

Este Modelo de Informação reconhece a natureza altamente distributiva dos documentos digitais na organização e a necessidade de implementação de políticas e procedimentos eficazes para apoiar a sua preservação no local. Entre as classes envolvidas na preservação digital de longo prazo, além do convencional triângulo *hardware*-*software*-dados, também considera o funcionário, o fornecedor, o fabricante, o certificador, o Suporte de armazenamento, a sala de informática, a sala de armazenamento, a Administração [gestão] e do Meio Ambiente. Há também uma grande quantidade de factores de preservação digital no interior das categorias, que terão de ser tidos em conta, não importa qual a posição da categoria no Modelo de Informação.

No geral, o Modelo de Informação da Preservação Digital e os factores associados oferecem uma orientação para:

- obtenção de um amplo entendimento das variáveis organizacionais envolvidas na preservação e acesso aos documentos digitais a longo prazo;
- descrever e comparar estratégias de preservação digital actuais e futuras;
- proporcionar uma base que pode ser expandida por outros esforços para lidar com a preservação a longo prazo dos documentos de arquivo que não estão em formato digital (por exemplo, papel, microfilme, etc.); e
- orientar a identificação e produção de novas normas.

Os principais resultados da investigação - Modelo de Informação da Preservação Digital, factores associados e comparações com outros aspectos-chave da literatura preservação digital - representam abordagens inovadoras e originais, e podem constituir ferramentas úteis para a gestão de preservação digital, uma vez que permitem a avaliação dos riscos associados à necessária tomada de decisão. Por exemplo, quando um programa de preservação digital é planeado, os factores negligenciados revelariam automaticamente os riscos correspondentes, ou seja, os factores, questões desafiadoras, as exigências de preservação e / ou funções de arquivamento que eram debilmente ou não considerada. A incerteza reina na ausência de informação.[153] Em contraste, a informação transforma a incerteza em risco, ou seja, na probabilidade de ocorrência de um certo efeito negativo. O risco pode ser melhor previsto e gerido quando há informações suficientes e precisas. Estas ferramentas, uma vez que representam o actual estado-da-arte, devem ser constantemente revistas e actualizadas, para que possam ser adaptadas a novas soluções desenvolvidas pela evolução das tecnologias e dos processos.

[153] GIDDENS, Anthony - As consequëncias da modernidade.

Finalmente, a investigação progrediu da teoria à prática, uma vez que este caminho fornece instrumentos de eficácia concreta. Este facto é relevante, dada a urgência de investigação, discussões e práticas relacionadas aos temas do património e da memória.

3 - Repositórios Digitais

Quando em Junho de 2007, a UNESCO avança com o documento *Towards an Open Source Repository and Preservation System - Recommendations on the Implementation of an Open Source Digital Archival and Preservation System and on Related Software Development*, no âmbito do programa *Memory of the World*. Neste documento declara o seguinte:

> *"for simple digital objects, the solution to digital preservation is relatively well understood, and that what is needed are affordable tools, technology and training in using those systems. (…)*
> *there is no ultimate, permanent storage media, nor will there be in the foreseeable future. It is instead necessary to design systems to manage the inevitable change from system to system. The aim and emphasis in digital preservation is to build sustainable systems rather than permanent carriers.* (…)
> *It is only in finding a solution to this problem that a sustainable approach will be found to meet the needs of many communities."* [154]

Assim, o relatório considera que um sistema de preservação operacional deve ter em conta todas as questões relativas aos repositórios digitais, e que se os repositórios de preservação forem bem planeados, tais sistemas utilizarão soluções de preservação digital já desenvolvidos sem incorrer nos custos da sua criação. A forma como as comunidades, fornecedor e distribuidores *open source* atingem esses objectivos serve de modelo de como um repositório digital sustentável deve funcionar, de forma constante, e ser actualizado e desenvolvido de acordo com as necessidades. De igual modo, muitas instituições culturais, arquivos e organismos de ensino superior têm participado nas comunidades de *software open source* para influenciar a seu favor, e a favor de todo o sector, a direcção do desenvolvimento desse *software*.

Owen (2007) refere que a solução para o problema da preservação do património digital seria o estabelecimento de um novo tipo de instituição patrimoniais para materiais digitais, juntamente com o reconhecimento de que as instituições patrimoniais já existentes devem continuar a tarefa de preservar o património pré-digital, especialmente aquele ligado à alta cultura e à cultura oficial. Este novo tipo de instituições, que poderiam ser nomeadas de Repositórios de Património Digital, seriam instituições de memória para a sociedade digital, englobando objectos digitais de todos os âmbitos (incluindo os seus processos de criação e utilização subjacentes) através dos quais a sociedade se expressa (o tecido digital da sociedade). São novas instituições ao lado de arquivos, bibliotecas e museus, que se baseiam mais em processos de utilização e sociais do que na produção nacional, que se baseiam em critérios de selecção debatidos publicamente, que se baseiam em investimentos financeiros públicos de recolha, armazenamento e manutenção, e que cooperam com o sector privado em termos de serviços de indexação e acesso.[155]

[154] BRADLEY, Kevin; LEI-Junran; BLACKALL, Chris - Towards an open source repository and preservation system, p. 3.
[155] OWEN, John Mackenzie – Preserving the digital heritage: roles and responsibilities for heritage repositories. p. 49.

Nesse mesmo ano, Bradley corrobora essas afirmações, defendendo que o actual paradigma de preservação digital conceptualiza os objectos digitais como partes de uma relação complexa, que modifica continuadamente o seu conteúdo e a sua forma, necessitando constantemente de interagir de novas maneiras com sistemas complexos. Para o autor, a preservação é cada vez mais considerada como acesso sustentado por parte dos repositórios e arquivos digitais, sendo que a ferramenta crítica neste processo, e que é fulcral em qualquer debate actual acerca da preservação digital, é o repositório digital, que idealmente guarda os materiais, fornece acesso, controla as alterações, e mantém a autenticidade do item durante o período de tempo considerado necessário para cada caso particular.[156]

Refere ainda que num ambiente digital sustentável, ocorre o mesmo debate inclusivo, e aqui o termo é utilizado para significar a construção de uma infrastrutura economicamente viável, tanto socialmente como tecnicamente, para manter dados valiosos sem perdas ou degradação significativas. Tal inclui toda a composição sociotécnica do repositório, o valor a curto e longo prazo do material, os custos de empreender uma acção, e o reconhecimento de que não são as tecnologias que mantêm os objectos digitais, mas sim as instituições, utilizando a tecnologia existente. Para ele não é possível preservar informação digital sem uma infrastrutura organizacional, económica, social, estrutural e técnica sustentável, nem é sensato preservar informação sem valor sustentado.[157]

Assim, de acordo com a perspectiva de Carla Ferreira (2011), verifica-se no início do séc. XXI uma alteração do paradigma na preservação digital em que esta:

> "*deixa de estar centrada em acções imediatas, como a preservação dos suportes, para se concentrar em acções a longo prazo e em infra-estruturas técnicas e sociais que assegurem a perenidade dos documentos digitais. Por esta altura, assume principal destaque a investigação na área dos repositórios digitais e dos metadados de preservação.*"[158]

Os repositórios digitais passam a ser o foco da preservação digital na medida em que estes são vistos como a garantia do armazenamento e autenticidade dos conteúdos digitais. Os repositórios digitais vão integrar as problemáticas e soluções técnicas referentes à preservação e autenticidade da informação digital, que só faz sentido guardar tendo em vista o seu acesso aos públicos. A utilização do plural tem implícito que se tratam de públicos com perfis, interesses e necessidades informacionais diferenciadas. A interoperabilidade tem aqui um lugar importante, na medida em que esses públicos integram-se não só indivíduos, mas também instituições que, por intermédio dos seus sistemas aplicacionais, pretendem aceder e captar a informação que necessitam e que se encontra nesses repositórios.

Conceito e Definição

Pretendemos então perceber a que se refere o conceito de repositório digital e que interpretações existem deste termo.

---

[156] BRADLEY, Kevin– Defining digital sustainability, p. 155-156.
[157] BRADLEY, Kevin– Defining digital sustainability, p. 157.
[158] FERREIRA, Carla - Preservação da informação digital : uma perspectiva orientada para as bibliotecas p. 13.

Conseguimos identificar o conceito de Repositório Digital no Relatório publicado em 1996 pela *Task Force on Archiving of Digital Information* da *Commission on Preservation & Access* (CPA)/RLG. Esta Task Force:

> *"envisions the development of a national system of digital archives, which it defines as repositories of digital information that are collectively responsible for the long-term accessibility of the nation's social, economic, cultural and intellectual heritage instantiated in digital form."*[159]

O conceito de repositório de informação digital surge aqui no âmbito dos arquivos digitais.

Em Março de 2000 o RLG e o *Online Computer Library Center* (OCLC) iniciaram uma colaboração para estabelecer quais as características de um repositório digital para organismos de investigação, baseando-se no Modelo de Referência OAIS, que se abordará no capítulo 4. Foi criado um grupo de trabalho para identificar as características e as responsabilidades dos repositórios digitais confiáveis para colecções heterogéneas de grande escala, detidas por organizações culturais. Tal deu origem, em 2002, ao documento *Trusted Digital Repositories: Attributes and Responsibilities*. Para eles:

> *"Repository: An organization that intends to maintain information for access and use."*[160]

Em Portugal, em 2003, Saramago refere que para as instituições que pretendem criar repositórios digitais a longo prazo poderem dar resposta ao problema dos custos da preservação devem existir discussões e consensos ao mais alto nível. A autora considera repositórios digitais os arquivos e bibliotecas digitais que decidiram manter e preservar os seus recursos ou que têm a capacidade de armazenar os recursos de outrem, fornecendo ou não acesso a utilizadores externos.[161]

Wheatley (2004) considera necessário identificar as finalidades da preservação digital no repositório digital para compreender o processo necessário para garantir a preservação a longo prazo dos objectos colocados no repositório, convém antes de mais perceber o que se entende efectivamente por preservação, sendo que as finalidades funcionais se podem resumir a dados que podem ser mantidos no repositório sem degradação, perda ou alterações maliciosas; dados que podem ser localizados, extraídos do arquivo e entregues a um utilizador; dados que podem ser interpretados e compreendidos pelo utilizador; e que essas finalidades devem atingidas a longo prazo.[162]

O autor aborda ainda a questão da estrutura do repositório, no sentido de garantir que o conteúdo do repositório sobreviva à evolução tecnológica, ou mesmo ao próprio repositório ou instituição que o custodia. Para ele, o método ou estratégia passa pelo planeamento por camadas e a escolha de tecnologias estáveis na construção do repositório. Assim, tal como a

[159] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. III.
[160] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 59.
[161] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais, p. 5.
[162] WHEATLEY, Paul - Institutional repositories in the context of digital preservation.

Informação de Representação precisa de ser monitorizada e actualizada tendo em conta o impacto que a obsolescência tecnológica tem nela, os repositórios necessitam eles próprios de se modificar e desenvolver ao longo do tempo. Tal modificação pode ser necessária para garantir o funcionamento continuado do arquivo face às tecnologias que utiliza se tornarem obsoletas, mas também pode derivada da solicitação de novos ou diferentes serviços no âmbito da utilização. A necessidade da sobrevivência do repositório a longo prazo tem que acarretar a ideia de que partes significativas do repositório terão que sofrer modificações.

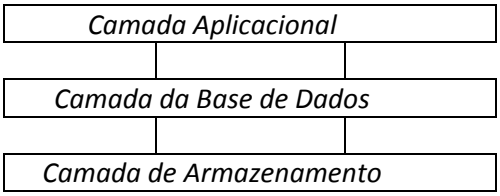

Figura 2 - Abstracção de Repositório

A figura, apresentada pelo autor, apresenta uma abstracção das camadas do repositório. Ao planear cuidadosamente as interfaces entre estas camadas, as tecnologias usadas nas próprias camadas (principalmente nas camadas superior e inferior) podem ser modificadas sem grande impacto para o repositório no seu todo. À medida que os paradigmas técnicos, funcionais e de utilizador da computação moderna se vão modificando (e vão entrando e saindo do estado de graça), temos que que estar cientes de que as aplicações delas dependem também mudarão. Assim, as interfaces externas de visualização actuais não sobreviverão mais de cinco anos na sua presente forma, e muito menos cem anos. Escolher um planeamento de alto nível correcto pode simplificar esta modificação inevitável e talvez prevenir qualquer perda de dados no processo. Ao observar as várias implementações de repositórios institucionais na web verifica-se a existência de vários com avisos relativos ao adicionar conteúdo em sistemas que podem encerrar sem qualquer esperança de migração dos dados para um sistema que o substitua. Os perigos da não abordagem desta questão são por demais evidentes.[163]

No âmbito do *Digital Repositories Programme* do *Joint Information Systems Committee* (JISC), é publicado o *Digital Repositories Review* em 2005, que define, de forma que considera pouco satisfatória, que uma gama cada vez maior de áreas de actividade dentro do ambiente da informação refere-se aos depósitos de colecções de conteúdos como "repositórios", numa perspectiva em que os repositórios são assim considerados colecções de objectos digitais.[164]

Esta entidade considera que para encorajar a comunicação entre estas áreas de actividade e promover a interoperabilidade, é necessário definir as características dos repositórios e procurar uma abordagem comum e coerente, na medida que a utilização generalizada de um termo leva a um aumento da diversidade de significados.[165]

Neste âmbito o JISC financiou, entre 2006 e 2013, o *Repositories Support Project (RSP)*, uma iniciativa que visava contribuir para o desenvolvimento da capacidade, conhecimentos e

[163] WHEATLEY, Paul - Institutional repositories in the context of digital preservation.
[164] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 1.
[165] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 1.

competências no âmbito dos repositórios de instituições de ensino superior do Reino Unido. Nesse sentido define que:

> "*A digital repository is a mechanism for managing and storing digital content.* (…) *Digital repositories may include a wide range of content for a variety of purposes and users. What goes into a repository is currently less an issue of technological or software ability, and more a policy decision made by each institution or administrator.*"[166]

Em 2006 o *Working Group on Trusted Repositories Certification* do NESTOR - *Network of Expertise in long-term STORage*, com participações de várias bibliotecas e arquivos alemães e austríacos produziram a primeira versão do seu *Catalogue of Criteria for Trusted Digital Repositories*, afirmando que um repositório digital se define como uma organização (consistindo em sistemas de pessoas e técnicas) que assume a responsabilidade da preservação e acessibilidade a longo prazo dos objectos digitais, assegurando a sua usabilidade por parte de um grupo-alvo específico, ou "Comunidade Designada". O conceito de "longo prazo" neste conceito significa para além das modificações tecnológicas (de *hardware* e *software*) e também modificações à sua Comunidade Designada. Mais uma vez, esta definição de repositório digital baseia-se na apresentada no Modelo de Referência OAIS.[167]

A segunda versão, de 2008, acrescenta que:

> *"The digital repository can be an element within a larger institution which also archives conventional objects. The connections between analogue and digital objects should be maintained and represented accordingly in the search."*[168]

Miguel Ferreira no seu livro, Preservação Digital, de 2006, refere que:

> *"Repositório digital. Sistema de informação responsável por gerir e armazenar material digital."*[169]

O *International Federation of Library Associations and Institutions* (IFLA), publica, em 2008, *Networking for Digital Preservation: Current Practice in 15 National Libraries*, onde define:

> *"Digital repository or electronic repository is the system (or combination of systems) that provides long-term storage and preservation of and permanent access to digital objects."*[170]

Arellano refere em 2008 que:

> *"Um repositório digital é um serviço de armazenamento de objetos digitais que tem a capacidade de manter e gerenciar materiais por longos períodos de tempo e*

[166] JISC – What is a Repository?. In Repositories Support Project (RSP).
[167] DOBRATZ, Susanne [et al.] – NESTOR catalogue of criteria for trusted digital repositories, p. 2.
[168] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 4.
[169] FERREIRA, Miguel - Introdução à preservação digital, p. 71.
[170] VERHEUL, Ingeborg - Networking for digital preservation, p. 21.

prover o seu acesso apropriado. (…) O propósito dos repositórios estaria dirigido a dois aspectos: o acesso e o armazenamento."[171]

Para este autor:

"Os repositórios digitais compreendem um conjunto de ferramentas necessárias para os produtores, disseminadores e usuários de documentos digitais."[172]

Torna-se claro que os repositórios digitais, na sua essência, são sistemas de informação que têm o intuito de gerir e armazenar colecções de objectos digitais. Esses sistemas de informação são da responsabilidade de um organismo ou instituição, que vai definir a finalidade, os objectivos, os tipos e características dos objectos que armazena, tendo em conta as necessidades e expectativas da comunidade de interesse, potenciais clientes do repositório digital.

Tal é demonstrado pela afirmação do *Digital Curation Centre* (DCC) e o *Digital Preservation Europe* (DPE), que em 2007 criam a ferramenta *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA), de que os repositórios formam um cruzamento de interesses de diferentes comunidades de prática: bibliotecas digitais, investigação, ensino, e-ciência, publicações, exploração de dados comerciais, gestão de documentos de arquivo, preservação. A motivação destas comunidades para criar repositórios pode diferir e os serviços chave que os repositórios podem fornecer abrangem várias áreas funcionais, como o acesso avanço a recursos, novas formas de publicação e revisão de pares, gestão de informação empresarial (sistemas de gestão de conteúdos e de documentos de arquivo); partilha de dados (reutilização de dados de investigação, objectos de ensino-aprendizagem, etc.); preservação de recursos digitais a longo prazo.[173]

Âmbitos de Utilização

Teremos então que verificar o que a literatura científica e técnica nos diz acerca dos âmbitos de utilização dos repositórios digitais, sem no entanto deixar de falar da profusão terminológica e conceptual, já verificada pelo JISC, e dos tipos de repositórios que vão surgindo, de acordo com o *Digital Repositories Programme*.

Repositórios e (/ou) Arquivos Digitais

Precisamos então de voltar ao Relatório da *Task Force on Archiving of Digital Information*, de 1996, que considera que os repositórios de informação digital a que se refere estariam ligados no âmbito de um sistema de arquivo nacional através de dois mecanismos de certificação, em que o primeiro diz respeito aos repositórios que afirmam cumprir funções de arquivo devem fazer prova de que são quem dizem ser, cumprindo ou excedendo os requisitos e normas de um programa independente de certificação de arquivos, e o segundo refere-se aos arquivos digitais certificados que devem ter disponível um mecanismo à prova de falhas críticas, mecanismo esse que deve ser suportado pela vontade, recursos económicos e direitos legais

[171] MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica, p. 124.
[172] MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica, p. 125.
[173] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment – DRAMBORA, p. 15-16.

da organização, e que permite um repositório de arquivo certificado executar uma função de salvaguarda agressiva para salvar informação digital com importância cultural.

Adicionalmente, o mesmo relatório da *Task Force* faz a distinção entre Arquivos Digitais e Bibliotecas Digitais define arquivo digital estritamente em termos funcionais como repositórios de informação digital que são colectivamente responsáveis pela garantia através da utilização de várias estratégias de migração, a integridade e acessibilidade a longo prazo do património social, económico, cultural e intelectual existente em forma digital. Os arquivos digitais distinguem-se das bibliotecas digitais, por estas serem repositórios que recolhem e fornecem acesso a informação digital, mas sem a obrigação de assegurarem o armazenamento e acesso a longo prazo dessa informação, podendo assim, em termos funcionais, ser consideradas ou não arquivos digitais. O documento assinala que muito do trabalho acerca das bibliotecas digitais não aborda as questões arquivísticas de garantia de armazenamento e acesso a longo prazo. Paralelamente, os arquivos digitais abarcam as funções das bibliotecas digitais no que se refere à selecção, obtenção, armazenamento, e fornecimento de acesso à informação digital. Muitos dos requisitos por eles definidos para arquivos digitais justapõem-se aos das bibliotecas digitais.[174]

Face a esta distinção entre estes dois tipos de repositórios, considero importante introduzir algumas definições fornecidas pelo Modelo de Referência OAIS[175], o qual será aprofundado no capítulo 4. Este documento de 2002, considera:

> *"Open Archival Information System (OAIS) - an archive, consisting of an organization of people and systems, that has accepted the responsibility to preserve information and make it available for a Designated Community.*
> (…) *The information being maintained has been deemed to need Long Term Preservation, even if the OAIS itself is not permanent. Long Term is long enough to be concerned with the impacts of changing technologies, including support for new media and data formats, or with a changing user community. Long Term may extend indefinitely."*[176]

Estas definições são importantes porque, desde a sua emergência, tornaram-se incontornáveis, na medida em que a maioria dos documentos futuros passa a mencioná-las, mesmo que por comparação. É o caso do documento, já abordado, do RLG/OCLC, de 2002, o *Trusted Digital Repositories: Attributes and Responsibilities*:

> *"OAIS Reference Model uses "digital archive" to mean the organization responsible for digital preservation; this paper uses "archive" in place of "repository" only when "archive" is taken directly from the OAIS Model."* [177]

[174] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. 8.
[175] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): blue book. p. 1-1.
[176] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. III.
[177] BEAGRIE, Neil, [et al.] - Trusted digital repositories: attributes and responsibilities, p. 3.

Em 2003 é criada a Task Force on Digital da RLG-NARA (*National Archive and Records Administration*), que publica o *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC) em 2007, e refere que os termos repositório digital e arquivo digital são muitas vezes utilizados de forma indistinta, sendo que o OAIS utiliza arquivo quando se refere a um organização que pretende preservar informação para acesso e utilização de uma Comunidade Designada, e que o documento *Trusted Digital Repositories: Attributes and Responsibilities* prefere o termo repositório digital. No entanto o TRAC defende que estes dois termos não se devem confundir seja com as bibliotecas digitais, que coligem e fornecem informação digital, mas que podem não se responsabilizar pela preservação a longo prazo, seja pelos arquivos de dados, que se comprometem com a preservação a longo prazo, mas que limitam as suas colecções a conjuntos de dados estatísticos.[178] Esta será a mesma definição que a *Cornell University Library* utiliza no seu tutorial em linha, desde a sua criação em 2003.[179]

Assinalam assim a existência de uma equivalência entre Repositório Digital, usado pelo RLG/OCLC, e Arquivo Digital, tal como indicado no Modelo de Referência OAIS, e que diferenciam de Bibliotecas Digitais e Arquivos de Dados, definindo este conceitos.

Neste ano, a *Association of Research Libraries* (ARL) marca o surgimento de repositórios institucionais como:

> *"a new strategy that allows universities to apply serious, systematic leverage to accelerate changes taking place in scholarship and scholarly communication, both moving beyond their historic relatively passive role of supporting established publishers in modernizing scholarly publishing through the licensing of digital content, and also scaling up beyond ad-hoc alliances, partnerships, and support arrangements with a few select Faculty pioneers exploring more transformative new uses of the digital medium."* [180]

Por seu lado a UNESCO, ainda em 2003, tentando escapar às ambiguidades no entendimento da definição dos conceitos de arquivo e repositório para os gestores de documentos de arquivo e para os especialistas das Tecnologias [Digitais] da Informação, invoca o termo Programa de Preservação, para substituir os termos arquivo digital e repositório digitais, no sentido de conjunto articulado de operações com o objectivo de preservar materiais digitais, e que inclui todas as responsabilidades da preservação, desde a política, a estratégia, até à execução.[181]

A equivalência entre Repositório Digital e Arquivo Digital é reforçada por Lavoie, que em 2004, afirmava que a definição de sistema de informação de arquivo no Modelo de Referência OAIS enfatiza as funções principais dos repositórios, a de preservar informação, ou seja, garantir a sua continuidade (persistência) a longo prazo, e a de fornecer acesso à informação arquivada

[178] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 75.
[179] CORNELL UNIVERSITY LIBRARY; ICPSR; MIT LIBRARIES - Digital preservation management: implementing short-term strategies for long-term problems.
[180] LYNCH, Clifford - Institutional repositories: essential infrastructure for scholarship in the digital age, p. 1.
[181] WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage, p. 10.

de uma forma consistente com as necessidades dos utilizadores principais do OAIS, ou da Comunidade Designada.[182]

O mesmo autor (2005), especifica mais tarde que:

> *"The OAIS information model is a conceptualization of the information objects taken into, stored, and disseminated by a digital preservation repository."*[183]

No *Digital Repositories Review* de 2005, o JISC, elabora sobre um conjunto de questões que reflectem a diversidade de significados que, até à data, tinham sido utilizados para o termo Repositórios Digitais, dos tipos de repositórios digitais existentes, e que características o distinguiriam dos outros tipos de colecções de objectos digitais: será o repositório gerido como um repositório institucional? Ou repositório temático? Qual o conteúdo do repositório? É um repositório de e-prints? Um repositório de dados? Um repositório de objectos de ensino-aprendizagem? Será o objectivo do repositório a preservação, acesso ou gestão de dados? [184]

Assim defendem que o que caracteriza um repositório é o facto de o conteúdo ser depositado, seja pelo produtor, o proprietário ou por terceiros, da sua arquitectura gerir tanto o conteúdo como a metainformação, de ser capaz de oferecer um conjunto mínimo de serviços básicos, tais como a ingestão, disseminação, pesquisa e controlo de acesso, e, finalmente, ser sustentável e confiável, com um bom suporte e administração.

Em 2005 Barbedo, abordando a questão dos Arquivos Digitais, considera que a Norma OAIS, embora chamada de *Open Archival Information System*, o seu espectro de aplicação não se limita ao material de arquivo, até porque, ao ser a base das experiências executadas por organizações ligadas à biblioteconomia no âmbito da preservação digital, o termo arquivo é deturpado. O autor considera, no entanto, que esta norma tem uma importância fulcral em termos terminológico-conceptuais, de princípios e métodos utilizados no desenvolvimento de repositórios de informação digital e à sua preservação e acessibilidade.[185]

Defende que, no sentido de definir o termo de Arquivo Digital é necessário complementar a definição fornecida pelo Modelo de Referência OAIS:

> *"O Arquivo Digital é pois uma estrutura que compreende tecnologia, recursos humanos e um conjunto de políticas para incorporar, gerir e acessibilizar numa perspectiva continuada objectos digitais de natureza arquivística."*[186]

Paralelamente, Azevedo Pinto, e no âmbito de uma investigação que decorria em 2005 e que incidia sobre programas e projectos de gestão e preservação digital, evoca a seguinte dúvida:

> *"Bibliotecas digitais, arquivos digitais, repositórios. Será nítida a fronteira? Onde começa um e acaba o outro?"* [187]

---

[182] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 3.
[183] LAVOIE, Brain; GARTNER, Richard - Preservation metadata, v.1, p. 9.
[184] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 1.
[185] BARBEDO, Francisco - Arquivos digitais: da origem à maturidade, p. 11-12.
[186] BARBEDO, Francisco – Arquivos digitais: da origem à maturidade, p. 12.
[187] PINTO, Maria Manuela Gomes de Azevedo – Do «efémero» ao «sistema de informação», p. 58.

Face a este panorama conceptual e terminológico, a autora constata:

> *"a ocorrência do termo arquivo/repositório digital como elemento agregador de e-prints, e-journals, e-mails, páginas web, ou simples registos de actos administrativos em bases de dados (…)"*[188]

Esta investigação consistiu no levantamento efectuado por Azevedo Pinto, a nível mundial, de iniciativas, planos, programas e projectos desenvolvidos no período compreendido entre 1995 e 2007. Um dos âmbitos do levantamento era a identificação da percepção que os diversos promotores dessas acções tinham acerca do tipo de repositório que tinham em vista desenvolver, ou gerir, sendo que os valores identificados pela autora, por ordem decrescente, foram: repositório digital; vários; arquivo digital; biblioteca digital; repositório institucional; repositório cultural; arquivo; sítio web especializado; biblioteca; sítio web/plataforma de acesso; sítio web de referência; repositório de preservação; museu/sítios arqueológicos; repositório de *e-learning.*[189]

Neste âmbito a autora refere em 2009 que se verifica o domínio do termo repositório digital, que se sobrepõe aos termos de primeira vaga (arquivo e biblioteca digitais), e que, na sua opinião, engloba repositórios institucionais, de *e-learning* e culturais. Para a autora, e tendo em conta as necessidades de preservação, estes repositórios ultrapassam separações que, ela considera não terem fundamentação teórica, mesmo quando exista e esteja subjacente às acções mapeadas. Autora defende ainda que a posição emergente dos repositórios ligados ao *e-learning* e à preservação se deve à evolução das preocupações das comunidades de interesse nelas envolvidas.[190] A autora sustenta ainda que o segundo lugar do tipo "vários" confirma a existência de parcerias e de consórcios de entidades com o fim de resolverem problemas comuns, mas sem conseguir encontrar necessidades de especificação ou evolução no que se prende com o tipo de sistema de informação que gerem e à sua (re)estruturação.[191]

Com base nisso refere a existência de uma diversidade e dificuldade de especificação de conceitos e dos termos que melhor os definem.[192]

Nesse sentido defende que a dificuldade em definir e distinguir entre biblioteca digital, arquivo digital, repositório institucional e a generalização do uso do termo repositório ligada ao surgimento de parcerias e consórcios com o fim de diminuir as diferenças institucionais, remetem para a "*importância da inclusão da preservação na fundamentação epistemológico-teórica que sustenta a área científica da Ciência da Informação".*[193]

Embora a opinião aqui veiculada não coincida com esta autora, e não sendo as questões epistemológicas o cerne deste trabalho, considero que a investigação referenciada constitui um estudo incontornável do estado da arte desse período.

---

[188] PINTO, Maria Manuela Gomes de Azevedo – Do «efémero» ao «sistema de informação», p. 58.
[189] PINTO, Maria Manuela Gomes de Azevedo - Gestão da informação e preservação digital, p. 335.
[190] PINTO, Maria Manuela Gomes de Azevedo - PRESERVMAP, p. 185.
[191] PINTO, Maria Manuela Gomes de Azevedo - PRESERVMAP, p. 186.
[192] PINTO, Maria Manuela Gomes de Azevedo - PRESERVMAP, p. 151.
[193] PINTO, Maria Manuela Gomes de Azevedo - PRESERVMAP, p. 160.

Não é convincente o argumento de Manuela Pinto, particularmente quando especialistas das TI e com experiência teórico-prática no âmbito de repositórios digitais define, a nosso ver, clara e pertinente, repositórios digitais, tendo por consideração, os seus fins para os quais são utilizados.[194] Outro exemplo que reforça claramente a nossa opinião surgem pela mão de José Carlos Ramalho, que já em 2007, perante a profusão de termos (Bibliotecas Digitais, Arquivos Digitais, Repositórios Digitais, Biblioteca Electrónica, Biblioteca Virtual), define e distingue as Bibliotecas Digitais dos Arquivos Digitais, considerando que estes últimos se diferenciam por conterem essencialmente fontes primárias de informação (cartas, processos judiciais, registos paroquiais, etc.) produzidos directamente por um indivíduo ou organização) em lugar das fontes secundárias normalmente encontradas numa biblioteca (livros, etc.), terem os seus conteúdos organizados em grupos, isto é, os itens são agrupados por proveniência (indivíduo ou instituição criador) e ordem original (ordem mantida pelo criador) e não catalogados individualmente como nas bibliotecas e terem conteúdos únicos, na medida em que os registos de um arquivo são únicos e não podem ser encontrados ou consultados noutro local que não seja o seu arquivo, enquanto um livro pode ser encontrado em várias bibliotecas.[195]

A ferramenta DRAMBORA (2007), que refere as diferentes acepções do termo Repositório Digital, aponta que a especificidade da definição dada pelo Modelo de Referência OAIS se prende com a manutenção da compreensibilidade do material digital a longo prazo, mas que a maioria dos repositórios tinha, à data, somente preocupações ligadas ao acesso e utilização a curto-médio prazo, não tendo recursos ou obrigações, ou responsabilidades para preservação a longo prazo, pelo que os critérios e atributos para certificação de repositórios não estão orientados para eles, mas podem-lhes ser úteis.[196]

De facto, também autoras como Astrid Recker[197] e Julie Allinson[198] verificam que muitos repositórios não reconhecem a preservação como a sua função principal, derivado do desconhecimento das ameaças e perdas que podem ocorrer no futuro e por considerarem mais premente a necessidade de aumentar o conteúdo nos repositórios.

Em 2008 o *Digital Preservation Europe* (DPE), lança o PLATTER (*Planning Tool for Trusted Electronic Repositories*), que partindo de uma referência similar ao DRAMBORA, refere diferentes utilizações do termo Repositório Digital e que passam por identificar coleções digitais que implementam um modelo (OAIS) ou protocolo (OAI-PMH), ou uma organização responsável pela gestão de material digital para uma dada Comunidade Designada de utilizadores finais, ou, finalmente, um conjunto de serviços ligados à aquisição, gestão e disseminação de material digital, de especial relevância quando os serviços são geridos por várias instituições que trabalham numa estrutura federada.[199]

De igual forma, reconhecem a existência de repositórios de vários tipos, e que terão interesse no seu documento:

[194] Cf. FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital.
[195] RAMALHO, José Carlos - Repositórios digitais.
[196] MCHUGH, Andrew [et al.] – DRAMBORA, p. 10.
[197] RECKER, Astrid - The preservation of digital objects in german repositories, p. 7.
[198] ALLINSON, Julie - OAIS as a reference model for repositories: an evaluation, p. 4-5.
[199] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 8.

> *"common to repositories of many types – for example national libraries and archives, institutional repositories, subject-based repositories and scientific data archives."*[200]

Astrid Recker (2010) defende que o termo "repositório" é ambíguo, pelo que os repositórios considerados como tal pelos vários documentos com critérios de certificação de repositórios, são arquivos digitais de longo prazo, e que um subgrupo desses arquivos digitais podem ser repositórios temáticos ou institucionais. No entanto, estes podem não ter capacidade ou vontade de fornecer serviços de preservação a longo prazo, sendo assim arquivos de curto ou médio prazo, em que o termo "arquivo" é visto como uma coleção de informação.[201]

Em 2011 o CCSDS publica o *Audit and Certification of Trustworthy Digital Repositories*, onde se enfatiza, mais uma vez, a relação entre os termos Repositório Digital e Arquivo Digital, enquanto repositórios com responsabilidades e funcionalidades de preservação a longo prazo. Outro elemento distintivo face aos outros repositórios prende-se com as necessidades (e expectativas) da Comunidade de Interesse, que pode ser uma única e generalista, ou então podem ter várias comunidades designadas, como necessidades altamente especializadas, cada uma necessitando de diferentes funcionalidades ou apoio do repositório.[202]

Apesar desta aparente ambiguidade, surge no panorama internacional, intimamente relacionados com os esforços de certificação e garantia de fidedignidade nos repositórios, propostas que permitem a identificação tipológica e caracterização dos repositórios digitais, por parte dos mesmos. Nesse sentido, o PLATTER (2008) apresenta, no âmbito da planificação das finalidades, objectivos, e metas de desempenho, uma abordagem que permite caracterizar o repositório em termos de Objectivo e Funções, Dimensão, Funcionamento e características do material custodiado, soluções técnicas e implementações escolhidas.[203] Outras propostas ligadas a projectos e grupos de trabalho com valências similares serão apresentadas nos capítulos 4 e 5.

Em Janeiro de 2007, o *Center for Research Libraries* (CRL) organizou uma reunião de projectos de desenvolvimento de normas e mecanismos de apoio à auditoria, certificação e acreditação de repositórios. Esta reunião, em que também participaram o *Digital Curation Center* (DCC), o *Digital Preservation Europe* (DPE) e o NESTOR (*Network of Expertise in Long-term STOrage of Digital Resources*) resultou no desenvolvimento de um conjunto comum de critérios que todos os repositórios de preservação digital devem seguir, independentemente da sua missão, modelo de negócio e fonte de financiamento.[204] Estes serão apresentados no capítulo 5.

[200] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 10.
[201] RECKER, Astrid - The preservation of digital objects in german repositories: three case studies, p. 10.
[202] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book, p. 1-4.
[203] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 10.
[204] Cft. CENTER FOR RESEARCH LIBRARIES (CRL) - Ten principles; MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment – DRAMBORA, p 16.

Em 2012 é publicado em Portugal o relatório *Estado da Arte em Preservação Digital*[205], no âmbito do projecto *Repositório Científico de Acesso Aberto de Portugal* (RCAAP), que faz uma panorâmica geral do tema da preservação digital, e contextualizando-o no âmbito dos repositórios de acesso aberto.

O autor refere ainda a existência de um debate entre os que defendem a importância da preservação nos repositórios para aumentar a sua fidedignidade e aqueles que defendem a prioridade em aumentar o volume de conteúdos, considerando os repositórios como apenas um meio de acesso, de entre vários, e que a preservação deve ser assumida pelos editores dos artigos científicos.[206]

Repositórios de Acesso Aberto

Numa abordagem muito sintética acerca dos Repositórios de Acesso Aberto, apoiamo-nos na explicação de Mary M. Case (2003), segundo a qual a *Open Archives Initiative* (OAI) desenvolve e promove normas de interoperabilidade que pretendem facilitar a disseminação dos conteúdos. O *OAI Metadata Harvesting Protocol* permite que serviços de terceiros recolham metainformação normalizada de vários repositórios e efectuem pesquisas sobre a Metainformação angariada para identificar e recuperar documentos. Para autora, embora muitos partidários do OAI defendam o acesso livre, (ou seja, a existência de obras gratuitas na Internet), o enquadramento e as normas tecnológicas fundamentais do OAI são independentes tanto do tipo de conteúdo oferecido, como dos modelos económicos que envolvem esse conteúdo.[207]

O Protocolo *Open Archives Initiative Protocol for Metadata Harvesting* (OAI-PMH) é um protocolo desenvolvido pela *Open Archives Initiative* a partir de 1999, utilizado para distribuir e recolher metainformação principalmente no que concerne a descritores de documentos.

Neste âmbito, Miguel Ferreira[208] refere que os repositórios de acesso aberto foram inicialmente concebidos como um modo de fornecer acesso imediato e amplo a trabalhos de investigação científica, mas têm vindo a assumir o papel de curadores dessa produção científica, obrigando à adopção de políticas e ferramentas específicas para a sua preservação e curadoria. O autor indica que o primeiro repositório de acesso aberto, o *arXiv*, surge no início da década de 90 do século passado nos EUA e foi concebido inicialmente como um arquivo para *preprints*.[209]

Repositórios Institucionais e/ou Temáticos

Não querendo cingir-nos somente ao repositório digital como "Arquivo Digital" dedicado à preservação a longo prazo, e por considerarmos que a abordagem acerca dos repositórios digitais não ficaria completa sem elucidar sobre as especificidades Repositórios Institucionais e

[205] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital.
[206] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 7-8.
[207] CASE, Mary – Framing the issue: open access, p. 10.
[208] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 26.
[209] *Preprints* refere-se ao texto digital de um artigo que ainda não foi avaliado e revisto por pares (*peer-reviewed*) e ainda não foi aceite para publicação por uma revista científica.

as Bibliotecas Digitais tentaremos analisar estudos de autores que se debruçaram sobre esta área.

Segundo Miguel Ferreira, a generalização do uso de tecnologias digitais nas universidades e centros de investigação e as alterações que têm decorrido nas formas de armazenamento, acesso e partilha da informação das actividades científicas, desde dados primários até artigos de revistas, levaram a um crescimento de dimensão e complexidade, em sintonia com a evolução do meio científico. Pela importância e valor dessa informação, ela deve ser preservada para garantir a maximização no investimento, a reutilização do conhecimento, garantir a sua fiabilidade e para conservar a memória organizacional.[210]

O Relatório da *Task Force on Archiving of Digital Information* CPA/RLG, 1996 refere que as instituições de investigação científica e académicas necessitam de uma infrastrutura apropriada capaz de apoiar um sistema de arquivos digitais:

> *"Long-term preservation of digital information on a scale adequate for the demands of future research and scholarship will require a deep infrastructure capable of supporting a distributed system of digital archives."*[211]

Crow (2002) define repositórios institucionais como colecções digitais que capturam e preservam os resultados da produção intelectual das comunidades universitárias. Para este autor estes repositórios são essenciais para estimular a inovação nas comunicações nas áreas académicas e como indicador da qualidade da instituição, medida em termos de visibilidade, prestígios e valor para o público.[212]

Esta ideia é corroborada por Lynch (2003), que considera, como já vimos anteriormente, que o desenvolvimento de repositórios digitais se trata de uma nova estratégia que permite às universidades aplicar uma alavancagem séria e sistemática que acelere as mudanças que têm vindo a ocorrer na comunicação académica e de investigação, que estão a ultrapassar o seu papel historicamente passivo de apoio aos editores já estabelecidos, ao modernizar as publicações académicas pelo licenciamento de conteúdo digital, e ir para além das alianças e parcerias *ad-hoc* e apoiar acordos com algumas Faculdades pioneiras na exploração de novas utilizações mais transformadoras do suporte digital.[213]

Este autor apresenta a seguinte definição:

> *"…a university-based institutional repository is a set of services that a university offers to the members of its community for the management and dissemination of digital materials created by the institution and its community members. It is most essentially an organizational commitment to the stewardship of these digital*

[210] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 26.
[211] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. 40.
[212] CROW, Raym - The case for institutional repositories: a SPARC position paper, p. 2.
[213] LYNCH, Clifford - Institutional repositories: essential infrastructure for scholarship in the digital age, p. 1.

materials, including long-term preservation where appropriate, as well as organization and access or distribution."[214]

Nesse mesmo ano, e mais concretamente no Brasil, Café, juntamente com Arellano e outros (2003), defendem que:

"Um repositório institucional é a reunião de todos os repositórios temáticos hospedados em uma organização." [215]

Arellano (2008) irá mais tarde diferenciar vários tipos de repositórios digitais, avançando com definições para cada um deles: os repositórios temáticos dizem respeito a uma área do conhecimento; os repositórios institucionais são sistemas de informação que armazenam, preservam e disseminam a produção intelectual das instituições e comunidades científicas em formato digital; os repositórios centrais fornecem serviços de reunião de dados coligidos de bibliotecas digitais, repositórios temáticos e repositórios institucionais, a nível nacional ou internacional.[216]

Curiosamente Kingsley[217] (2008) e Astrid Recker[218] (2010) diferenciam repositórios institucionais e repositórios temáticos. O primeiro autor refere que nos repositórios institucionais, as políticas de selecção e retenção de material, bem como o foco e organização geral do repositório, é determinado pela instituição, enquanto nos repositórios temáticos as políticas de depósito são determinadas pelas comunidades de investigação. A autora alemã reforça esta ideia considerando que os repositórios institucionais e temáticos diferem na aceitação que têm por parte das respectivas comunidades alvo. Ela considera também que a definição de repositórios institucionais de Lynch também se aplica aos repositórios temáticos, excepto que estes prestam serviços a uma comunidade de académicos que não está delimitada institucionalmente, mas pelo seu trabalho na mesma área científica. Finalmente, ela considera que Salo[219] (2007), muito embora não aborde os repositórios temáticos, detalha várias razões pelas quais os investigadores hesitam em depositar conteúdos em repositórios institucionais.

Wheatley (2004) parte da definição repositórios institucionais dada por Lynch, considerando que:

"*The term institutional repository implies a community based service although this is interpreted by repository developers in different ways. Some embody a cross-subject, cross-department service which requires flexibility to meet the requirements of many different types of users. Some focus more specifically on a*

[214] LYNCH, Clifford - Institutional repositories: essential infrastructure for scholarship in the digital age, p. 2.
[215] CAFÉ, L., [et al.] - Repositórios institucionais: nova estratégia para publicação científica na rede, p. 13.
[216] MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica, p. 124.
[217] KINGSLEY, Danny - Those who don't look don't find: disciplinary considerations in repository advocacy, p. 3.
[218] RECKER, Astrid - The preservation of digital objects in german repositories: three case studies, p. 10.
[219] SALO, Dorothea - Inkeeper at the roach motel.

particular subject and possibly type of material to be archived, while still delivering an institution-wide service."[220]

O autor considera que, muito embora o termo repositório institucional sugira um contexto de ensino superior, nem sempre é o caso, visto que as instituições com necessidades de armazenamento, preservação e fornecimento de acesso a materiais digitais podem necessitar de ter os seus próprios repositórios, algo que, para o autor, será cada vez menos incomum. Para ele, o termo repositório institucional pode referir-se simplesmente a uma instância de um repositório institucional ou ao *software* que torna possível a existência do repositório institucional.[221]

O JISC, no *Digital Repositories Review* 2005, apoiando se em Lynch, considera que um dos principais motores para criação de repositórios, sejam repositórios institucionais ou repositórios temáticos, é a melhoria do acesso na comunicação a nível académico. Nesse âmbito defendem que os repositórios devem suportar o "acesso aberto". Para eles, os Repositórios de Acesso Aberto distinguem-se por fornecer acesso aberto ao seu conteúdo (a menos que haja limitações legais) e à metainformação para extracção (colheita) [Harvest].[222]

Na óptica do *Repositories Support Project* (RSP) os repositórios digitais têm um grande potencial para serviços de valor agregado e oferecem um leque de benefícios aos investigadores, instituições, e comunidade de investigação a nível global. Para eles, os repositórios de acesso aberto oferecem vantagens adicionais, ao recolher os resultados da investigação científica que já foram pagos e torná-los acedíveis em linha e gratuitamente, o que é vantajoso para autores, investigadores, instituições e para o processo de investigação, na medida em que permite uma melhor gestão dos resultados dos produtos intelectuais e libertar (leia-se facilitar) o processo de disseminação.[223]

O documento do JISC revela ainda que um número significativo de registos em repositórios institucionais são compostos apenas por metainformação, sem qualquer ligação ao texto completo. Isto parece ser devido ao cuidado especial relativamente a direitos de autor e direitos de propriedade intelectual. Os administradores de repositórios e os autores têm relutância em entrar em conflito com os editores sobre direitos de autor por isso não incluem texto completo, quando houver dúvida sobre direitos de autor. Além disso, alguns repositórios apenas incluem hiperligações para o texto completo para as entradas publicadas e / ou de autoria, enquanto o autor fizer parte da instituição.[224]

Para o JISC, outro elemento que diferencia os repositórios das outras colecções, são as motivações subjacentes à sua criação, na medida em que resultam de um cruzamento de interesses de diferentes comunidades de prática: bibliotecas digitais, pesquisa, aprendizagem, e-ciência, edição, gestão documental, preservação. A motivação do foco nos repositórios difere nessas comunidades, e os serviços essenciais que os repositórios podem proporcionar

[220] WHEATLEY, Paul - Institutional repositories in the context of digital preservation.
[221] WHEATLEY, Paul - Institutional repositories in the context of digital preservation.
[222] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 2.
[223] JISC – Benefits. In Repositories Support Project (RSP).
[224] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 13.

variam ao longo de áreas que passam pela melhoria do acesso aos recursos, por novas modalidades de publicação e revisão por pares, pela gestão da informação organizacional (sistemas de gestão de documentos de arquivo e de gestão de conteúdo), pela partilha de dados (reutilização dos dados de investigação e dos objectos de aprendizagem), e pela preservação dos recursos digitais. Sustentam esta ideia atentando à definição dada por Lynch que, segundo eles, denota uma ênfase na importância desses serviços e não num produto de *software* ou tipo de conteúdo específico.[225]

O JISC[226] sugere ainda uma simples tipologia de repositórios:

- por tipo de conteúdo, onde engloba dados primários de pesquisa, dados de pesquisa derivados, artigos académicos pré-publicados, artigos avaliados pelos pares em versões finais de revistas ou actas de conferências, teses em formato electrónico, publicações originais como relatórios técnicos institucionais ou departamental, objectos de ensino-aprendizagem, documentos de arquivo da organização, como processos de alunos e de funcionários, licenças, etc.;

- por área de cobertura, que pode ir desde o pessoal (arquivo pessoal do autor), revista (o resultado do produto de uma revista ou grupo de revistas), até departamental, institucional, interinstitucional (regional), nacional e mesmo internacional;

- por função principal do repositório, que inclui o realce no acesso aos recursos (pesquisa e localização de recursos), acesso aos recursos por temas; preservação de recursos digitais; novas formas de disseminação (ou publicação), gestão de bens da instituição, e partilha e reutilização de recursos;

- por grupo de utilizadores alvo, que vai desde os discentes aos professores e investigadores.

Na esteira de Crow, Helen Hockx-Yu (2006) sustenta que um repositório institucional armazena e torna acessível os bens educacionais, de pesquisa e associados de uma instituição, e que embora a maioria dos repositórios institucionais existentes à data eram repositórios de publicações electrónicas [e-prints] que fornecem acesso aberto aos resultados da investigação científica da instituição, o seu conteúdo não tem que se limitar a esses artigos publicados, podendo incluir dados primários de pesquisa, materiais de ensino-aprendizagem e outros tipos de conteúdo.[227]

A autora considera a falta de consenso quanto ao nível de responsabilidade que os repositórios digitais devem ter pela preservação na medida em que alguns defendem que os fins dos repositórios institucionais de acesso aberto se limitam ao acesso, utilização e impacto, por considerarem que a preservação dos artigos científicos da instituição que foram publicados é uma responsabilidade da editora e das bibliotecas de depósito legal, não devendo ser assim, uma motivação para o arquivo desses materiais. Do outro lado, surgem os

[225] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 2.
[226] HEERY, Rachel; ANDERSON, Sheila - Digital repositories review, p. 13-14.
[227] HOCKX-YU, Helen – Digital preservation in the context of institutional repositories, p. 1.

defensores da preservação a longo prazo como uma das funções que deve ser abordada logo de início pelos repositórios institucionais.[228]

Arellano (2008) apoia-se em Lynch, ao afirmar que as universidades, por todo o mundo, têm adoptado esta forma de publicação para divulgar os resultados das pesquisas científicas e desenvolvem políticas institucionais para legitimação dos seus repositórios de acesso aberto como detentores de produção científica reconhecida.[229]

Por sua vez Carla Ferreira (2011) baseia-se em Lynch[230] no contexto da infrastrutura dos repositórios digitais, indicando que no contexto da preservação, estes fornecem mecanismos para identificação persistente dos documentos, uniformização de formatos e atribuição de metainformação descritiva, de localização, gestão de direitos de autor e das alterações sobre os documentos, acções estas que são garantia de uma boa gestão das mudanças tecnológicas, aplicação de estratégias de preservação e automatização de processos. A autora dá o exemplo da migração, que assim se torna mais simples, rápida e menos dispendiosa quando aplicada a documentos com características comuns.[231]

Miguel Ferreira (2012) refere que se verifica, tanto a nível nacional como a nível externo, a existência de repositórios institucionais que recolhem uma grande percentagem da produção científica dos seus membros, informação essa que não é publicada externamente, pelo que os repositórios se tornam o local original, principal e mesmo único de publicação, defendendo por isso que a preservação digital deve ser uma preocupação futura destes repositórios.[232]

Este autor refere ainda que após o surgimento das plataformas para repositórios desenvolveram-se ferramentas de preservação, que vão desde a elaboração de planos de preservação, políticas de extracção de metainformação de preservação de ficheiros, juntamente com arquitecturas que permitem a ligação modular destas ferramentas. Para o autor, a diversidade de projectos e iniciativas que têm decorrido neste domínio demonstram o aumento da notoriedade e relevância que tem tido a preservação e curadoria no contexto dos repositórios institucionais.[233]

Ernesto Candeias Martins[234] (2013) considera o Repositório como imagem de marca e objecto de aprendizagem em meio digital. Parte do conceito de 'repositório' como lugar onde se guarda algo, armazena Dados e/ou trabalhos científicos em rede informática / sistema digital. Neste âmbito a utilidade do Repositório Científico repousa na actividade de aprender e partilhar. Para o autor, os repositórios são lugares criados para depositar / armazenar os objectos de aprendizagem que demonstram ter qualidade de conteúdos, uma adequação dos

[228] HOCKX-YU, Helen – Digital preservation in the context of institutional repositories, p. 3.
[229] MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica, p. 124-125.
[230] LYNCH, Clifford - Institutional Repositories: Essential Infrastructure for Scholarship in the Digital Age, p. 6-7.
[231] FERREIRA, Carla - Preservação da Informação Digital : uma perspectiva orientada para as bibliotecas, p. 72.
[232] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 8.
[233] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 29.
[234] MARTINS, Ernesto - O repositório: imagem de marca e objeto de aprendizagem em meio digital.

objectivos, uma retroalimentação e adaptabilidade, capacidade de motivar e gerar interesse em quem pesquisa. O repositório *online* pretende consolidar competências na procura/busca de objectos de aprendizagem, efectivar a socialização activa entre investigadores, docentes, alunos e utentes da comunidade educativa, tendo relevância no contexto das instituições do ensino superior. O Repositório será o objecto de aprendizagem nas bibliotecas digitais especializadas, onde se deposita e se gere os recursos digitais.

O autor considera ainda os repositórios institucionais, que diz serem sítios na Web que recolhem, preservam e difundem a produção científica académica duma instituição, permitindo o acesso a objectos digitais que contêm, com os seus meta-dados. O objectivo destes repositórios é favorecer a difusão dos conteúdos académicos da instituição, dar visibilidade à investigação realizada na instituição pelos seus membros, facilitar a conservação e preservação dos objectos documentais criados, armazenados e organizados. Trata-se de uma forma de difusão nos sistemas digitais de difundir a sua produção científica por áreas de conhecimento.

Bibliotecas Digitais

O termo Biblioteca digital foi utilizado pela primeira vez em 1994 pela *Digital Libraries Initiative* da NSF (*National Science Foundation*), DARPA (*Defense Advanced Research Projects Agency*) e NASA (*National Aeronautics and Space Administration*).[235]

De acordo com Candela (2011):

> "*Vannevar Bush*[236] *devised "a device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility."*"[237]

Arms (2000) [238] define bibliotecas digitais como:

> *"a managed collection of information, with associated services, where the information is stored in digital formats and accessible over a network. A key part of this definition is that the information is managed. (…) Digital libraries contain diverse collections of information for use by many different users."*

O autor identifica semelhanças e diferenças entre as bibliotecas digitais e as bibliotecas ditas tradicionais:

> *" In some ways, digital libraries are very different from traditional libraries, yet in others they are remarkably similar.(…) They still create information that has to be organized, stored, and distributed. They still need to find information that others have created, and use it for study, reference, or entertainment. However, the form*

[235] FOX, Edward - The digital libraries initiative - update and discussion.
[236] BUSH, Vannevar - As we may think.
[237] CANDELA, Leonardo; CASTELLI, Donatella; PAGANO, Pasquale - History, evolution and impact of digital libraries, p. 2.
[238] ARMS, William - Digital libraries.

in which the information is expressed and the methods that are used to manage it are greatly influenced by technology and this creates change."

Para além disso enumera ainda um conjunto de aspectos positivos decorrentes das bibliotecas digitais, na medida em que facilitam e aumentam a utilização da biblioteca sem ter que sair da secretária, estando apenas dependentes de um computador e rede, que são utilizados para pesquisa e descoberta da informação, que podem ser partilhadas e disponibilizadas a todos, sem custos de duplicação física ou de inacessibilidade. A informação pode actualizar-se facilmente e leva ao surgimento de novos tipos de informação, como bases de dados, que podem registar e disseminar informação passível de ser analisada e manuseada de uma maneira melhor e mais fácil do que a pesquisa em suporte papel.

A DELOS, uma rede de excelência sobre Bibliotecas Digitais parcialmente financiada pela Comissão Europeia no quadro do Programa de Tecnologias da Sociedade da Informação, produziu em 2001, um *Brainstorming Report* em que defende que:

"Digital libraries should enable any citizen to access all human knowledge any time and anywhere, in a friendly, multi-modal, efficient, and effective way, by overcoming barriers of distance, language, and culture and by using multiple Internet-connected devices."[239]

Na sua perspectiva:

"The potential exists for digital libraries to become the universal knowledge repositories and communication conduits of the future, a common vehicle by which everyone will access, discuss, evaluate and enhance information of all forms. Furthermore, we see the potential for digital libraries to become the strongest shield of humanity protecting its historic, cultural and scientific artefacts from time, natural disasters, thieves, vandals and terrorists."[240]

Saramago(2003), baseando-se na rede DELOS, define Biblioteca digital como:

"uma colecção de recursos electrónicos de informação proveniente de uma variedade de fontes, incluindo a Web."[241]

A autora refere que são estruturas de bibliotecas digitais cuja criação espelha os modelos das bibliotecas convencionais, museus, arquivos e repositórios digitais, e que podem armazenar qualquer tipo de recurso digital, cumprindo com as funções de divulgação e acesso a longo prazo.[242]

Saramago parte das orientações dadas pela rede DELOS, para definir uma biblioteca digital quanto aos seus objectivos, que são a oferta de serviços integrados para acesso a recursos em

[239] DELOS ASSOCIATION - Digital libraries: future directions for a european research programme, p. 5.
[240] IOANNIDIS, Yannis - Digital libraries at a crossroads, p. 265.
[241] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: Estado da Arte e Boas Práticas em Repositórios Digitais, p. 10.
[242] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: Estado da Arte e Boas Práticas em Repositórios Digitais, p. 16.

colecções culturais ou científicas, podendo basear-se em sistemas tradicionais ou em novas estruturas que aproveitam as potencialidades do ambiente tecnológico.[243]

De acordo com a autora, a funcionalidade dos serviços integrados assenta em pressupostos como as necessidades de informação de grande qualidade, que esteja relacionada em fontes diversas e dispersas, que seja heterogénea, cujas fontes sejam ricas e fiáveis, seja multimédia, e com uma comunidade de utilizadores definida, e composta por utilizadores motivados. A orientação deve ser dada por domínios do conhecimento, com acessos em várias línguas, e sempre baseada no espírito colaboração que se consubstancie em protocolos de cooperação.

Quanto aos propósitos e tempo de vida, Saramago refere que as bibliotecas são procuradas no âmbito da investigação e aprendizagem, devendo fornecer acesso a informação preservada a médio-longo prazo, de acordo com as necessidades dos utilizadores.[244]

Borbinha (2004), no âmbito da iniciativa *BND – Biblioteca Nacional Digital*[245] da *BN – Biblioteca Nacional de Portugal*, identifica os principais problemas no depósito de obras digitais em bibliotecas patrimoniais, no âmbito de conteúdos concebidos apenas para a Internet, muitas vezes assentes em sistemas de publicação digital complexos e sofisticados, no âmbito de conteúdos concebidos para distribuição tanto pela Internet como pelos meios tradicionais, produzidos em ambiente digital mas de complexidade menor que os anteriores, e no âmbito de conteúdos concebidos somente para distribuição tradicional, como a impressão, mas que a parte final do processo é desenvolvida recorrendo a processos digitais.[246]

O autor chega mesmo a defender que:

> "*na realidade toda a informação e conteúdos que circulam hoje em dia na nossa sociedade existiram algures em formato digital. Levando esta constatação às suas últimas consequências, devemos então reconhecer que os problemas do depósito e preservação digital não devem ser encarados já como uma excepção, mas talvez como a regra.*"[247]

Arellano (2008) defende que a relação e especificidades entre as bibliotecas digitais e os repositórios digitais, definindo ambos os termos, considerando os repositórios digitais como responsáveis colectivamente pela garantia da integridade e acesso de longo prazo do património da sociedade, por intermédio de estratégias de preservação, enquanto que a biblioteca digital é um repositório que colige e fornece acesso à informação digital, sem a obrigação de garantir o armazenamento a longo prazo e o acesso à informação, pelo que, em seu entender, muitas bibliotecas digitais podem ou não ser repositórios digitais, mas os repositórios digitais realizam algumas funções da biblioteca digital (selecção, obtenção,

[243] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: Estado da Arte e Boas Práticas em Repositórios Digitais, p. 16.
[244] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: Estado da Arte e Boas Práticas em Repositórios Digitais, p. 17.
[245] PORTUGAL. Biblioteca Nacional – BND: Biblioteca Nacional Digital.
[246] BORBINHA, José – Depósito e preservação na Biblioteca Nacional Digital, p. 1.
[247] BORBINHA, José – Depósito e preservação na Biblioteca Nacional Digital, p. 1.

armazenamento e fornecimento de acesso), pelo que pode ser considerados parte da infra-estrutura de serviços das bibliotecas digitais.[248]

Este autor, apoiando-se em Arms (2000), refere que uma biblioteca digital pode incluir sistemas de *software* aplicacional para estruturar uma colecção digital, gerindo e administrando os recursos digitais antes do seu depósito e publicação. Tais ferramentas influenciam a forma de preservação dos documentos e custos associados. A gestão dos sistemas informáticos das bibliotecas digitais não se limita às funções e actividades das bibliotecas tradicionais (aquisição, selecção, classificação, armazenamento), incluindo as questões ligadas à interoperabilidade dos acervos digitais em termos de arquitecturas, metainformação, e formatos normalizados, que já são tidas em conta no desenvolvimento destes sistemas para fins e comunidades específicas.[249]

Em 2011 é publicado um *Modelo de Referência da Biblioteca Digital,* no contexto de uma parceria entre a DELOS e a *DL.org: Coordination Action on Digital Library Interoperability, Best Practices and Modelling Foundations*, que define: Biblioteca Digital, Sistema de Biblioteca Digital e Sistema de Gestão de Biblioteca Digital. Assim, para eles, Biblioteca digital é uma organização potencialmente virtual, que colecta, gere e preserva a longo prazo, de forma aprofundada, conteúdos digitais enriquecidos, e que oferece funcionalidades especializadas sobre esse conteúdo às comunidades de utilizador alvo, com qualidade especificada de acordo com políticas definidas aprofundadamente. Um sistema de biblioteca digital é um sistema *software* baseado numa arquitectura para distribuição e que fornece todas os elementos necessários para uma biblioteca digital. Os utilizadores interagem com uma biblioteca digital através do respectivo sistema de biblioteca digital. O sistema de gestão de biblioteca digital é um sistema genérico de *software* que fornece a infrastrutura de *software* apropriada para produzir e administrar um sistema de biblioteca digital que incorpora o conjunto de funcionalidades consideradas fundamentais para as bibliotecas digitais, e integrar *software* adicional que forneça funcionalidades mais refinadas, especializadas ou avançadas.[250]

Para Carla Ferreira (2011) uma das missões das bibliotecas é a preservação da memória colectiva, garantindo o acesso às gerações futuras da documentação literária e científica, pelo que a preservação digital deve ser considerada uma actividade complementar aos serviços prestados pelas bibliotecas, numa perspectiva diferente da preservação tradicional, em que a gestão das colecções digitais assume uma importância maior no âmbito da gestão das colecções.[251]

A autora, baseando-se em Gladney, refere que a maioria dos bibliotecários considera que a preservação digital incorre em problemas que passam pela incapacidade de definir por onde começar a acção, pela falta de conhecimentos especializados, a inexistência de ferramentas confiáveis e de fácil utilização, e também a incapacidade de determinar custos.[252]

[248] MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica, p. 124.
[249] MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica, p. 122.
[250] CANDELA, Leonardo [et al.] - The digital library reference model, p. 17.
[251] FERREIRA, Carla - Preservação da informação digital: uma perspectiva orientada para as bibliotecas, p. 17.
[252] Cft GLADNEY, Henry – Preserving digital information, p. 44.

Mas a autora considera que, apesar disso, o contexto digital não pode ser sinónimo de ameaça, mas uma oportunidade para as bibliotecas, se redefinirem e assumirem-se como instituições incontornáveis da Sociedade da Informação. As tecnologias da informação ajudarão a cumprir a sua missão de fornecimento de acesso e preservação da informação, aumentando e melhorando a sua disseminação, devendo para tal identificar os problemas que a informação digital coloca aos processos de preservação.[253]

Witten em 2010 define bibliotecas digitais como:

> *"focused collections of digital objects, including text, video and audio, along with means for access and retrieval, and for selection, organization and maintenance."*[254]

Perla Innocenti ao propor, em 2011, uma abordagem holística da interoperabilidade de políticas em bibliotecas digitais e repositórios digitais, afirma:

> "(…)*without a policy framework a digital library is little more than a container for content."*[255]

Para concluir o Estado da Arte dos Repositórios Digitais

É inegável a constatação de que os repositórios digitais, ao garantir o armazenamento e autenticidade dos conteúdos digitais, se tornam o cerne da preservação desses conteúdos.

De igual forma, considera-se que a verdadeira distinção quanto à nomenclatura e utilização de repositórios digitais só poderá ser feita através dos documentos de política e estratégia de cada um, numa lógica de transparência e garantia de fidedignidade em relação aos seus agentes e utilizadores.

Miguel Ferreira em 2012 verifica que:

> "*No panorama internacional, têm vindo a registar-se múltiplas atividades, iniciativas e projetos, em especial nos últimos cinco anos. São iniciativas com origens e âmbitos diversificados, desde projetos menor dimensão promovidos por grupos de investigação até projetos de grande dimensão internacional."*[256]

Estas actividades incluem iniciativas no âmbito da certificação de repositórios digitais, que serão abordadas nos capítulos 4 e 5, e outras também indicadas por Miguel Ferreira: o desenvolvimento de *softwares* e/ou plataformas de repositórios como o *EPrints, DSpace* e o *Fedora Commons*; projectos e arquitecturas de preservação para repositórios como o *CASPAR*, o *CRiB*, o *PANIC*, o *PLANETS*, o *PRESERV* e *Keepit*, o *RepoMMan* e *REMAP*, o *Seamless Flow*, o

[253] FERREIRA, Carla - Preservação da informação digital: uma perspectiva orientada para as bibliotecas, p. 18.
[254] WITTEN, Ian; BAINBRIDGE, David; NICHOLS, David - How to build a digital library, p. XVI.
[255] INNOCENTI, Perla [et al.] - Towards a holistic approach to policy interoperability in digital libraries and digital repositories, p. 111.
[256] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 44.

SHAMAN, o *SHERPA DP*, e o *SCAPE*; estratégias para a preservação em repositórios, como o Modelo de Referência OAIS e o *PREMIS*, o *CAIRO*; e Ferramentas que auxiliam no planeamento de preservação, como o *AONS II*, o *PLATO*, e o *PRONOM ROAR*.

Mais recentemente, a União Europeia para os projectos de investigação europeus até 2020, está a introduzir políticas Open Access, onde os dados gerados pelos projectos podem ser armazenados em repositórios digitais.[257]

Para o autor, muito embora se verifique uma crescente consciencialização e interesse relativamente à preservação digital, são poucos os repositórios onde se verifique a existência de políticas, estratégias e acções de preservação formalizadas e consolidadas. Tal situação decorre da inexistência de enquadramento jurídico apropriado em termos de preservação digital, que defina, entre outros, responsabilidades em termos de preservação, curadoria e interoperabilidade entre repositórios.[258]

Nesse sentido Miguel Ferreira termina o relatório sugerindo linhas de orientação para promover e facilitar os processos de preservação e curadoria em repositórios de acesso aberto em Portugal, que passam pela constituição de grupos de interesse na área, análise a políticas, procedimentos e estratégias de preservação e que permitam identificar recursos e custos envolvidos, condicionalismos legais e éticos no âmbito dos repositórios digitais portugueses, produção de um projecto que visa dotar os repositórios com ferramentas para a preservação digital, cooperando com iniciativas e projectos revelantes para as boas práticas nesta área, produzir documentos e acções de sensibilização e formação e suporte, com casos exemplares (nomeadamente no que se refere à utilização de formatos de ficheiro que facilite a preservação d longo prazo), tanto para gestores de repositórios como responsáveis institucionais.[259]

[257]Cft. UNIÃO EUROPEIA. Comissão - Guidelines on data management in Horizon 2020; UNIÃO EUROPEIA. Comissão - Guidelines on best practices for using electronic information; G8 SCIENCE MINISTERS STATEMENT: news story.

[258] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 44; UNIÃO EUROPEIA. Comissão – Online survey on scientific information in the digital age.

[259] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital, p. 44-45.

4 - O Modelo OAIS

Entre 1994 e 1996 o grupo de trabalho sobre preservação de informação digital patrocinado pela RLG e pela CPA começou a abordar a questão dos arquivos digitais sustentáveis. Este trabalho teve continuidade, pela mão da *Consultative Committee for Space Data Systems (*CCSDS), que dá origem a um projecto de elaboração de uma norma de armazenamento a longo-prazo de dados digitais gerados no âmbito das missões espaciais. O grupo de trabalho era constituído por representantes da NASA (Estados Unidos), do *Centre National d'Études Spatiales* (CNES) da França, do *British National Space Centre* (BNSC) do Reino Unido, e da Agência Espacial Europeia (ESA), entidades com experiência no tratamento, armazenamento, descrição e fornecimento de acesso de informação digital. A análise preliminar efectuada por esse grupo permitiu concluir que o problema, não sendo específico dos dados digitais das missões espaciais, devia ser integrado num trabalho de desenvolvimento de normas. Tal levou à reunião de um grande número de organizações, como arquivos, bibliotecas e empresas que lidavam com a problemática da preservação da informação digital. Por outro lado, a investigação, análise e *feedback* nesta área revelaram a necessidade de um entendimento comum que desse origem a um modelo de referência conceptual, terminológico e funcional que fosse consensual.

Neste âmbito em 2002, foi definido, como recomendação do CCSDS, o Modelo de Referência para um Sistema de Informação Aberto de Arquivo, ou simplesmente Modelo OAIS. O termo "aberto" significa que a norma foi desenvolvida num fórum aberto a todas as comunidades[260]; tal não quer dizer que não haverá restrições de acesso à informação arquivada. Esta recomendação do CCSDS foi publicada no ano seguinte como a Norma ISO 14721:2003. Em 2012 é publicada uma versão revista pela CCSDS, agora como Prática Recomendada[261], com o apoio de onze entidades-membro e 28 entidades observadoras, e que dá origem à ISO 14721:2012.

O modelo OAIS fornece uma visão coerente do problema do arquivo e da preservação digital, definindo um conjunto de conceitos e funções que são os elementos básicos essenciais para a sua compreensão. Para tal apresenta uma terminologia completa que não se destina a substituir terminologias existentes, mas pretende manter o modelo num nível geral de abstracção independente de qualquer contexto de aplicação específico, para torná-lo reutilizável e aplicável a todas as áreas, sectores e tipos de informação digital. De acordo com Saramago (2003), esta terminologia neutra visa facilitar o intercâmbio entre os diferentes actores[262] e definir as diferentes responsabilidades entre esses actores.

O arquivo é definido neste modelo como "uma organização encarregada de preservar informação para permitir o acesso e utilização por parte de uma comunidade-alvo de

[260] LAVOIE, Brain - The open archival information system reference model: introductory guide, p. 3; EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): blue book.
[261] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book.
[262] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais, p. 58.

utilizadores.[263] Reconhece-se nesta definição as funções principais dos repositórios de arquivo, a conservação e a comunicação da informação[264], mas salienta a necessidade de garantir a sua inteligibilidade, e, portanto, a sua usabilidade.

Resumindo, e de acordo com Lavoie, o uso do termo OAIS, ou do termo arquivo no contexto do modelo OAIS, refere-se a um sistema de arquivo dedicado à preservação e disponibilização de informação digital a longo prazo, bem como o cumprimento de seis responsabilidades ou obrigações[265], que serão abordadas com mais profundidade no capítulo 5.

O modelo de referência OAIS consiste em três partes distintas, porém relacionadas, centradas em torno do conceito de um arquivo tipo OAIS. A primeira parte descreve o ambiente externo no qual o OAIS opera; a segunda parte descreve as entidades funcionais ou mecanismos internos, que cumprem, de forma colectiva, as responsabilidades de preservação do OAIS. A terceira parte descreve os objectos de informação que são ingeridos, geridos, e disseminados pelo OAIS.[266]

O Modelo de Ambiente Externo

O modelo de ambiente externo que rodeia o Arquivo OAIS é composto por três intervenientes com os seguintes papéis[267], a saber:

Figura 3 - O Modelo de Ambiente de um OAIS

- O produtor, que fornece a informação a preservar. As interacções entre o OAIS e o produtor são definidas num Acordo de Submissão de informação entre as duas entidades, e que identifica os Pacotes de Submissão de Informação (SIP) com os dados que o produtor solicita que sejam preservados no OAIS, juntamente com a metainformação associada[268], o

[263] Cft. "an organization (…) of people and systems that has accepted the responsibility to preserve information and make it available for a Designated Community." in EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book; LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 4.
[264] This definition emphasizes two primary functions for an archival repository: first, to preserve information – i.e., to secure its long-term persistence – and second, to provide access to the archived information, in a manner consistent with the needs of the OAIS's primary users, or Designated Community." In LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 3.
[265] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 4.
[266] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 4-5.
[267] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-2.
[268] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 6.

calendário das Sessões de Submissão de Dados, o tipo de suportes ou de transmissão de dados e o modelo de dados em que se baseiam essas Sessões de Submissão de Dados, incluindo os componentes lógicos dos SIPs (Objectos de Conteúdos de Dados, Informação de Representação, PDI; Informação de "Empacotamento" e informação de Descrição).[269] Tal Acordo de Submissão inclui ainda informação sobre as restrições de acessos aos dados e requisitos de aplicação das medidas[270], e procedimentos e protocolos que permitem o OAIS verificar com o Produtor a chegada e completude das Sessões de Submissão de Dados, ou questioná-lo acerca dos conteúdos da mesma.[271]

- O Administrador ou Gestor[272], que fornece a política geral do arquivo OAIS e efectua o controlo de gestão. O gestor distingue-se da administração (entidade funcional de administração) por o primeiro não estar envolvido nas actividades e operações do dia-a-dia do arquivo; A Gestão fornece e/ou aprova os Estatutos e Objectivos do OAIS, que determinam a extensão dos grupos de Produtores e Consumidores que o Arquivo pretende atender. A título de exemplos de interacção entre a Gestão e o OAIS são o financiamento e fornecimento de orientações para utilização dos recursos, a avaliação do cumprimento dos objectivos a longo-prazo e dos riscos a que tanto o OAIS como a informação custodiada estão expostos, pela política de preços dos serviços fornecidos, pela resolução de conflitos entre produtores, consumidores e administração interna do OAIS, e finalmente pelo estabelecimento de procedimentos que assegurem a utilização do OAIS dentro da sua esfera de influência.[273]

- O consumidor, que procura e adquire informação que se encontra preservada no arquivo OAIS. A informação que o OAIS pretende preservar tem que ter interesse para os potenciais consumidores, cliente, ou Comunidade Designada.[274] Por norma é o arquivo OAIS que define a Comunidade Designada alvo, podendo ser objecto de acordo com os financiadores e outras partes interessadas. As interacções entre os consumidores e o OAIS são de vários tipos e incluem perguntas de serviço de apoio/"*helpdesk*", solicitação de manuais, pesquisas de catálogo e informação sobre estados de encomendas/pedidos. O procedimento de encomendas/pedidos reveste-se de especial interesse para o Modelo de Referência OAIS, uma vez que lida com o fluxo que existe entre o OAIS e os consumidores, da informação custodiada.[275] O consumidor estabelece um Acordo de encomendas/pedidos de informação com o OAIS, e que identifica um ou mais AIPs de interesse, como esses AIPs devem ser transformados e mapeados em DIPs e como estes DIPs serão "empacotados" na

[269] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-9.
[270] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-10.
[271] EUA. CCSDS - Reference Model for an Open Archival Information System (OAIS): magenta book, p. 2-10.
[272] O termo original, *Management*, é traduzido por Lurdes Saramago como Gestor, enquanto outros autores lusófonos, como Miguel Ferreira, utilizam o termo Administração.
[273] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-9.
[274] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-3.
[275] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-10.

Sessão de Disseminação de Dado. O Acordo de encomendas/pedidos estabelece ainda os prazos de entrega, o número de Sessões de Disseminação de Dados, informação sobre a entrega (nome, endereço), direitos de informação (restrições de utilização, consumidores autorizados, ou taxas) e os preços acordados. As encomendas/pedidos podem efectuar-se *ad-hoc* ou serem programadas com base num evento que o despolete.

O modelo de referência define uma classe especial de consumidores referida como Comunidade Designada: O conjunto de consumidores que se presume compreender de forma independente a informação arquivada, tal como se encontra preservada e disponibilizada pelo OAIS. Estes utilizadores principais são a Comunidade Designada do OAIS.[276] É o âmbito da Comunidade Designada que determina tanto o conteúdo do OAIS como a forma em que os conteúdos são preservados, de modo a que permaneçam à disposição da Comunidade Designada de maneira independentemente compreensível. Entende-se o termo independentemente compreensível como o acesso, compreensão, e interpretação da informação do OAIS sem necessidade de recorrer a estratégias, interpretes, ou mesmo aos produtores especializados. A definição do âmbito da Comunidade Designada é um aspecto crítico do processo de preservação de um arquivo OAIS, uma vez que, quanto mais amplo for o âmbito da Comunidade Designada, maiores serão os requisitos de metainformação necessários para a manutenção da informação digital a longo prazo.[277] De notar que o âmbito Comunidade Designada não é necessariamente estático: nada que impede que a Comunidade Designada mude ao longo do tempo. Estas alterações podem ser em termos de Características dinâmicas da Comunidade Designada incluir o seu alcance, bem como as expectativas dos seus membros em relação ao acesso e utilização do conteúdo do OAIS.

Os conceitos Gestão, Produtores, Consumidores, e Comunidade Designada, bem como um OAIS, representam papéis mais funcionais do que organizacionais, pelo que todos estes papéis podem ser partes de uma única estrutura organizacional, ou distribuídos por várias organizações. O ponto essencial não é a separação física de um papel de outro, mas sim, a separação lógica das funções de tomada de decisão e os interesses das partes interessadas ligadas à maioria das actividades de preservação digital.[278]

O Modelo de Informação do OAIS

O Modelo de Referência OAIS apresenta um modelo de informação que se apoia na linguagem UML (*Unified Modeling Language*) de representação de objectos, num diagrama de classes. Uma classe descreve as responsabilidades, o comportamento e o tipo de um conjunto partilhado de propriedades do objecto. Uma classe é um conceito abstracto que representa objectos concretos. Estes objectos concretos chamam-se instância da classe. Neste âmbito, a Informação define-se como qualquer tipo de conhecimento que pode ser transmitido, que é sempre representado por um tipo de dados.[279]

[276] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 6.
[277] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 6.
[278] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 7.
[279] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-3.

O Objecto de Dados

O objecto de dados de conteúdo (ou seja, uma sequência de bits) pode ser constituído por um único ficheiro digital, - por exemplo, um documento em formato PDF; também podem incluir vários ficheiros, como um sítio web que consiste em texto (ficheiros HTML) e imagens estáticas (GIF ou JPEG). O ponto fulcral é que o OAIS é responsável pela preservação a longo prazo do objecto de dados de conteúdo, assim como da sua disponibilização sob uma forma que seja independentemente compreensível para a Comunidade Designada.[280]

O objecto de dados pode ser expresso como um objecto físico (por exemplo, uma pedra da Lua), juntamente com alguma informação de Representação, ou pode ser expressa como um objecto digital (ou seja, uma sequência de bits), juntamente com a informação de Representação dando sentido aos bits.[281]

O Objecto de Informação

Para preservar a informação digital, como um ficheiro, que é constituída por código binário, é indispensável saber, por exemplo, o tipo de formato, o código dos caracteres. Essa informação consta no Objecto de Informação. Para o Modelo de Referência OAIS, o Objecto de Informação é a combinação de Dados com Informação de Representação.[282] O Objecto da Informação é assim composto pelo objecto de dados físicos ou digitais, e a Informação de representação, que permite a interpretação completa dos dados em informação significativos.[283]

A Informação de Representação

Para cumprir com a segunda responsabilidade - disponibilizar o objecto de dados de conteúdo de uma forma que seja independentemente compreensível pela Comunidade Designada - o objecto de dados de conteúdo deve ser acompanhada por uma quantidade adequada de informação de Representação.[284]

A Informação de Representação é a informação que mapeia um objecto de dados em conceitos mais significativos[285], permitindo a interpretação/compreensão dos dados para obter a informação. Assim podemos dizer que os dados interpretados utilizando a sua Informação de representação "fornecem" Informação[286], como se pode ver na figura seguinte.

---

[280] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 12.
[281] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-21.
[282] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-20.
[283] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-20/21.
[284] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 12.
[285] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 1-14.
[286] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-4.

Figura 4 - Obtenção de Informação a partir dos Dados

A informação de Representação que acompanha um objecto digital, ou sequência de bits, é usado para dar significado adicional. Normalmente mapeia os bits em tipos de dados comumente reconhecidos e agrupa-os com base nestes tipos de dados. Associa estes grupos a significados de alto nível: inclui a descrição das maneiras, possivelmente complexas, de como os objectos estão interrelacionados[287].

> *"Representation Information might include a description of the hardware and software environment needed to display the Content Data Object and/or access its contents; it might also summarize the appropriate interpretation of the Content Data Object. For example, if the Content Data Object is an ASCII file of numbers, Representation Information might indicate that the numbers correspond to average daily air temperature readings for Manhattan, measured in degrees Celsius, for the period 1972 – 2000.*[288]"

Para que esse Objecto de Informação seja preservado com êxito, é fundamental que o OAIS identifique e compreenda claramente o objecto de dados e a sua Informação de Representação associada. No caso da informação digital, isso significa que o OAIS deve identificar claramente os bits e a Informação de Representação relativa a esses bits. Esta transparência necessária ao nível dos bits é uma característica que distingue a preservação da informação digital, e vai contra as concepções orientadas a objectos que tentam esconder essas questões de implementação.[289]

O âmbito da Comunidade Designada tem impacto na quantidade de metainformação necessária para suportar o processo de preservação, no que se refere à Informação de Representação. Normalmente quanto mais abrangente for o âmbito da Comunidade Designada, menos especializada será a base de conhecimento ligada a essa comunidade, o que se traduz na assunção por parte do OAIS de que a Comunidade Designada possui menos informação relevante para interpretar e compreender a informação arquivada. Se a base de conhecimento for menos especializada será necessária mais informação de representação para garantir que a informação preservada contínua processável e compreensível a longo prazo para a Comunidade Designada.[290]

A Informação de Representação é um Objecto de Informação que pode ter seu próprio objecto de dados e sua própria Informação de Representação associada à compreensão de cada

[287] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-21.
[288] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 12.
[289] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-4.
[290] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 13.

objecto de dado.[291] O conjunto de objectos resultante pode ser referido como uma rede de representação.[292] Ou seja, a Natureza recursiva da informação de representação, composta pelos seus dados e pela sua informação de representação, resulta numa rede de objectos de informação de representação.[293]

Como se referiu anteriormente, o objecto digital é em si composto por uma ou mais sequências de bits. O objectivo do Objecto de Informação de Representação é converter as sequências de bits em informação mais significativa. Isto é feito através da descrição do formato, ou conceitos de estrutura de dados, os quais serão aplicadas às sequências de bit e que por sua vez resultam em valores mais significativos, tais como caracteres, números, pixéis, matrizes, tabelas, etc.[294]

A Informação Estrutural refere-se a esses tipos comuns de dados informáticos, agregações destes tipos de dados e regras de mapeamento que mapeiam desde dos tipos de dados subjacentes até aos conceitos de mais alto nível necessários para entender o Objecto Digital. Estas estruturas são normalmente identificadas pelo nome ou pela posição relativa dentro das sequências de bit associados. A Informação Estrutural é muitas vezes referida como o "formato" do objecto digital.[295]

A Informação Semântica diz respeito à informação adicional acerca da linguagem utilizada quando o objecto digital é interpretado como uma sequência de caracteres de texto, e descrito como tal na Informação Estrutural, que deve ser fornecida.[296] Irá incluir significados especiais associados com todos os elementos da informação estrutural, as operações que podem ser executadas em cada tipo de dados, e suas inter-relações.[297] A Informação semântica associada com partes de alguma informação codificada digitalmente é independente do formato.[298]

A Informação de Representação pode conter Outra Informação de Representação. Isso quer dizer que a taxonomia de Informação de Representação aqui apresentada está longe de estar completa.[299] A Informação relativa às relações entre a Informação Semântica e a Informação

[291] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-23.
[292] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-23.
[293] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-4.
[294] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.
[295] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.
[296] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.
[297] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.
[298] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.
[299] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.

estrutural, ou acerca do *software* necessário para processar um ficheiro de base de dados deve considera-se como Outra Informação de Representação.[300]

A Informação Estrutural, a informação semântica e a Outras Informações de Representação são subtipos e componentes da Informação de Representação.[301]

Taxonomia dos Objectos de Informação

Existem muitos tipos de informação envolvidos na preservação a longo prazo de informação dum OAIS. Cada um destes tipos pode ser encarado como um Objecto de Informação completo, na medida em que contém um objecto de dados e Informação de representação adequada para compreender os dados.[302] Os objectos são classificados pelo seu conteúdo e função no funcionamento de um OAIS, incluindo objectos de Informação de Conteúdo, objectos de Informação de Descrição de Preservação, objectos de Informação de "Empacotamento", e objectos de Informação de Descrição.[303]

Informação de Conteúdo

A Informação de Conteúdo é o conjunto de informação que é o objecto alvo de preservação pelo OAIS[304]. Decidir o que é a Informação de Conteúdo pode não ser óbvio e poderá ter de ser negociado com o produtor[305]. A Informação de Conteúdo consiste no objecto de dados de conteúdo e a Informação de representação associada necessária para tornar o objecto de dados de conteúdo compreensível para a Comunidade Designada.[306]

O OAIS necessita de ter bastante Informação de Representação associada aos bits do objecto de dados de conteúdo na Informação de Conteúdo para que ele considere que os membros da Comunidade Designada possam entrar na Rede de Representação com conhecimentos suficientes para começar a interpretar a Informação de Representação de forma precisa.

Uma função importante do OAIS é decidir que partes da Informação de Conteúdo são o objecto de dados de conteúdo e que partes são da Informação de Representação. Este aspecto é fundamental para uma compreensão clara do que está a ser preservado.[307]

Informação de Descrição de Preservação

O OAIS deve garantir a existência de informação para apoiar a confiança, o acesso e o contexto da Informação de Conteúdo durante um período de tempo indefinido. O conjunto específico

[300] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-22.
[301] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-23.
[302] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-25.
[303] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-25.
[304] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6 e p. 4-26.
[305] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-26.
[306] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6.
[307] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-28.

de Objectos de informação que são necessários para esta função, é chamado colectivamente de Informação de Descrição de Preservação (PDI).[308] A Informação de Descrição de Preservação deve incluir a informação que é necessária para preservar adequadamente a Informação de Conteúdo específica ao qual ele está associado[309], para garantir claramente a sua identificação e compreender o ambiente em que ela foi criada.[310] Ele está especificamente voltado para descrever os estados passados e presentes da Informação de Conteúdo, garantindo que é inequivocamente identificável, e garantir que não tenha sido alterado inadvertidamente.[311] Por esse motivo, só se pode avaliar a Informação de Descrição de Preservação após se ter definido claramente a Informação de Conteúdo.[312] A Informação de Descrição de Preservação divide-se em cinco tipos de informação de preservação:

1. Proveniência: refere-se à origem ou a fonte da Informação de Conteúdo, quem teve a sua custódia desde a sua origem, e a sua história (incluindo a história da sua tramitação)[313], quaisquer alterações que possam ter ocorrido desde a sua origem, proporcionando um registo de auditoria para a Informação de Conteúdo. Isso dá aos futuros utilizadores alguma garantia quanto à provável fiabilidade da Informação de Conteúdo, uma vez que contribui como evidência que suporte a Autenticidade. A Proveniência pode ser encarada como um tipo especial de informação de contexto.[314]

2. Contexto: descreve as relações da Informação de Conteúdo com o seu ambiente/outras informações fora do Pacote de Informação.[315] Isto inclui a razão por que a Informação de Conteúdo foi criada e como se relaciona com outros objectos de Informação de Conteúdo existentes noutros lugares.[316]

3. Referenciação: identifica e, se necessário descreve, um ou mais mecanismos usados para fornecer um ou mais identificadores ou sistemas de identificadores, que podem ser utilizados como identificadores únicos da Informação de Conteúdo.[317] Também fornece esses identificadores que permitem que sistemas externos referenciem, de forma inequívoca, essa Informação de Conteúdo em particular. Exemplos desses sistemas incluem

[308] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-29.
[309] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-29.
[310] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6.
[311] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-29.
[312] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6.
[313] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6.
[314] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-30.
[315] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6.
[316] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-30.
[317] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-6.

sistemas de taxonomia, sistemas de referenciação e sistemas de registo. No modelo de referência OAIS a maioria (se não a totalidade) dessas informações são replicadas em Descrições de Pacotes, que permitem que aos consumidores aceder à Informação de Conteúdo de interesse.[318]

4. Fixidez (integridade): proporciona um envelope ou escudo protector contra qualquer alteração do Conteúdo de Informação que não esteja documentada.[319] Fornece as verificações de integridade de dados ou chaves de validação / verificação utilizados para assegurar que o Objecto de Informação de Conteúdo específico não foi alterado de forma não documentada. Inclui esquemas especiais de codificação e detecção de erros que são específicas das instâncias dos Objectos de conteúdo. Não inclui mecanismos de preservação da integridade fornecidos pelos serviços subjacentes ao OAIS, protecção contra erros fornecidos pelos suportes e dispositivos usados pelo armazenamento de arquivo. Pode indicar a qualidade mínima do serviço para esses mecanismos.[320] Trata-se de Informação de inalterabilidade e não de integridade dos suportes e sistemas de armazenamento

5. Privilégios de Acesso: reflectem os direitos de acesso, incluindo a preservação, distribuição e utilização da Informação de Conteúdo.[321] Identifica as restrições de acesso relativos à Informação de Conteúdo, incluindo o enquadramento legal, termos de licenciamento e controlo de acesso. Contém as condições de acesso e de distribuição estabelecidas no âmbito do Acordo de Submissão, relacionadas tanto com a preservação (pelo OAIS) como com a utilização final (pelo consumidor). Também inclui as especificações para a aplicação das medidas relativas a direitos.[322] A Informação de Direitos de Acesso surge somente na edição do Modelo de Referência OAIS de 2012.

O OAIS precisa de decidir de forma explícita qual a definição exacta de Informação de Conteúdo, de modo a ser capaz de garantir que ele também possui a PDI necessária para preservar a Informação de Conteúdo. Após a definição da Informação de Conteúdo é possível avaliar a Informação de Descrição de Preservação.[323]

Informação de "Empacotamento"

A Informação de "Empacotamento" refere-se à informação que junta, identifica e relaciona, de forma real ou lógica, a Informação de Descrição de Preservação e Informação de Conteúdo.[324] Refere ou liga os componentes do pacote numa entidade identificável num dado suporte.[325]

---

[318] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-30.
[319] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-7.
[320] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-30.
[321] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-7.
[322] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-30.
[323] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-32.
[324] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-7.

A Informação de "Empacotamento" não precisa necessariamente ser preservada pelo OAIS uma vez que não contribui para o conteúdo da informação ou o PDI. No entanto, existem casos em que o OAIS necessita de reproduzir a submissão original de maneira exacta. Neste caso, a Informação de Conteúdo é definida para incluir todos os bits submetidos.[326]

O OAIS também deve evitar guardar PDI ou Informação de Conteúdo somente nas convenções de nomenclatura de estruturas de directórios ou nome de ficheiros. Estas estruturas são mais susceptíveis de ser utilizados como Informação de "Empacotamento". A Informação de "Empacotamento" não é preservada por todas as Migrações Digitais. Todas as informações gravadas em nomes de ficheiros ou estruturas de directórios podem ser perdidas quando a Informação de "Empacotamento" é alterada. O assunto da Informação de "Empacotamento" é uma questão importante para a migração de Informação dentro de um OAIS para suportes mais recentes.[327]

Informação de Descrição

O OAIS tem que fornecer ferramentas para permitir aos consumidores localizar informação de interesse potencial, analisar essa informação e solicitar a informação desejada. Isto é realizado através de um Objecto de Informação especial chamado Informação de Descrição, que contém os dados que servem como entradas para documentos ou aplicativos chamados Instrumentos Auxiliares de Acesso. [328.]

A Informação de Descrição é utilizada para o consumidor descobrir qual o pacote que contem a Informação de Conteúdo pretendida, podendo ir desde um simples título descritivo do Pacote de Informação que surge numa mensagem, até a um conjunto completo de atributos de metainformação pesquisáveis numa base de dados de pesquisa.[329]

A Informação de Descrição deriva geralmente da Informação de Conteúdo e da PDI. A Informação de Descrição pode ser vista como um índice para permitir um acesso eficiente ao Pacote de informação associado através dos Instrumentos Auxiliares de Acesso associados. Os Instrumentos Auxiliares de Acesso são documentos ou aplicativos que podem ser usados para localizar, analisar, recuperar ou solicitar informação ao OAIS.[330.]

O Modelo de Referência também fornece uma descrição de alto nível dos objectos digitais geridos pelo arquivo.[331]

---

[325] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-32.
[326] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-32.
[327] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-32.
[328] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.
[329] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-7.
[330] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.
[331] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 10.

Pacotes de Informação

Toda a submissão de informação que um produtor efectua no OAIS e toda a disseminação de informação para um Consumidor ocorre como uma ou mais transmissões discretas.[332] Estas transmissões ocorrem utilizando um Pacote de Informação[333], a estrutura conceptual de apoio à preservação da informação a longo prazo[334], ou seja, e como se pode ver na figura seguinte, um contentor conceptual que contém dois tipos de objectos de informação: a Informação de Conteúdo e a Informação de Descrição de Preservação.[335] O Pacote de Informação pode ser associado a dois outros tipos de objectos de informação[336]: a Informação de "Empacotamento", que encapsula[337] e delimita[338] o pacote, e a Descrição do Pacote, que o identifica[339] para permitir o acesso eficiente.[340] Existem vários tipos de pacotes de informação, que são utilizados no âmbito do processo de arquivamento. Estes pacotes de informação podem ser usados para estruturar e armazenar a informação custodiada no OAIS, para transportar a informação necessária do produtor ao OAIS, ou para o transporte de informação solicitada entre o OAIS e os consumidores Existem diferentes requisitos de informação para cada uma dessas funções.[341]

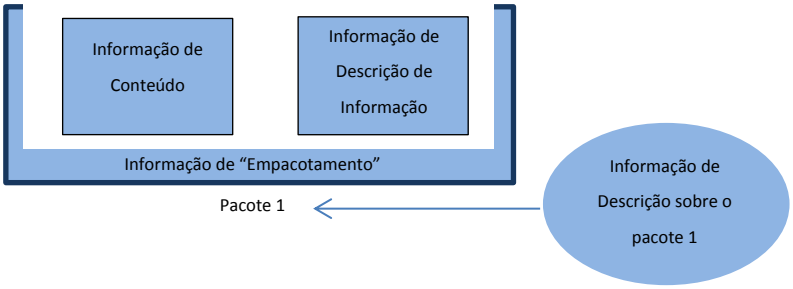

Figura 5 - O Pacote de Informação

Em resumo:

[332] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-5.
[333] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-5.
[334] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.
[335] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-5 e 4-33.
[336] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.
[337] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-5.
[338] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.
[339] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-5.
[340] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.
[341] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-33.

> *"The information components described above – Content Information (the Content Data Object and Representation Information), Preservation Description Information (Reference, Context, Provenance, and Fixity Information), Packaging Information, and Descriptive Information collectively form the Archival Information Package, which in turn represents the combination of the preserved digital information and a complete set of associated metadata."*[342]

É necessário distinguir entre um pacote de informação que é preservado por um OAIS e os pacotes de informação que são submetidos a, ou disseminados a partir de, um OAIS. Estes pacotes variantes são necessários para reflectir o facto de que alguns pedidos a um OAIS terão informação de Representação ou PDI insuficiente para atender aos requisitos de preservação do OAIS. Além disso, eles podem ser organizados de forma muito diferente do modo como o OAIS organiza a informação que está a preservar. Finalmente, o OAIS pode fornecer informação aos Consumidores que não inclui toda a informação de Representação ou todo o PDI com a Informação de Conteúdo associada a ser disseminada.[343]

Dentro dos Pacotes de Informação podemos distinguir três tipos ou variantes, tendo em conta a sua função, a saber: o Pacote de Submissão de Informação (SIP), o Pacote de Informação de Arquivo (AIP), e o Pacote de Disseminação de Informação (DIP). Embora sejam todos pacotes de informação, eles diferem em conteúdo obrigatório e na multiplicidade das associações entre classes contidas.[344] As definições destes tipos de pacotes baseiam-se em função do processo de arquivamento, que usa o pacote, e a conversão de um pacote para outro à medida que vai avançando no processo de arquivamento.[345]

- O SIP é o pacote enviado por um produtor para um OAIS. A sua forma e conteúdo detalhado é normalmente negociado entre o produtor e o OAIS.[346]

  > "*The concept of the SIP emphasizes the fact that information may not be preserved in the exact form in which it is submitted by the Producer."*[347]

  A maioria dos SIPs inclui Informação de Conteúdo e alguma PDI que, tal como a sua Informação de Representação, pode considerar-se incompleta para cumprir com os requisitos de preservação da Informação.[348] Podem ser necessários vários SIPs para fornecer um conjunto completo de Informação de Conteúdo e PDI associado.[349]

---

[342] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 14.
[343] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-35.
[344] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 4-35.
[345] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 4-34.
[346] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 4-35.
[347] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 11.
[348] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 2-7.
[349] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 4-35.

"the Producer may provide the information in a format not supported by the OAIS, necessitating migration to another format prior to inclusion in the archival store."[350]

A informação de descrição associada a um SIP será provavelmente fornecida antes da submissão do SIP ao OAIS, mas pode ser fornecida a qualquer momento.[351]

- O AIP, com funções de preservação, é fruto da transformação de um ou mais SIPs. É composto por um conjunto completo de PDI da Informação de Conteúdo a que se refere, podendo também conter uma colecção de outros AIPs. A sua Informação de "Empacotamento" tem que estar em conformidade com as normas internas OAIS e pode variar uma vez que é gerido pelo OAIS.[352] A informação de descrição associada a um AIP pode ser extensa e será gerida pelo OAIS para que os consumidores possam encontrar e solicitar a Informação de Conteúdo do seu interesse.[353]

- O DIP é fornecido em resposta de um pedido de um Consumidor, e contendo parte ou todo o conteúdo de um AIP ou colecção de AIPs.[354] A Informação fornecida pode ou não incluir a totalidade da Informação de Representação ou da PDI[355], mas a forma de apresentação tem que ter em conta os requisitos do suporte e do Consumidor. Adicionalmente, a Informação de "Empacotamento" tem que estar presente numa forma em que o Consumidor possa distinguir claramente a informação que solicitou.[356] A Informação de "Empacotamento" pode assumir várias formas, dependendo do suporte usado para disseminação e as exigências dos consumidores. A informação de descrição associada com um DIP pode ser fornecida em qualquer momento antes, durante ou depois da transferência do DIP. O seu objectivo é dar ao consumidor informação suficiente para reconhecer o DIP entre possíveis pacotes semelhantes. Pode haver mais do que uma descrição de texto com um nome ou título, como transportado pela Informação de "Empacotamento", através do qual o DIP pode ser reconhecido.[357]

O conteúdo de informação exacto do SIP e do DIP e a sua relação com o AIP correspondente dependem dos acordos celebrados entre o Arquivo e seus produtores e consumidores.[358]

---

[350] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 11.
[351] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 4-35.
[352] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 2-8.
[353] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 4-36.
[354] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 2-8.
[355] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 2-7.
[356] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 2-8.
[357] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-36.
[358] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-36.

Embora a implementação do AIP possa variar de arquivo para arquivo, a especificação do AIP como um contentor que contém toda a informação necessária para permitir a preservação de longo prazo e o acesso à informação custodiada pelo Arquivo permanece válida.[359]

A figura 6 [360] mostra as ligações dos vários elementos abordados no âmbito do Modelo de Informação apresentado no Modelo de Referência OAIS.

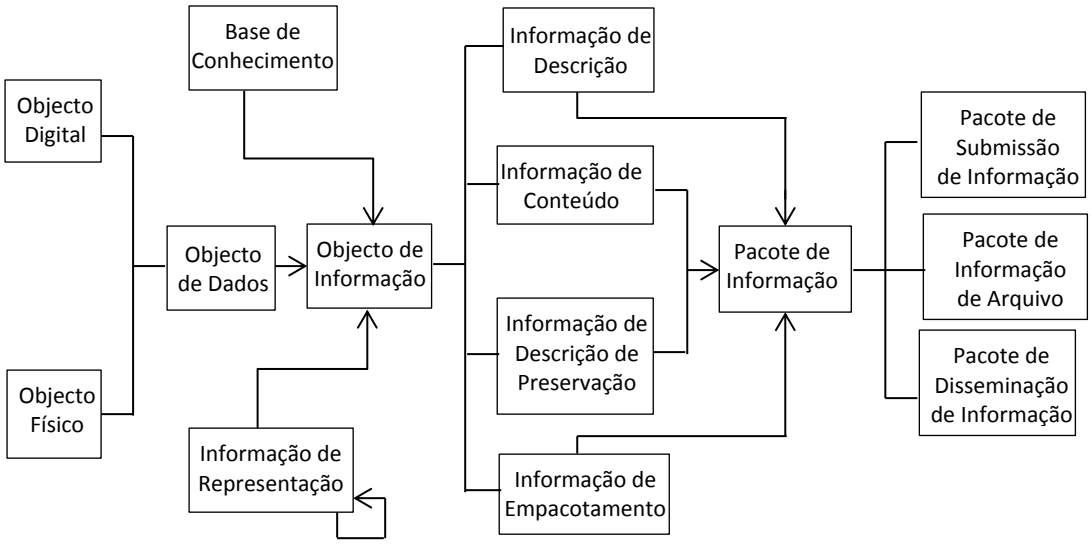

Figura 6 - O Modelo de Informação OAIS

O Modelo Funcional do OAIS

Para além do modelo de informação, o Modelo de referência OAIS, inclui o modelo funcional, que identifica e descreve o conjunto central de mecanismos com que um arquivo OAIS cumpre a sua missão de preservar e disponibilizá-la à Comunidade Designada. Estes mecanismos são resumidos no modelo funcional OAIS e incluem um conjunto de seis serviços ou componentes funcionais de alto nível, que em conjunto, cumprem com o papel duplo de preservar e fornecer acesso à informação custodiada.[361]

[359] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-36.
[360] Figura adaptada de THOMAZ, Katia; SOARES, Antonio José - A preservação digital e o modelo de referência Open Archival Information System (OAIS).
[361] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 7.

O OAIS pode ser dividido em seis entidades funcionais e interfaces relacionadas. Como se pode ver na seguinte figura, as linhas de conexão das entidades identificam fluxos de informação.[362]

Figura 7 - O Modelo Funcional OAIS

O Papel de cada uma das entidades é o seguinte:

- Entidade Funcional de Ingestão aceita os Pacotes de Submissão de Informação (SIPs) de Produtores (ou de elementos internos sob o controlo da Entidade Funcional de Administração) e prepara os conteúdos para armazenamento e gestão dentro do Arquivo. As funções de Ingestão incluem a recepção dos SIPs[363], efectuar o controlo de qualidade dos SIPs[364], gerar um pacote de informação de arquivo (AIP), gerar Informação Descritiva[365] pela extracção de informação descritiva dos AIPs, coordenação das actualizações para as entidades funcionais de Armazenamento de arquivo e de Gestão de Dados.[366]

[362] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-1.
[363] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-1.
[364] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-1.
[365] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-7.
[366] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-1.

"*In short, the Ingest function serves as the OAIS's external interface with Producers, managing the entire process of accepting custody of submitted information and preparing it for archival retention.*"[367]

- Entidade Funcional de Armazenamento de Arquivo[368] fornece os serviços e funções de armazenamento, manutenção e recuperação do AIP. As funções de armazenamento de arquivo incluem a recepção do AIP da entidade funcional de Ingestão e adicionamento do mesmo no armazenamento permanente[369], gestão da hierarquia de armazenamento[370] para responder às exigências de qualidade de serviço das entidades utilizadoras, refrescamento dos suportes nos quais estão armazenados as informações custodiados pelo Arquivo OAIS[371], realização de verificações de rotina e de erro[372], fornecimento de recursos para recuperação de desastres[373], envio do AIP para a entidade funcional de Acesso para resolução de encomendas.

  "Note that the Archival Storage function has no direct external interface; interaction with Archival Storage is confined to the OAIS's internal high-level services."[374]

- Entidade Funcional de Gestão de Dados fornece os serviços e funções de preenchimento, manutenção e acesso à Informação Descritiva que identifica e documenta a informação custodiada pelo Arquivo e dados administrativos utilizados para gerir o Arquivo OAIS. As funções de gestão de dados incluem a administração da base de dados do arquivo OAIS (mantendo as definições de esquema e de visualização, e integridade referencial)[375], realização das actualizações à base de dados (carregamento de nova Informação Descritiva ou dados administrativos do Arquivo)[376], realização de consultas sobre os dados de gestão de dados para gerar respostas a consultas[377], e elaboração de relatórios a partir das respostas a consultas.[378]

---

[367] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 8.
[368] O termo original, Archival Storage, é traduzido por Lurdes Saramago como Repositório, enquanto outros autores lusófonos, como Miguel Ferreira, utilizam o termo Repositório de Dados.
[369] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[370] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[371] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[372] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[373] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[374] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 9.
[375] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[376] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[377] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[378] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.

- Entidade Funcional de Acesso fornece os serviços e funções de apoio aos consumidores na verificação da existência, descrição, localização e disponibilidade das informações armazenadas no OAIS e permite aos consumidores a solicitação e recepção de produtos de informação.[379]

  > *"it is the primary mechanism by which the OAIS meets its responsibility to make its archived information available to the user community."*[380]

  As funções de acesso incluem a comunicação com os consumidores para receber pedidos[381], a aplicação de controlos para restringir o acesso à informação de protecção especial[382], a coordenação da execução de pedidos para conclusão com êxito[383], gerar respostas (Pacotes de disseminação de informação, respostas a consultas, relatórios)[384] e entregar as respostas aos Consumidores.[385]

- Entidade Funcional de Administração fornece os serviços e funções referentes ao funcionamento global do sistema de arquivo,

  > *"as well as coordinating the activities of the other five high-level OAIS services."*[386]

  As funções de administração incluem a solicitação e negociação de acordos de submissão com os produtores[387], auditoria de submissões para assegurar que cumprem as normas do Arquivo[388], controlo e fornecimento de mecanismos para restringir ou permitir o acesso físico (portas, fechaduras, guardas) a elementos do arquivo, conforme determinado pelas políticas de Arquivo.[389] As funções de engenharia de sistemas incluem a manutenção da gestão de configuração do *hardware* e *software* do sistema[390], monitorizar e aperfeiçoar as operações do Arquivo[391], inventariar, reportar e migrar / actualizar os conteúdos do

[379] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[380] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 9-10.
[381] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-3.
[382] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-3.
[383] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-3.
[384] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-3.
[385] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2 e 4-3.
[386] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 10.
[387] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[388] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[389] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-12.
[390] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[391] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.

Arquivo.[392] Outras funções incluem o estabelecimento e manutenção de normas e políticas de arquivo[393], fornecimento de suporte ao cliente[394], activar pedidos/solicitações armazenadas.[395]

> *"Administration serves as the central hub for the OAIS's internal and external interactions: it communicates directly with the five other OAIS high-level services – Ingest, Archival Storage, Data Management, and Access, as well as the OAIS's external stakeholders – Producers, Consumers and Management."*[396]

- Entidade Funcional de Planeamento de Preservação fornece os serviços e funções de monitorização do ambiente envolvente do OAIS e fornecimento de recomendações e planos de preservação para assegurar que a informação armazenada no OAIS permanece acessível e compreensível pela Comunidade Designada a longo prazo, mesmo que o ambiente informático inicial se tiver tornado obsoleto, ou mesmo se ocorrerem:

  "*shifts in the scope or expectations of the Designated Community."*[397]

  As funções de planeamento de preservação incluem avaliar o conteúdo do Arquivo e recomendar actualizações periódicas de informações de arquivo[398], recomendar a migração de informação depositada no Arquivo[399], desenvolver recomendações para normas e políticas do Arquivo[400], fornecer relatórios periódicos de análise de risco[401], monitorizar alterações ao ambiente tecnológico[402], monitorizar alterações nas necessidades de serviços e conhecimento de base da Comunidade Designada[403], desenhar modelos de pacote de informação[404], desenvolver planos de migração detalhados, protótipos de *software* e planos de teste para permitir a implementação de metas de migração da Administração[405],

[392] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[393] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[394] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[395] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[396] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 10.
[397] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p.9.
[398] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[399] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[400] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[401] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[402] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[403] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[404] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[405] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.

proporcionar assistência no planeamento e revisão para especializar esses modelos em SIPs e AIPS para submissões específicas.[406]

- Os Serviços Comuns são considerados como constituindo uma outra entidade funcional neste modelo. Esta entidade é tão profunda que, para maior clareza, não é mostrada na figura.[407] Estes serviços incluem serviços do sistema operativo que fornecem os serviços básicos necessários para operar e administrar a plataforma aplicacional e fornecer uma interface entre o *software* aplicativo e a plataforma[408], serviços de rede que fornecem os recursos e mecanismos para suportar aplicações distribuídas que necessitam de acesso a dados e a interoperabilidade das aplicações em ambientes heterogéneos ligados em rede[409], serviços de segurança que fornecem recursos e mecanismos para proteger a informação sensível e tratamento no sistema de informação. O nível apropriado de protecção é determinado com base no valor da informação para os utilizadores finais da aplicação e a percepção de ameaças a ele.[410]

> *"In summary, the OAIS encompasses six high-level functional components which, taken together, constitute the mechanisms by which the OAIS preserves information over the long-term and makes it available to the Designated Community. An OAIS-type archive will implement each of these services, in one form or another, in the course of building a complete archival system."*[411]

Este modelo parece ser reminiscente do modelo de comunicação desenvolvido por Shannon (1948) e a que se junta Weaver (1949) e que levou ao desenvolvimento da *Teoria da Informação.* Assim:

- A fonte de informação teria como equivalente o Produtor, por produzir a mensagem;
- A mensagem referir-se-ia aos pacotes de informação SIPs, AIPs e DIPs, como dados ou informação de que é enviada para o destinatário de forma verbal, escrita, registada, ou visual;
- O canal, que inclui as entidades funcionais de gestão de dados, de armazenamento de arquivo ou repositório de dados, e de planeamento de preservação, e que garantem que os dados ou a informação são adaptados para a sua transmissão.
- O transmissor equivaleria à entidade funcional de Ingestão, que codificaria a mensagem;

[406] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-2.
[407] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-3.
[408] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-3 e 4-4.
[409] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-4.
[410] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 4-4 e 4-5.
[411] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 10.

- O receptor ou descodificador, à entidade funcional de Disseminação, que descodifica ou reconstrói a mensagem para ficar compreensível ao destinatário.

- O destinatário, que corresponde ao consumidor.

- O ruído, aqui considerado como elemento de degradação da informação e da própria transmissão dos dados, é antecipado, evitado, mitigado e tratado pela intervenção das entidades funcionais de planeamento de preservação e de Administração.

Outras semelhanças entre o modelo de Shannon e o modelo OAIS prendem-se com o facto de ambos não especificarem as questões ligadas com o contexto (de produção, transmissão, recepção) nem diferenciarem suportes de transmissão.[412]

Por outro lado a entidade funcional de Disseminação também adquire propriedades de transmissor aquando do feedback dos consumidores, embora o feedback não tenha sido abordado no modelo de Shannon, por não ser bidireccional. Para além disso, o modelo de Shannon não leva em consideração o dinamismo da dimensão Tempo, algo que tem suma importância no Modelo OAIS, evidenciada na existência da entidade funcional de planeamento de preservação, por influir no risco de obsolescência da informação armazenada.

OAIS e a Normalização

O modelo identificou um conjunto de áreas para desenvolvimento de normas relacionadas com o modelo OAIS, que dizem respeito, em particular, às relações arquivo-produtor, bem como a certificação de arquivos. Também serviu de referência para o desenvolvimento de muitas aplicações de *software*.

As áreas de normalização incluem interfaces entre Arquivos OAIS, metodologia de submissão (ingestão) utilizada pelo Arquivo, submissão (ingestão) de fontes de informação digital para o Arquivo, fornecimento (disseminação) de fontes digitais pelo Arquivo, submissão de metainformação digital ou fontes de dados físicos para o Arquivo, normas de sintaxe para a identificação de fontes digitais dentro do Arquivo, protocolos de pesquisa e localização de metainformação sobre fontes de dados físicos e digitais, acesso a suportes que permita a substituição de sistemas de gestão de suporte sem necessidade de regravar o suporte, suporte físicos em específico, migração de informação para vários formatos e suportes, práticas de gestão documental, práticas de certificação de Arquivos. Para além da norma OAI-PMH, que abordamos anteriormente, apresentam-se de seguida outras iniciativas.

Metainformação de preservação

Embora o modelo não define esquemas de metainformação, apresenta um modelo de informação que serve de base à definição de várias normas relativas a metainformação. Exemplos disso são o projecto *CURL Exemplars in Digital Archives* (CEDARS)[413], o projecto

[412] No caso do OAIS, este tanto pode ser aplicado em repositórios em suporte digital como em suporte analógico, como se pode constatar nos exemplos em EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): blue book, p. A1-A27.
[413] DAY, Michael - CEDARS guide to preservation metadata.

Networked European Deposit Library (NEDLIB)[414], *National Library of Australia* (NLA)[415] e especialmente o PREMIS (*PREservation Metadata: Implemetation Strategies*). Este grupo está na origem de um esquema de metainformação bastante detalhado e abrangente.

O OCLC e o RLG patrocinaram actividades de desenvolvimento de consensos em duas áreas relacionadas com o modelo de referência OAIS. A primeira área abordou os requisitos de metainformação associados à preservação de informação digital a longo prazo.[416] Isto resultou na publicação, em 2001, de um Livro Branco intitulado *Preservation Metadata for Digital Objects: A Review of the State of the Art*[417], resultante do trabalho do grupo de trabalho internacional de especialistas que analisava a preservação digital na perspectiva do património cultural. Nessa publicação é introduzido o conceito de metainformação de preservação, definindo a sua importância no âmbito da preservação digital a longo prazo, e apresenta ainda uma análise e sistematização de uma série de esquemas de metainformação de preservação já existentes, nomeadamente do NLA e dos projectos CEDARS e NEDLIB, com o objectivo de identificar pontos convergentes e divergentes. Um dos aspectos que consideramos de maior importância é a utilização dos conceitos do modelo de referência OAIS como ponto de partida para o esquema.

O Livro Branco forneceu o contexto para o desenvolvimento do relatório *A Metadata Framework to Support the Preservation of Digital Objects*[418], em 2002, em que o mesmo grupo de trabalho apresentava um quadro abrangente de metainformação de preservação, que identificava e descrevia os tipos de informação que podiam ser utilizados para apoiar a preservação da informação digital. Este quadro apresentava-se como uma estrutura conceptual expandida para o modelo OAIS, juntamente com um conjunto de elementos "protótipo" de metainformação, mapeados para a estrutura conceptual e reflectindo os conceitos e requisitos de informação estabelecidos no modelo de referência OAIS. O quadro aprofundou a definição dos componentes de informação constitutivos de um AIP, e clarificou como é que a metainformação de preservação oferece suporte ao processo preservação.[419]

Na continuidade deste trabalho, a OCLC e a RLG estabeleceram um segundo grupo de trabalho, *Preservation Metadata: Implementation Strategies*, ou PREMIS, composto por representantes de bibliotecas, museus, organismos governamentais e do sector privado de vários países com experiência no desenvolvimento de repositórios para preservação digital a longo prazo.[420] Usando como ponto de partida do quadro de metainformação de preservação apresentada pelo outro grupo de trabalho, desenvolveu recomendações para um conjunto implementável de elementos "centrais" de metainformação de preservação, apoiados por um dicionário de dados, e amplamente aplicáveis dentro da comunidade da preservação digital e

[414] LUPOVICI, Catherine; MASANÈS, Julien - Metadata for the long term preservation of electronic publications.
[415] AUSTRÁLIA. National Library of Australia - Preservation metadata for digital collections.
[416] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 14.
[417] DALE, Robin - Preservation metadata for digital objects : a review of the state of the art : a white paper.
[418] LAVOIE, Brain [et al.] - Preservation metadata and the OAIS information model: a metadata framework to support the preservation of digital objects.
[419] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 15.
[420] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 15.

suportados por recomendações e orientações para codificação, armazenamento e gestão de metainformação dentro de um sistema de arquivo digital OAIS. O PREMIS lançou em 2005 o relatório *Data Dictionary for Preservation Metadata: Final Report of the PREMIS Working Group*[421] que inclui o Dicionário de Dados PREMIS 1.0, um recurso abrangente e prático para a implementação de metainformação de preservação em sistemas de arquivo digital, o relatório de acompanhamento, que fornece contexto, modelo de dados, pressupostos, tópicos especiais, glossário, exemplos de utilização, e o esquema XML desenvolvido para apoiar o uso do Dicionário de Dados. Após a publicação do Dicionário de Dados o grupo de trabalho foi substituído pelo *PREMIS Maintenance Activity*, apoiado pela Biblioteca do Congresso dos Estado Unidos, e que foi incumbido de manter o Dicionário de Dados e coordenar esforços para aprofundar a compreensão de metainformação de preservação e tópicos relacionados. Este trabalho resultou na publicação da versão 2.0 do PREMIS em Março de 2008.[422] Seguiram-se alterações incrementais ao Dicionário de Dados e esquema XML na versão 2.1[423] em 2011 e na versão 2.2[424] no ano seguinte. Mais recentemente, *na PREMIS Implementation Fair* no iPres2013 in Lisboa, começaram a ser discutidas as alterações a serem incluídas no PREMIS 3.[425]

Confiança e Certificação

A segunda iniciativa patrocinada pela OCLC / RLG que criou um grupo de trabalho composto por especialistas internacionais para abordar as características de um repositório digital confiável, com o objectivo de enumerar as características que, em conjunto, servissem para inspirar, na Comunidade Designada, a confiança de que o repositório é de facto capaz de preservar e disponibilizar a parte da informação académica e cultural sob sua custódia.[426] Partindo dos conceitos e modelos apresentados na norma OAIS, publicaram em 2002 o relatório *Trusted Digital Repositories: Attributes and Responsibilities.*[427] Este documento apresenta um quadro de atributos e responsabilidades para repositório digital confiável, fiáveis e sustentáveis, capazes de lidar com a variedade de materiais mantidos por grandes e pequenas instituições de património cultural e de investigação. O quadro era suficiente amplo para acomodar uma heterogeneidade de situações, arquitecturas tecnológicas e responsabilidades institucionais, facultando uma base para as expectativas de um repositório confiável. Este documento foca atributos organizacionais e técnicos de alto nível e apresenta modelos potenciais para a certificação repositório digital. Outro aspecto deste documento é o facto de não tecer considerações sobre a natureza específica dos repositórios e arquivos digitais rapidamente emergentes, tendo em vez disso, reiterado o apelo à certificação de repositórios digitais, recomendando o desenvolvimento de programas de certificação e articulação de critérios auditáveis.

Baseando-se nos conceitos do modelo de referência OAIS, e em particular, na definição de um repositório digital confiável identificada no relatório do RLG/OCLC, foi estabelecido um grupo

[421] CAPLAN, Priscilla [et al.] - - Data dictionary for preservation metadata: final report of the PREMIS working group.
[422] GUENTHER, Rebecca [et al.] - PREMIS data dictionary for preservation metadata, v 2.0.
[423] GUENTHER, Rebecca [et al.] - PREMIS data dictionary for preservation metadata, v 2.1.
[424] GUENTHER, Rebecca [et al.] - PREMIS data dictionary for preservation metadata, v 2.2.
[425] PREMIS – 2013 PREMIS Implementation Fair (PIF) minutes.
[426] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 15.
[427] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities.

de trabalho constituído por indivíduos de uma variedade de origens institucionais e geográficas, a *Task Force on Digital Repository Certification*, sob o patrocínio do *National Archives and Records Administration* (NARA) e a RLG. O grupo de trabalho identificou "elementos certificáveis" de um repositório digital, e desenvolveu um plano para o estabelecimento de organismos, políticas e procedimentos competentes para certificação de repositórios digitais.[428] Em 2005 o grupo de trabalho publicou um projecto de lista de verificação para certificar repositórios digitais com o nome de *An Audit Checklist for the Certification of Trusted Digital Repositories*[429] e convidou a comunidade de interesse a comentar sobre este projecto de documento. A versão final resultou em 2007 no *Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)*[430], que reflecte esse feedback e os resultados de projectos do CRL, com a intenção de apresentar o seu trabalho para o processo de normalização no seio da Organização Internacional de Normalização (ISO). Esta intenção foi levada a cabo pela CCSDS, que partindo do *TRAC,* publica em 2011 as recomendações *Audit and Certification of Trustworthy Digital Repositories*[431] e *Requirements for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories*[432], actualmente, cuja segunda versão data de Março de 2014.[433] A primeira recomendação é aprovada como norma ISO 16363:2012[434] em 2012 e a segunda encontra-se actualmente em fase de análise como ISO/PRF 16919.[435]

Digno de nota é ainda o desenvolvimento na Alemanha, onde o Ministério da Educação e Investigação reuniu representantes de bibliotecas, arquivos, museus, instituições de investigação, organismos editoriais e especialistas em *software* e da área da certificação num grupo de trabalho para a certificação de repositórios digitais e que deu origem ao projecto *Network of Expertise in long-term STORage and Accessibility of Digital Resources in Germany* (NESTOR)[436], com o fito de criar um catálogo de critérios de fidedignidade e preparar a certificação de repositórios digitais de acordo com procedimentos nacionais e internacionais, nomeadamente no modelo de referência OAIS. Partindo de documentos como o *DINI Certificate for document and publication services*[437] do DINI (Iniciativa Alemã para a Informação de Rede), o relatório "*Trusted Digital Repositories: Attributes and Responsibilities*", e no trabalho que estava a ser desenvolvido pelo NARA/RLG no âmbito da produção do TRAC, publicou em 2006 a primeira versão do *NESTOR Catalogue of Criteria for Trusted Digital*

[428] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 16.
[429] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories - draft for public comment.
[430] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist.
[431] EUA. CCSDS - Audit and certification of trustworthy digital repositories. magenta book.
[432] EUA. CCSDS - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories. magenta book, V.1.
[433] EUA. CCSDS - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories: magenta book, V.2.
[434] ISO 16363:2012 - Space data and information transfer systems -- Audit and certification of trustworthy digital.
[435] ISO/PRF 16919 - Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories.
[436] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories.
[437] ALEMANHA. DINI Working Group “Electronic Publishing“ – DINI certificatedocument and publication services.

Repositories[438], tanto em alemão como em inglês, e a segunda versão data de 2008 (a tradução inglesa é publicada em 2009). Com base neste trabalho, o grupo de trabalho *DIN Working Group "Trusted Archives - Certification"* desenvolveu a norma *DIN 31644 "Information and documentation- Criteria for trustworthy digital archives"* [439], o que permitiu o desenvolvimento *do Nestor Seal for Trustworthy Digital Archives.*[440]

A intenção do desenvolvimento de um processo de certificação e acreditação num contexto internacional e com um conjunto unificado de critérios esbarrou em pequenas mas importantes diferenças entre os critérios da lista de requisitos de auditoria do TRAC e Catálogo de Critérios do NESTOR. Por enquanto, têm demonstrado ser impraticável um único conjunto normalizado de critérios e regras aplicáveis por razões geopolíticas[441], pelo que somente os critérios identificados no TRAC entraram no processo de normalização que deu origem à norma ISO 16363:2012.[442]

As questões da confiança, da certificação e dos instrumentos de apoio a essa certificação serão abordadas mais profundamente no capítulo 5.

Interface Produtor-Arquivo

Outra iniciativa do CCSDS abordou o desenvolvimento de uma descrição normalizada sobre a interface Produtor-Arquivo: ou seja, as interacções que ocorrem entre os produtores e um arquivo OAIS. Esta abordagem levou à publicação em 2004 da norma *Producer-Archive Interface Methodology Abstract Standard* (PAIMAS).[443] A norma divide o processo de transferência de informação do produtor para o OAIS num conjunto de fases distintas, e fornece uma descrição detalhada do resultado esperado de cada fase, bem como o conjunto de acções que devem ocorrer para produzir esse resultado. Este quadro serve como base para a identificação de áreas dentro da interface do Produtor-Arquivo que beneficiariam com normas, recomendações e boas-práticas mais aprofundadas, e também fornece uma base para o desenvolvimento de processos automatizados e aplicações de *software* que apoiem o processo de transferência de informação. Por fim, a norma oferece uma apresentação mais detalhada das responsabilidades e funções das entidades funcionais de Ingestão e de Administração do OAIS.[444] A Norma deu origem à ISO 20652:2006[445], sendo uma contribuição importante para dar forma à transferência de informação do produtor para o OAIS num processo consistente e bem compreendido. Isto é particularmente útil em termos de desenvolvimento de uma compreensão mútua entre produtores e arquivos no que diz respeito às suas responsabilidades e expectativas, enquanto participantes do processo de ingestão. A

[438] DOBRATZ, Susanne [et al.] – NESTOR catalogue of criteria for trusted digital repositories.
[439] ALLIANCE FOR PERMANENT ACCESS TO THE RECORDS OF SCIENCE NETWORK (APARSEN) - Report on peer review of digital repositories, p. 10; KEITEL, Christian - DIN Standard 31644 and NESTOR certification.
[440] HARMSEN, Henk [et al.] - Explanatory notes on the NESTOR seal for trustworthy digital archives; KEITEL, Christian - DIN Standard 31644 and NESTOR certification.
[441] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 5.
[442] ISO 16363:2012 - Space data and information transfer systems - Audit and certification of trustworthy digital.
[443] EUA. CCSDS - Producer-archive interface methodology abstract standard: magenta book.
[444] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 16.
[445] ISO 20652:2006 - Space data and information transfer systems -- Producer-archive interface : methodology abstract standard.

interface do Produtor-Arquivo está actualmente sob a forma de um projecto de norma, e foi disponibilizado aos interessados na comunidade de preservação digital para análise e comentário.

Metainformação Estrutural

No levantamento de actividades em curso voltadas para a preservação a longo prazo de materiais digitais, não é incomum encontrar o termo "compatível com OAIS" usado em relação a um sistema de arquivo digital. Os arquitectos da *Metadata Encoding and Transmission Standard* (METS)[446] , um documento sobre o formato de XML de apoio à gestão e intercâmbio de objectos digitais, destacam a sua potencial utilização como uma implementação do conceito de SIP ou um DIP. Tendo nascido no âmbito do projecto *Making of America II*[447] (1998), é uma norma de codificação cujo *schema* XML foi projectado para a produção de informação que expresse a estrutura hierárquica dos objectos digitais, registar os nomes e as localizações dos ficheiros que compõem esses objectos, e registar a metainformação descritiva, administrativa e estrutural associada. A última versão, 1.10[448] data de Setembro de 2013, e em Setembro de 2014 vão ser discutidas as bases da versão 2.0.

Para Concluir o Estado da Arte do OAIS

O modelo trata igualmente da migração da informação digital para novos suportes e formatos, propondo uma tipologia da migração e analisa os riscos inerentes a cada tipo de migração proposta. Analisa também a questão dos diferentes tipos cooperação possíveis entre os arquivos electrónicos. Estes tipos de cooperação podem ir desde um simples acordo referente às normas de empacotamento dos SIPs e DIPs até à partilha de recursos materiais e aplicacionais. A cooperação entre os arquivos digitais é uma questão essencial na medida em que constitui uma forma de consolidação de normas e ferramentas utilizadas e pode ser um factor decisivo em termos de redução de custos.[449]

Segundo Lavoie:

> *"The OAIS reference model is a conceptualization of the environment, functional components, and information objects associated with a system designed to effect the long-term preservation of digital materials."*[450]

No entanto Allinson considera que o modelo:

> *"OAIS is not an architectural model. It is an ontology, a terminology underlying a shared view and, as such, provides a means of communication […]."*[451]

De facto, o modelo OAIS não define qualquer implementação. Tal implementação estará, em parte, dependente da tecnologia e ferramentas disponíveis. A implementação da infrastrutura de *hardware* e *software* do arquivo evoluirá ao longo do tempo em resposta à evolução e

[446] METS - Metadata Encoding and Transmission Standard.
[447] HURLEY, Bernard [et al.] - The Making of America II testbed project: A digital library service model.
[448] METS – METS schema v1.10.
[449] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 55-56.
[450] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 14.
[451] ALLINSON, Julie - OAIS as a reference model for repositories: an evaluation, p. 11.

desaparecimento das tecnologias, enquanto que o modelo OAIS deve continuar válido, servindo como guia essencial para a implementação. Note-se também quem absoluto, o modelo OAIS não está especificamente destinado aos especialistas das Tecnologias da Informação Digital: deve permitir que todos os envolvidos, directa ou indirectamente, num processo de arquivo digital compreendam a lógica geral e possam participar nele de forma efectiva.[452]

> "*However, the reference model provides a starting point for implementation, in the sense that it characterizes the high-level responsibilities, services, and informational requirements that the implemented system must, in one form or another, incorporate."*[453]

O modelo também fornece uma base geral que cobre a conservação de informação que não esteja em formato digital (arquivos em papel, mas também colecções de objectos na área da arqueologia, amostras de laboratório, maquetes de arquitectura, etc.). Isto é importante porque, nos próximos anos, parecendo evidente que os arquivos terão de se adaptar ao mundo digital, os documentos em papel não vão desaparecer completamente. Alguns produtores de informação podem transmitir objectos digitais enquanto outros oferecem documentos em formato analógico. Durante um período transitório, que poderá ser bastante longo, os arquivos serão, portanto, obrigados a gerir tanto informação em formato digital como em forma física.[454]

O modelo OAIS fornece ainda uma estrutura para descrever e comparar arquitecturas e o funcionamento de serviços de arquivos digitais. É também um ponto de partida para uma nova geração de normas especializadas que lidam com os vários aspectos dos repositórios digitais.

O OAIS fornece uma visão abstracta e geral do problema, aplicável a vários contextos, o que resultou numa rápida adopção por parte de um vasto leque de comunidades profissionais: arquivos institucionais, bibliotecas, aeronáutica, pesquisa espacial.[455]

O modelo de referência OAIS tem sido muito bem-sucedido na consolidação da compreensão dos requisitos fundamentais para garantir a persistência a longo prazo de materiais digitais. A percepção partilhada desses requisitos é uma condição necessária para a construção de sistemas de arquivo digitais bem-compreendidos, sustentáveis, e, finalmente, confiáveis.[456]

Finalmente, na medida em que o modelo é amplamente reconhecido e utilizado, é um guia essencial para o desenvolvimento de *software* aplicacional livre e comercial no âmbito dos arquivos digitais.[457] O modelo OAIS é uma base fundamental para a reflexão em cada empresa ou organização para a implementação de um arquivo digital.[458]

---

[452] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 41-42.
[453] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 14.
[454] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 42.
[455] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 56.
[456] LAVOIE, Brain - The Open Archival Information System reference model: introductory guide, p. 17.
[457] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 42.
[458] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme, p. 56.

5 - Confiança e Certificação

O relatório da *RLG/CPA Task Force on Archiving of Digital Information* (1996) referindo-se à questão da confiança no âmbito dos arquivos digitais afirma que:

> *"For assuring the longevity of information, perhaps the most important role in the operation of a digital archive is managing the identity, integrity and quality of the archives itself as a trusted source of the cultural record. Users of archived information in electronic form and of archival services relating to that information need to have assurance that a digital archives is what it says it is and that the information stored there is safe for the long term."*[459]

Thibodeau, apoiando-se em Lynch (2000)[460] refere que a autenticação de objectos preservados é acima de tudo uma questão de confiança e que existem maneira de reduzir o risco que acarreta confiarem alguém, mas no fundo, precisamos de confiar numa pessoa, organização, sistema ou método que exerce controlo sobre a transmissão de informação pelo espaço, tempo ou fronteiras tecnológicas. Para ele, mesmo no caso dos objectos físico duráveis, como tábuas de argila, temos de crer, que confiar, que ninguém as substituiu por falsificações.[461]

De acordo com o relatório *Trusted Digital Repositories: Attributes and Responsibilities* (2002) a Arquivística e a Informática têm definido uma série de conceitos e termos de base para definir as características dos repositórios digitais seguros. No âmbito de projectos de produção, gestão e utilização de objectos digitais, podem encontrar-se termos como "credível" [Reliable], "responsável" [Responsible], "fidedigno ou digno de confiança" [Trustworthy] e "autêntico" [Authentic]. O debate terminológico é particularmente evidente no âmbito do desempenho, dos sistemas militares e das companhias aéreas, deu origem a novas abordagens, experiências, literatura, aplicações e ferramentas[462] que ajudam na definição de características, e o desenvolvimento e manutenção de sistemas seguros de repositórios digitais.[463] Mas o que querem dizer com os termos "arquivos confiáveis" ou "repositório confiável"?

Para dar resposta a estas questões, será necessário abordar:

- o conceito (confiança, confiabilidade, fidedignidade, etc.);

- o seu significado no âmbito dos repositórios digitais;

- que instrumentos existem para garantir ou pelo menos para reforçar a confiança e fidedignidade dos repositórios digitais.

[459] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. 23.
[460] LYNCH, Clifford - Authenticity and integrity in the digital environment.
[461] THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years, p. 14.
[462] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 8.
[463] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 8.

Conceitos

Confiança

Embora o conceito de confiança seja utilizado comumente, e seja amplamente estudado em várias disciplinas, ainda não foi alcançado um consenso total sobre a sua definição no âmbito de relações sociais que incorporam confiança e, mais concretamente, em sistemas perpetuadores de confiança [464]. Autores como Rousseau[465] e Gambetta[466] consideram que o conceito de confiança é difícil de definir ou medir, na medida em que se revela um termo vago e com uma definição evasiva. Definir confiança no âmbito dos repositórios digitais tem é uma questão subjectiva que está dependente do contexto de utilização.

As definições de "confiança" [*trust*] que se encontram nos dicionários incluem a "crença" [*confidence*] ou o "crédito" [*reliance*] em alguma qualidade ou atributo de uma pessoa ou coisa, ou a verdade de uma afirmação.[467] Para Simmel[468] estes termos estão ligados com a "fé", enquanto que Luhman[469], admitindo a relação entre esta e "confiança", destingue-as afirmando que a confiança é algo que está relacionada com o risco e que só pode ser compreendida em relação a ele. Isto prende-se com a percepção de que as nossas actividades ou decisões podem ter como consequência acontecimentos ou resultados imprevistos, em vez de algo ligado à sorte, fado ou fortuna. Assim, apesar de tanto a confiança e a crença se referirem a expectativas que podem ser frustradas ou desencorajadas, esta consciência das circunstâncias de risco não existe no âmbito da crença, que para Luhman, tem a ver com uma atitude mais ou menos tida como certa de que as coisas familiares permanecerão estáveis. Para este autor, numa situação de confiança, o indivíduo mede as consequências e possíveis perigos, analisa as alternativas, calcula o risco, e, em situação de frustração assume parcialmente a responsabilidade e pode arrepender-se de ter depositado confiança em alguém ou algo.

Esta distinção entre confiança e crença, e entre risco e perigo é assumida por Giddens[470], mas refere que a confiança não se limita a um estado contínuo, sendo um tipo específico de crença [*confidence*].[471] Este autor considera que não existe conexão intrínseca entre crença [*confidence*] e perigo, na medida em que este existe em circunstâncias de risco, sendo relevante para a definição deste. Face a Gambetta e Dunn[472], que defendem que que a confiança é um dispositivo para se lidar com a liberdade dos outros, Giddens acrescenta que o requisito principal para a confiança é a falta de informação plena, informação esse que adviria de actividades continuadamente visíveis, processos transparentes, conhecidos e

[464] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development, p. 22.
[465] ROUSSEAU, Denise [et al.] - Not so different after all: across-discipline view of trust.
[466] GAMBETTA, Diego - Can we trust trust?.
[467] Cft. MERRIAN-WEBSTER DICTIONARY. In Merriam Webster Web site; trust in INFOPÉDIA. Dicionários Porto Editora; confiança In INFOPÉDIA. Dicionários Porto Editora; fidedigno In INFOPÉDIA. Dicionários Porto Editora; fiável In INFOPÉDIA. Dicionários Porto Editora.
[468] SIMMEL, Georg – The philosophy of Money.
[469] LUHMANN, Niklas - Familiarity, confidence, trust: problems and alternatives.
[470] GIDDENS, Anthony - As consequëncias da modernidade.
[471] GIDDENS, Anthony - As consequëncias da modernidade, p. 34.
[472] GAMBETTA, Diego - Can we trust trust?; DUNN, John - Trust and political agency, no mesmo volume.

compreendidos.[473] O autor avança a seguinte definição de confiança: "crença [*confidence*] na credibilidade [*reliability*] de uma pessoa ou sistema, tendo em vista um dado conjunto de resultados ou eventos, em que essa crença expressa uma fé na probidade ou amor de um outro, ou na correção de princípios abstratos (conhecimento técnico)".[474] Assim, a confiança existe na medida em que se considera que toda a actividade humana é criada socialmente (e não pela natureza ou por influência divina), e que a acção humana tem como intuito a transformação, derivada do dinamismo das instituições sociais modernas.[475] Adicionalmente, Giddens refere que o risco pressupõe o perigo, entendido como uma ameaça aos resultados pretendidos e que a confiança serve para reduzir ou minimizar os perigos a que estão sujeitos tipos específicos de actividade.[476] Assim, assumir um "risco calculado" é estar consciente das ameaças decorrentes de uma linha de acção, e, quando os padrões de risco são institucionalizados no interior de estruturas abrangentes de confiança, desenvolve-se conceito de risco "aceitável" – minimização do perigo – que é fulcral para a manutenção da confiança.[477] Tal parece vir na linha de Yakel, que recupera a definição de Rousseau*:*

> *"A psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another."*[478]

Neste âmbito, Giddens avança com a definição de segurança que considera ser a situação em que o conjunto de perigos está neutralizado ou minimizado e cuja experiência se traduz num equilíbrio de confiança e risco aceitável.[479]

Apresentando uma evolução da definição de Confiança, Yoon (2014), baseia-se em Rousseau (1998) para sustentar a existência de dois pré-requisitos: o risco, ou probabilidade percepcionada de perda, ligado ao conceito de incerteza que pode resultar da falta de informação e da existência de vulnerabilidades; e a interdependência, neste caso entre a entidade que confia e a entidade que é objecto de confiança.[480]

Quanto às dimensões da confiança, a autora refere que existem diferentes tipos, dependendo de diferentes factores:

- Confiança baseada no cálculo, com base numa escolha racional derivada de informação credível sobre a boa intenção do outro, e que pode ser fornecida pela reputação ou certificação;

- Confiança Relacional, derivada da interacção repetida ao longo do tempo entre as duas partes;

[473] GIDDENS, Anthony - As consequëncias da modernidade, p. 35.
[474] GIDDENS, Anthony - As consequëncias da modernidade, p. 36.
[475] GIDDENS, Anthony - As consequëncias da modernidade, p. 36.
[476] GIDDENS, Anthony - As consequëncias da modernidade, p. 36.
[477] GIDDENS, Anthony - As consequëncias da modernidade, p. 36 e 37.
[478] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 144, cft. ROUSSEAU, Denise [et al.] - Not so different after all: across-discipline view of trust, p. 395.
[479] GIDDENS, Anthony - As consequëncias da modernidade, p. 37.
[480] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development, p. 22; ROUSSEAU, Denise [et al.] - Not so different after all: across-discipline view of trust, p. 395.

- Confiança baseada na instituição, sentimento de segurança de quem confia, por causa das garantias de estrutura, tais como salvaguardas, regulamentos ou o sistema legal.

Nos dois primeiros tipos, a fiabilidade e a confiança em interacções anteriores cria e aumenta as expectativas ou crenças positivas de quem confia acerca da entidade que é objecto de confiança.[481]

Nesse sentido podemos considerar que as instituições ligadas ao património cultural são fidedignas, na medida em que são responsáveis pelos materiais e objectos que compõem esse património, e também pela sua guarda, pelas condições de acesso e de garantia de preservação a longo prazo. A confiança nestas instituições baseia-se no conhecimento, experiência e prática demonstrável pela salvaguarda de objectos físicos. Mas no âmbito do património digital, dadas as suas características e desafios apresentados na sua preservação, esta confiança e garantia de fidedignidade são mais difíceis de alcançar, e muitas das instituições culturais, como bibliotecas, museus e arquivos, não estão actualmente preparadas para cumprirem com as suas funções tradicionais de armazenamento, preservação e de garantir a acessibilidade, no âmbito do património digital, tendo que recorrer a serviços especializados de entidades externas.

O relatório *Trusted Digital Repositories: Attributes and Responsibilities* [482] refere que no âmbito dos repositórios digitais confiáveis, se aplicam três níveis de confiança:

1. Como as instituições culturais conquistam a confiança das suas comunidades designadas;

2. Como as instituições culturais confiam nos fornecedores externos;

3. Como os utilizadores confiam nos documentos que lhes são fornecidos por um repositório.[483]

A confiança no primeiro nível decorre da reputação que tem origem na experiência demonstrada e da expectativa que o público tem de que essas entidades vão continuar a garantir o acesso à informação de forma confiável, através do desenvolvimento contínuo de sistemas que suportam o acesso a longo prazo aos materiais.

A confiança no segundo nível decorre da comprovação de confiabilidade através do cumprimento das responsabilidades contratuais e da demonstração de sensibilidade com as questões da comunidade, principalmente num quadro de certificação com base em critérios ou atributos que as entidades externas que fornecem serviços devem cumprir, para alcançarem um nível de reputação elevado.

A confiança no terceiro nível decorre da capacidade de garantir a autenticidade, integridade e fidedignidade da informação digital fornecida ao utilizador. Isto passa pela garantia de detecção de qualquer modificação ao documento digital, seja ela intencional ou acidental, que o documento recebido foi o solicitado e que se pode verificar que se trata exactamente do

[481] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development. p. 22-23.
[482] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities.
[483] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 9.

mesmo objecto que foi anteriormente depositado no repositório digital. Exemplos disso são fornecidos por Gladney[484]: a utilização de tecnologias como técnicas de detecção de erros sistemas de criptografia, e normas e boas práticas relativas a metainformação.

O grupo de trabalho NESTOR (2008) refere que a confiabilidade ou fidedignidade de um sistema reside na capacidade deste operar de acordo com os seus objectivos e especificações, ou seja, que faz aquilo que diz fazer. Do ponto de vista da segurança das tecnologias da informação, ela tem como base integridade, a autenticidade, a confidencialidade e a disponibilidade dos objectos digitais. A Segurança no âmbito das tecnologias da informação é assim o pré-requisito mais importante para repositórios digitais de confiança.[485] Desta forma a confidencialidade (ou segurança) diz respeito aos privilégios e permissões inerentes à utilização dos recursos de informação.[486]

A literatura referente à confiança e organizações na área da gestão e dos sistemas de informação consagra-se às questões da confiança dos funcionários/colaboradores e da confiança das partes interessadas externas na organização. Yakel[487] parte das perspectivas da confiança organizacional no âmbito da gestão, e da aceitação da tecnologia no âmbito dos sistemas/tecnologias da informação, focando-se em três factores:

1. Confiança das partes interessadas na organização;

2. Garantias da Estrutura; e

3. Factores Sociais.

O primeiro factor apresenta quatro dimensões: a benevolência, ou percepção que os clientes têm de que a organização demonstra boa vontade para com o cliente; a integridade, ou percepção que a organização é honesta e trata as partes interessadas com respeito; a identificação ou percepção de que significa que a organização compreende e internaliza os interesses das partes interessadas; e transparência, ou partilha de informação relevante para a confiança das partes interessadas

O segundo factor refere-se à sensação de segurança emanada de garantias, redes de segurança, ou outras estruturas impessoais inerentes a um contexto específico[488], focando-se em aspectos como o aval dado por terceiros, garantias (acções por parte da organização que os interessados entendem como mitigação de riscos), e a reputação.

O terceiro factor está ligado à influência social de três tipos: Colegas ou Pares, Mentores ou colegas mais experiente, e finalmente, as Instituições.

---

[484] GLADNEY, Henry - Perspectives on trustworthy information.

[485] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 9.

[486] DOBRATZ, Susanne; SCHOGER, Astrid - Trustworthy digital long-term repositories: the NESTOR approach in the context of international developments, p. 212; DOBRATZ, Susanne; SCHOGER, Astrid; STRATHMANN, Stefan - The NESTOR catalogue of criteria for trusted digital repository evaluation and certification.

[487] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 145-148.

[488] GEFEN, David; KARAHANNA, Elena; STRAUB, Detmar W. - Trust and TAM in online shopping: an integrated model. MIS Quarterly. Minneapolis, Mn. ISSN: 02767783. Vol. 27, nº. 1 (2003), p. 51-90, *apud* YAKEL, Elizabeth [et al.] - Trust in digital repositories.

A Confiança no Âmbito dos Repositórios Digitais

Como já vimos anteriormente, o *Relatório RLG/CPA Task Force on Archiving of Digital Information* (1996)[489] defende que para serem confiáveis, os arquivos digitais têm que demonstrar que conseguem preservar a informação e a sua autenticidade a longo prazo, enfatizando as competências e objectivos das organizações "confiáveis", em termos de armazenamento, migração e fornecimento de acesso à informação. A necessidade de demonstração decorre do facto de que o estabelecimento de um clima de confiança junto dos vários intervenientes, desde os produtores aos consumidores, que interagem com o repositório não é suportável somente pela afirmação de capacidade de garantia de acesso continuado à informação.[490]

A produção do relatório *Trusted Digital Repositories: Attributes and Responsibilities*[491] pelo grupo de trabalho patrocionado pela OCLC / RLG em 2002, e de que já se falou no capítulo 4, desperta o interesse de Granger, que no mesmo ano, tece alguns comentários no âmbito do exposto deste relatório:

> *"The report:*
> *Proposes a definition of a trusted digital repository;*
> *Identifies the primary attributes of a trusted digital repository;*
> *Articulates a framework for the development of a certification program;*
> *Identifies the responsibilities of an OAIS-compliant digital repository;*
> *Informs the RLG/OCLC communities of other developments necessary to implement a reliable repository; and,*
> *Provides formal recommendations for future work."*[492]

O *Trusted Digital Repositories: Attributes and Responsibilities* (2002) apresentam assim a necessidade de repositórios digitais confiáveis, que definem:

> *"A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future."*[493]

Este documento considera também que os repositórios digitais confiáveis/fidedignos/de confiança podem assumir diferentes formas, que podem ir desde a opção de construir repositórios locais por parte de algumas instituições, até à opção de gerir apenas os aspectos

[489] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information.
[490] Cft. SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais; AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 94; BECKER, Christoph - Trustworthy preservation planning; FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital.
[491] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities.
[492] GRANGER, Stewart - Digital preservation and deep infrastructure.
[493] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. I.

lógicos e intelectuais de um repositório, contratualizando o seu armazenamento e manutenção a uma entidade externa.[494]

A questão tem eco em Portugal, logo no ano seguinte, pela mão de Saramago (2003), que adopta ainda a definição da RLG/OCLC:

> *"Um repositório de recursos digitais confiável é aquele cuja missão consiste em fornecer acesso a longo prazo a recursos digitais de uma designada comunidade no presente e no futuro de forma permanente e garantida."*[495]

A autora, bebendo do relatório do RLG/OCLC de 2002, refere que independentemente da infrastrutura de base adoptada, para atingir os seus objectivos, 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, que aceite a responsabilidade da manutenção dos recursos digitais a longo prazo de acordo com os interesses dos depositantes e dos actuais e futuros utilizadores, que demonstre a responsabilidade e sustentação financeira, que o seu planeamento seja de acordo com as recomendações e normas internacionais referentes à gestão, acesso e segurança a longo prazo dos recurso digitais depositados, que defina metodologias para avaliação da qualidade dos sistemas de acordo com as expectativas de confiabilidade da comunidade, e que mantenha políticas, práticas e desempenhos auditáveis e aferidas por entidades independentes.[496]

Hockx-Yu (2006) refere que a confiança é um assunto que se pode tornar uma barreira importante para repositórios institucionais e aumentar a complexidade da preservação digital, e não está somente relacionada com a longevidade dos objectos digitais armazenados dentro do repositório, mas também com a sustentabilidade financeira do próprio repositório e as questões humanas ligadas à competência e confiabilidade.[497]

Se para o NESTOR (2006 e 2008), a segurança das tecnologias da informação é assim o pré-requisito mais importante para os repositórios digitais de confiança[498], o TRAC vem criticar esta definição, defendendo que é preciso olhar não só para o sistema aplicativo de preservação digital, mas para todo o sistema em que a informação digital é gerida, incluindo a organização que opera o repositório[499], as práticas de gestão de objectos digitais, a infra-estrutura tecnológica e a segurança dos dados, que devem ser satisfatórios e adequados para cumprir a missão e os compromissos do repositório.[500] Por outro lado, o NESTOR considera que a implementação de critérios ou requisitos para o desenvolvimento de um repositório

[494] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 5.
[495] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais, p. 71.
[496] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais, p. 71. Cft. BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 5.
[497] HOCKX-YU, Helen – Digital preservation in the context of institutional repositories, p. 5.
[498] DOBRATZ, Susanne [et al.] – NESTOR catalogue of criteria for trusted digital repositories, p. 3. BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 5.
[499] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 3.
[500] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 3.

digital de longo prazo que seja confiável tem que ser verificada à luz dos objectivos gerais do sistema.[501] Nesta linha o TRAC afirma que um repositório digital confiável requer monitorização, planeamento e manutenção constantes, bem como acções e implementação de estratégias conscientes, no âmbito da percepção e avaliação das ameaças e riscos dentro dos seus sistemas.[502] Para o NESTOR tal requer um processo de várias fases, que vão da concepção, planeamento e especificação, Execução e implementação e Avaliação, sempre num quadro de gestão de qualidade para monitorizar o processo [503,] e que permita a adequação das medidas para cumprimento dos critérios. O TRAC refere que a demonstração de resultados de auditoria ao público -transparência- dará origem a uma maior confiança e auditorias objectivas adicionais, conducentes a possível certificação, irão promover ainda mais a confiança no repositório e no sistema que o suporta.[504] Para o NESTOR, tal é feito pela publicação de documentação pertinente para este processo, na medida em que ajuda a aumentar a transparência e, logo, a confiança nele depositada.[505] Finalmente, o TRAC não esquece um aspecto considerado muito importante: alcançar o estatuto de confiável não é uma realização de uma só vez - alcançada e esquecida. Para manter o estatuto de confiança, um repositório terá que empreender um ciclo regular de auditoria e / ou certificação.[506]

A certificação é já abordada na conclusão do relatório da Task Force (2002), que afirma que um componente essencial da infrastrutura de arquivo digital é a existência de um número suficiente de organizações de confiança capazes de armazenar, migrar e fornecer acesso às colecções digitais, sendo necessário um processo de certificação de arquivos digitais para criar um clima de confiança generalizado relativo à preservação de informação digital, uma vez que os arquivos digitais certificados devem ter o direito e o dever de exercer funções de salvaguarda activa, como um mecanismo de salvaguarda para preservar informação digital valiosa que está em risco de destruição, negligência ou abandono pelo actual depositário[507].

Esta necessidade de demonstrar e de formas de avaliar/auditar a confiabilidade do repositório transparece em Saramago (2003), que afirma:

> *"[…] um elemento da maior importância será a existência de um processo de certificação de repositórios digitais que assegure um clima de segurança no que diz respeito ao futuro da preservação digital."*[508]

Seamus Ross e Andrew Mc Hugh referem mesmo que é evidente que a certificação seja uma marca que ajuda os utilizadores a determinar o nível de confiança razoável que podem ter

[501] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 6.
[502] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 3.
[503] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 6.
[504] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 4.
[505] BERGMEYER, Winfried - nestor criteria catalogue of criteria for trusted digital repositories, p. 38.
[506] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 4.
[507] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. 40.
[508] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais, p. 9.

num repositório digital em particular, e que a auditoria é um passo fundamental para verificar se existem condições para certificar esse repositório.[509]

Para o NESTOR:

> *"A* [trusted]*, long-term digital repository is a complex interrelated system"*[510]*,*

sendo a confiança uma necessidade inerente à comunidade na qual o repositório digital se insere, quer para os seus utilizadores, quer para os produtores de informação e conteúdos, quer para as entidades financiadoras que cedem os seus recursos, ou os próprios repositórios. Por essa razão a avaliação/certificação deve ter em conta as necessidades e expectativas das partes interessadas, o que também assegura um maior grau de validação universal, adequação prática para a utilização do dia-a-dia, e também uma base ampla de aceitação dos resultados obtidos.[511]

O PLATTER (2010) refere que o conceito de confiança tem uma definição mais clara, no sentido em que um repositório é considerado de confiança de se conseguir demonstrar a sua capacidade para cumprir com as suas funções, e se essas funções satisfazem um conjunto mínimo de critérios acordados que se supõe serem exigidos a todos os repositórios confiáveis. O requisito de comprovação de conformidade é essencial, na medida que se assume que a conquista de confiança está intimamente ligado a processos de auditoria e certificação.[512]

Ross[513] e DRAMBORA[514] referem um conjunto de elementos que constituem evidência para qualquer processo de avaliação transparente, e que podem ir desde evidência documental (como mandato de organização e da missão; exemplo de contratos de depósito, descrições de funções, organogramas e currículos dos funcionários, planos de negócios e relatórios financeiros anuais; documentos de política e manuais de procedimentos, documentos de fluxo de trabalho, planos de arquitectura técnica, relatórios de manutenção, e os resultados publicados de outras auditorias, registo de riscos, etc.), observação de práticas, testemunhos de vários agentes (Administradores, gestores da infrastrutura, gestores dos macroprocessos do repositório, depositantes e consumidores de informação)

Para Prieto[515], a confiança tem muitas interpretações e é um factor importante numa variedade de transacções, concluindo que os repositórios digitais podem ser fidedignos por aderirem a normas tecnológicas, práticas aceites e mecanismos para autenticação de autoria e precisão do seu conteúdo, mas, em última análise, são as percepções das suas partes interessadas - tanto os que depositam como os que usam o conteúdo - que desempenham um papel central em assegurar a fidedignidade de um repositório digital.[516]

---

[509] ROSS, Seamus; HUGH, Andrew - The role of evidence in establishing trusting repositories.
[510] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 6.
[511] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 1.
[512] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance (PLATTER), p. 8.
[513] ROSS, Seamus; HUGH, Andrew - The role of evidence in establishing trusting repositories.
[514] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment p. 29-30.
[515] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories.
[516] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 596 e p. 603.

Prieto, sustentando-se na definição da missão dos repositórios fornecida pelo documento *Trusted Digital Repositories: Attributes and Responsibilities*[517], refere que os repositórios digitais podem assumir diversas formas, e as suas comunidades de utilizadores (depositantes e consumidores dos recursos digitais) podem também variar, tal como as suas necessidades, ou as suas práticas de trabalho, pelo que estas devem ser tidas em conta para tornar o repositório confiável. Tal concorrerá para que a percepção de confiança das comunidades de utilizador aumente a possibilidade de um repositório ter sucesso entre os depositantes e utilizadores de conteúdo.[518]

Para o autor, os repositórios digitais confiáveis podem ser classificados como ''de confiança'' no âmbito do processo de certificação principalmente porque eles cumprem ou excedem as expectativas e as necessidades das comunidades de utilizadores para os quais foram projectados. Isto passa pelo reconhecimento de normas e boas práticas relevantes para a sua comunidade e empresas do ramo da gestão e segurança da informação.[519] O autor considera que esta definição também reconhece que componentes, como as normas, segurança e um sistema de auditorias desempenham papéis importantes no desenvolvimento de uma infrastrutura de repositório concebido para alcançar um estatuto de fidedignidade aos olhos dos gestores de conteúdo, produtores e utilizadores. Da mesma forma isso implica estabelecer metodologias para avaliação do sistema que atendam às expectativas da comunidade de confiabilidade[520], bem como cumprir com as suas responsabilidades de forma aberta e explicita relativamente depositantes e utilizadores.[521]

O TRAC refere ainda que um repositório digital confiável deve ter estratégias de preservação documentadas. No entanto, um repositório digital confiável não pode simplesmente dizer que o fará; deve demonstrar as suas políticas, práticas e procedimentos. Nesse sentido, o repositório deve ser capaz de demonstrar que tomou decisões relevantes sobre os formatos aceitáveis, a existência de fluxos de trabalho automatizados e/ou manuais com abrangência para encaminhar objectos digitais adequados, o desenrolar de acções de preservação antecipadas e/ou aplicadas relativamente a AIPs individuais ou de grupos de AIPs, a existência de políticas, procedimentos e práticas de armazenamento de arquivo que garantam a captura e armazenamento de arquivo eficaz e de confiança, e que dêem resposta às mudanças tecnológicas inevitáveis, e que detêm meios independentes para verificar o conteúdo do repositório previsto com base num rastreio seguro dos objectos digitais recebidos.[522]

A pesquisa de Yakel conseguiu ainda concluir que as funções do repositório são indicadores de confiança; que a transparência é de facto um factor de confiança[523]; que a disciplina/área do saber e o nível de especialização afectam a percepção de confiança[524]; que o segundo factor

[517] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p I.
[518] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 595.
[519] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 603; Cft. AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 6.
[520] Cft. BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 5.
[521] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 595.
[522] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 85.
[523] Cft. SCHUMANN, Natascha - Tried and trusted: experiences with certification processes at the GESIS Data Archive.
[524] Cft. PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 598-599.

anteriormente apresentado (Garantias da estrutura), deve ainda incluir os aspectos de garantia de preservação (Preservação implica que determinados regimes estão em vigor para garantir o acesso contínuo aos dados) e a sustentabilidade (sustentabilidade implica que o repositório tomou as medidas para se estabelecer organizacionalmente com as estruturas de governança, financeiras e legais adequadas.); e, finalmente, que Reputação institucional é deveras importante.[525] Constata-se assim que a confiança no repositório é um factor separado e distinto de confiança nos dados[526]. Vendo a confiança como parte integrante da relação entre as comunidades designadas e repositórios digitais, tal reflecte a qualidade das outras operações de repositório.

Podemos concluir, de acordo com RAMALHO[527], que um repositório se torna digno de confiança pela via da reputação, documentando todo o ciclo de vida dos Objectos Digitais que custodia e seguindo requisitos para auditoria e certificação.

Responsabilidades

O *Trusted Digital Repositories: Attributes and Responsibilities* (2002) também apresenta as Responsabilidades de um repositório digital confiável, que divide em Responsabilidade Organizacional de alto nível e de Curadoria e Responsabilidades Operacionais. A primeira responsabilidade deve ser entendida a três níveis básicos: as organizações devem primeiro identificar os requisitos que têm que cumprir; em segundo lugar devem identificar outras organizações com as quais podem partilhar essas responsabilidades; em terceiro lugar devem identificar quais as responsabilidades que podem partilhar e como. Os principais factores a ter em conta neste âmbito são:

- O âmbito das Colecções;
- A gestão da Preservação e do Ciclo de Vida;
- O vasto leque de partes interessadas;
- A propriedade material e outras questões legais;
- As implicações dos custos.[528]

As Responsabilidades Operacionais baseiam-se na recomendação, emanada pelo relatório CPA / RLG (1996) de encetar um diálogo entre as organizações e as entidades competentes acerca das normas, critérios e mecanismos necessários para certificar os repositórios de informação digital como arquivos[529], e nas responsabilidades identificadas pelo Modelo de Referência OAIS[530], às quais acrescenta o papel crucial que os repositórios digitais confiáveis

[525] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 153.
[526] Cft. PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 599.
[527] RAMALHO, José Carlos - RODA: Repositório de Objectos Digitais Autênticos.
[528] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 17.
[529] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. IV.
[530] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): magenta book, p. 3-1.

desempenham na promoção das normas desta área[531], no sentido de realizar economias de escala e redução de custos, assegurando a criação de património digital de acordo com os procedimentos e práticas de preservação digital.[532] Resumidamente, as responsabilidades referenciadas são:

- Negociar e aceitar informação adequada da parte dos produtores da informação.[533] Deve negociar os critérios que ajudam na determinação dos tipos de informação que está disposta ou é obrigada a aceitar;[534]

- Obter um nível de controlo da informação fornecida suficiente para garantir a preservação a longo prazo;[535]

- Definir quais as comunidades que devem ser consideradas parte da Comunidade Designada do repositório e assegurar que conseguem compreender a informação fornecida;[536]

- Assegurar que a informação a preservar é compreensível para a Comunidade Designada, sem necessidade de recursos especiais, tal como o apoio dos especialistas que a produziram;[537]

- Promover Boas Práticas na criação de recursos digitais, seguindo políticas e procedimentos fundamentados documentalmente e que assegurem que a informação é preservada/protegida contra todas as contingências razoáveis, no âmbito de uma estratégia aprovada;[538]

- Disponibilizar a informação preservada à Comunidade Designada e possibilitar a sua divulgação tanto como cópias ou de forma a associá-la aos objectos de dados originais ingeridos com elementos que provem da sua autenticidade.[539]

Banat-Berger (2009) identifica estas responsabilidades com as dos arquivos ditos tradicionais, mas acrescenta aspectos ligados aos riscos derivados da perda da inteligibilidade da

[531] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 21.
[532] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 31.
[533] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-1.
[534] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-2.
[535] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-1.
[536] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-1.
[537] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-1.
[538] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-1.
[539] EUA. CCSDS - Reference model for an Open Archival Information System (OAIS): Magenta Book, p. 3-1.

informação electrónica, e pela falta de domínio de conteúdos estáveis num ambiente instável.[540]

Está-se assim em condições de afirmar que esta estrutura de atributos e responsabilidades para comprovar a confiabilidade e a confiança dos repositórios digitais, é claramente influenciada pelo relatório da CPA/RLG de 1996, que, como já se viu anteriormente, pretendia que os repositórios deveriam cumprir com requisitos de certificação que garantissem prova de que cumpriam a sua função de arquivo, e que tal certificação incluiria a existência de um plano de sucessão em que um outro repositório de arquivo certificado salvaguardasse o património cultural digital:

> *"The current repository may be a digital library, another digital archives, or some other individual, organizational, public or private source of digital information. Without the operation of a formal certification program and a fail-safe mechanism, preservation of the nation's cultural heritage in digital form will likely be overly dependent on marketplace forces, which may value information for too short a period and without applying broader, public interest criteria."*[541]

Certificação

Tendo abordado o conceito de confiança e o que significa no âmbito dos repositórios digitais, verifica-se que a certificação é o caminho a seguir para garantir ou pelo menos para reforçar a confiança e fidedignidade dos repositórios digitais. Falta agora referir as abordagens ou modelos e ainda os instrumentos que existem actualmente para o suporte da certificação.

O *Trusted Digital Repositories: Attributes and Responsibilities* (2002) considera também que existem pelo menos dois modelos viáveis para a certificação de repositórios digitais confiáveis: o modelo de auditoria, aplicável a entidades que guardam documentos governamentais, especialmente os documentos de arquivo electrónicos; e o modelo de normas, que opera em vários arquivos e bibliotecas, em que as instituições envolvidas nestas actividades aderem às normas estabelecidas pelos órgãos competentes, enquanto outras entidades "certificam" o produto ou serviço através da sua aceitação e / ou uso do mesmo. No entanto, muito embora ambos os modelos funcionem bem, não conseguem resolver completamente a variedade de actividades, funções e responsabilidades relacionadas com os repositórios digitais."[542]

O *Trusted Digital Repositories: Attributes and Responsibilities* (2002) sublinha a identificação de quatro abordagens gerais para certificação, por Bruce Ambacher (NARA), no âmbito do *Archival Workshop on Ingest, Identification, and Certification Standards* (AWIICS) em 1999: individual, programa, processo e dados.[543] O primeiro diz respeito à certificação ou acreditação

[540] BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme. Les débuts de la maturité, p. 42.
[541] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. 9.
[542] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 33.
[543] ARCHIVAL WORKSHOP PROGRAM COMMITTEE - Archival workshop on ingest, identification, and certification standards (AWIICS) draft report.

dos profissionais a título individual; o segundo refere-se à certificação com base num conjunto de auto-avaliação com base numa lista de requisitos normalizados e inspecções por entidades de acreditação referentes às áreas de competência/autoridade legal, a autoridade de administração, recursos financeiros, pessoal, instalações, desenvolvimento de colecções, preservação, acesso e divulgação do acervo; o terceiro, ou seja, o Processo de certificação avalia os métodos e procedimentos que podem ser submetidos a orientações quantitativas ou qualitativas para a adesão aos requisitos internos e externos; o último, a certificação de dados aborda a persistência ou a confiabilidade de dados ao longo do tempo e segurança de dados. A Certificação para persistência de dados inclui o controlo interno e externo de qualidade, manuais de procedimentos e documentação dos processos de migração de dados, criação e manutenção de metainformação, a actualização de dados ou ficheiros, e autenticação de novas cópias.

Com base em elementos de certificação referentes a cada um destas quatro abordagens, os participantes do *workshop* AWIICS criaram uma lista preliminar de requisitos com vista ao desenvolvimento de um programa de certificação passível de fornecer confiança[544] no âmbito do esforço de normalização referente ao modelo de referência OAIS. Tanto o conceito de lista de verificação como os elementos certificáveis previstos no workshop servem de base a um quadro de certificação.

Instrumentos de suporte à Certificação

Como já foi referido anteriormente, o Relatório *RLG/CPA Task Force on Archiving of Digital Information* (1996) considera ainda que os repositórios de informação digital a que se referem estariam ligados no âmbito de um sistema de arquivo nacional através de dois mecanismos: um programa de certificação independente de arquivos baseado em normas e critérios, e que os arquivos digitais certificados teriam um mecanismo de segurança crítica para garantir a recuperação da informação digital de valor cultural.[545]

O *Trusted Digital Repositories: Attributes and Responsibilities* (2002) considera que os repositórios digitais confiáveis, independentemente das situações e responsabilidades institucionais, devem ter as suas características expectáveis enquadradas em termos de:

- Conformidade com o Modelo de Referência OAIS;
- Responsabilidade administrativa;
- Viabilidade Organizacional;
- Sustentabilidade financeira;
- Adequação tecnológica e procedimental;
- Segurança do sistema

[544] ARCHIVAL WORKSHOP PROGRAM COMMITTEE - Certification of digital archives and preservation methodology: certification input document.
[545] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. III.

- Prestação de contas procedimental (ligada à certificação).[546]

As relações entre os atributos dos repositórios digitais confiáveis (TDR) são retratadas no modelo de Cornell (figura 8).[547] A conformidade OAIS está implícita no diagrama. Para McGovern[548], o *Trusted Digital Repositories: Attributes and Responsibilities* (2002) destaca a importância do contexto organizacional e coloca a tecnologia dentro desse contexto. Este posicionamento reconhece que a tecnologia deve estar adaptada ao âmbito e às necessidades de cada programa de preservação digital. O modelo de Cornell para repositórios digitais confiáveis adicionou uma " fronteira de arquivos digitais " para os atributos dos repositórios digitais confiáveis porque uma organização pode manter mais que uma instância de repositórios, devendo neste caso as camadas exteriores poderem ser coordenadas transversalmente pela organização, e várias organizações podem unir-se para gerir um repositório (por exemplo, um consórcio).

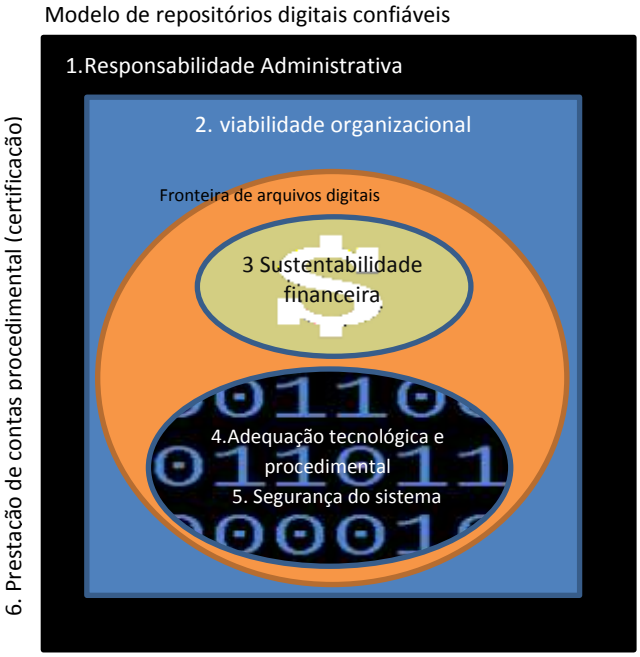

Figura 8 - O Modelo Cornell para Atributos de Repositórios Digitais Confiáveis

Tanto este modelo como o conceito de lista de verificação e os elementos certificáveis previstos no *workshop* servem de base a um quadro de certificação identificados no AWIICS, tiveram como consequência uma série de instrumentos de suporte à certificação que serão agora apresentados.

[546] BEAGRIE, Neil [et al.] - Trusted digital repositories: attributes and responsibilities, p. 13.
[547] CORNELL UNIVERSITY LIBRARY; ICPSR; MIT LIBRARIES – Attributes of a TDR. In *Digital preservation management:* http://dpworkshop.org/dpm-eng/foundation/tdr/index.html.
[548] MCGOVERN, Nancy - A digital decade: where have we been and where are we going in digital preservation?.

Certificação e Auditoria: o TRAC e a ISO 16363:2012

Como vimos no capítulo anterior, o Modelo de Referência OAIS e o Relatório do RLG/OCLC levou ao desenvolvimento do *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment* pela *Task Force on Digital Repository Certification do RLG/NARA*, e, com base neste, o TRAC.

De acordo com *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment* e o TRAC, Cornell[549] apelidou o conjunto das seguintes características ou atributos apresentados pelo relatório do RLG/OCLC (2002) - responsabilidade administrativa, viabilidade organizacional, sustentabilidade financeira e prestação de contas procedimental (certificação) - como Infra-estrutura Organizacional. De acordo com Cornell, "a infrastrutura de uma organização está melhor consagrada nas suas políticas e procedimentos", e documentação da infra-estrutura organizacional está integrada em três níveis distintos: Estrutura de política [*policy framework*], políticas e procedimentos [*policies and procedures*], planos e estratégias [*plans and strategies*] (Cornell, 2004).[550] Os atributos ou características organizacionais são indicadores de planeamento, prontidão, capacidade de lidar com as suas responsabilidades e confiabilidade abrangentes de um repositório digital.[551] A ISO 16363:2012[552], que, como já se relatou anteriormente, teve origem no TRAC, apresenta a mesma configuração. A informação desta norma vai ser referenciada pelo documento homónimo do CCSDS, o *Audit and Certification of Trustworthy Digital Repositories - Magenta Book*[553], do qual emana. Apesar de se fazer uma comparação entre estes dois documentos em capítulo próprio, apresenta-se aqui a sua organização.

Para o *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment,* o TRAC (e a ISO 16363:2012), a Infrastrutura Organizacional inclui elementos como Governança [Governance], Estrutura organizacional [Organizational structure], Mandato ou finalidade [Mandate or purpose], Âmbito [Scope], Funções e responsabilidades [Roles and responsibilities], enquadramento da Política [Policy framework], Sistema de Financiamento [Funding system], Questões financeiras, incluindo activos [Financial issues, including assets], contratos, licenças e passivos [Contracts, licenses, and liabilities], Transparência [Transparency][554]. Verifica-se na ISO 16363:2012 a admissão de que o enquadramento da Política se prende com a Preservação [*Preservation Policy Framework].*[555]

Tanto o *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment* como o *TRAC* organizam as métricas ou critérios da Infrastrutura Organizacional nas seguintes secções:

---

[549] CORNELL UNIVERSITY LIBRARY; ICPSR; MIT LIBRARIES – Attributes of a TDR. In Digital Preservation Management: http://dpworkshop.org/dpm-eng/foundation/tdr/index.html.
[550] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories, p. 8; AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 9.
[551] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 9.
[552] ISO 16363:2012, Space data and information transfer systems - Audit and certification of trustworthy digital. Geneva: ISO.
[553] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book.
[554] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories: draft for public comment, p. 8; AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 9.
[555] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book.

"A1 Governance and organizational viability
A2 Organizational structure and staffing
A3 Procedural accountability and policy framework
A4 Financial sustainability
A5 Contracts, licenses, and liabilities"[556]

Por sua vez, a ISO 16363:2012, apresenta as suas "métricas normativas" ligadas à Infrastrutura Organizacional, com a seguinte organização:

"3.1 Governance and Organizational Viability
3.2 Organizational Structure and Staffing
3.3 Procedural Accountability and Preservation Policy Framework
3.4 Financial Sustainability
3.5 Contracts, Licenses, and Liabilities" [557]

O *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment* aborda as funções, processos e procedimentos do repositório estabelecendo as métricas ou critérios ligados à ingestão e aquisição de material digital, às condições mínimas para preservação de AIPs a longo prazo, às melhores, mais actuais e estratégias de preservação documentadas e implementadas para garantir o acesso a longo prazo, aos requisitos mínimos de metainformação necessária para localização e gestão dos objectos digitais, e à funcionalidade de acesso dos repositórios. Esses critérios são organizados nas seguintes secções:

"B1. Ingest/acquisition of content
B2. Archival storage: management of archived information
B3. Preservation planning, migration, & other strategies
B4. Data management
B5. Access management" [558]

O TRAC inclui nas responsabilidades de gestão de objectos digitais de um repositório alguns aspectos "organizacionais" e técnicos relacionados com essas responsabilidades, nomeadamente a fase inicial da ingestão que aborda aquisição dos conteúdos digitais, a fase final da ingestão que coloca os conteúdos digitais adquiridos nos pacotes de informação de arquivo (AIPs), utilizados pelo repositório para a preservação a longo prazo, as estratégias de preservação sólidas, actuais e documentadas, juntamente com mecanismos para as manter actualizadas face à evolução tecnológica, as condições mínimas necessárias que garantam a preservação a longo prazo da AIP, o nível básico de metainformação que permita a localização e gestão dos objectos digitais no sistema, a capacidade do repositório de produzir e disseminar versões exactas e autênticas dos objectos digitais:

[556] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories: draft for public comment, p. 8; AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 9.
[557] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book.
[558] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories: draft for public comment, p. 14-31.

"B1. Ingest: acquisition of content
B2. Ingest: creation of the archivable package
B3. Preservation planning
B4. Archival storage & preservation/maintenance of AIPs
B5. Information management
B6. Access management." [559]

Quanto à ISO 16363:2012, esta adopta o título Preservação de AIP para os atributos que o TRAC define como Armazenamento de Arquivo e a preservação ou manutenção de AIP:

"4.1 Ingest: Acquisition of Content
4.2 Ingest: Creation of the AIP
4.3 Preservation Planning
4.4 AIP Preservation
4.5 Information Management
4.6 Access Management" [560]

O *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment* aborda as questões referentes à Comunidade Designada e à usabilidade da informação, desenvolvendo métricas ou critérios ligados à existência de documentação com vista à prova e transparência, à metainformação que seja significativa para a Comunidade Designada, com vista a que a informação possa ser utilizável pelas partes interessadas, e que essa informação seja compreensível. Esses critérios são abordados nas seguintes secções:

"C1. Documentation
C2. Descriptive metadata appropriate to the Designated Community
C3. Use & usability
C4. Verifying understandability"[561]

De notar que este conjunto de elementos não se encontra reunido em secção própria no TRAC ou na ISO13636:2012, pelo que os critérios que dele fazem parte encontram-se espalhados pelos grupos ligados à Infrastrutura Organizacional e à Gestão de Objectos Digitais desses dois documentos.

Tanto o *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment* como TRAC agrupam os requisitos de tecnologias, de infra-estrutura técnica e de segurança nos critérios para avaliar a adequação da infra-estrutura técnica do repositório e sua capacidade de atender às exigências de gestão de objectos e de segurança do repositório e dos seus objectos digitais, nomeadamente os requisitos gerais de infra-estrutura do sistema, as tecnologias adequadas, com base nos requisitos da infra-estrutura do sistema, com critérios adicionais que especifiquem a utilização de tecnologias e estratégias adequadas à(s) comunidade(s) designada(s) do repositório, de sistemas de segurança, desde servidores,

[559] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 21-41.
[560] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book.
[561] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories: draft for public comment, p. 32-38.

firewalls ou *routers* até sistemas de protecção contra incêndios e detecção de inundações, e ainda sistemas que envolvam acções humanas:

No *An Audit Checklist for the Certification of Trusted Digital Repositories - Draft for Public Comment:*

> " D1. System infrastructure
> D2. Appropriate technologies
> D3. Security" [562]

No TRAC:

> " C1. System infrastructure
> C2. Appropriate technologies
> C3. Security" [563]

Neste grupo, a que a ISO 16363:2012 vai chamar de Gestão de Risco da Infrastrutura e de Segurança [Infrastructure and Security Risk Management], ficam unidas as infrastruturas e as tecnologias no âmbito da gestão de risco da infrastrutura técnica e aborda a Segurança também na perspectiva da Gestão de Risco, demonstração da necessidade de uma cultura de avaliação de risco como forma de garantir o funcionamento e serviço de confiança:

> " 5.1 Technical Infrastructure Risk Management
> 5.2 Security Risk Management" [564]

De acordo com Yakel, a ISO 16363:2012 apresenta um conjunto de funções ligados à selecção, processamento de dados, preservação, a adoptar pelos repositórios com a finalidade de serem considerados dignos de confiança.[565]

Segundo a autora, esta norma defende que as comunidades designadas têm um papel activo na verificação dos seus critérios e, logo, na construção de confiança. A título de exemplo, a secção 3.3.2 afirma que a política de preservação pode incluir informação acerca do nível de compreensibilidade esperado pela Comunidade Designada do repositório para cada AIP. De igual forma, a secção 4.2.5.2. remete para uma reacção por parte da Comunidade Designada.[566]

Yakel verifica ainda que, apesar da ISO 16363:2012 não corresponder quanto à forma exacta de cumprir os requisitos de auditoria, esta norma fornece sugestões quanto aos tipos de provas que considera aceitáveis para o cumprimento dos critérios definidos. No entanto, essas sugestões variam entre o muito específico e o muito genérico. Por exemplo, a secção 3.1.3 requer uma política de colecção e avança com a definição de uma política de colecção como

[562] AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories: draft for public comment, p. 39-44.
[563] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 43-49.
[564] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book.
[565] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 145.
[566] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 145.

sendo tanto a acção como a prova pretendida para o cumprimento deste critério. Em contraste, a secção 4.1.1 lista uma variedade de tipos possíveis de provas para demonstrar a identificação das Propriedades da Informação, que vão desde declarações de missão até documentos de política de preservação e fluxos de trabalho. Estes materiais de prova concernem a várias funções do repositório a diferentes níveis (administrativo, operacional, etc.).[567]

A própria norma defende que a comunicação dos resultados da auditoria ao público, o que considera ser um acto de transparência, gera mais confiança, e mais auditorias objectivas, promovendo ainda mais confiança no repositório e no sistema que o suporta.[568] Assim, e para Yakel, a reputação institucional é fundamental, porque ela é construída ao longo do tempo e reflecte o reconhecimento de comportamento específico, acumulado por parte de uma organização das partes interessadas.[569]

Sendo a Certificação pela ISO 16363:2012 um exemplo de autenticação de certificados emitidos por entidades externas, ela reforça a afirmação da importância no reconhecimento do valor em saber se uma organização está certificada de acordo com as normas ou outros controlos que podem ser relevantes para uma auditoria.[570]

Seguindo o raciocínio de Yakel, no ambiente do repositório, as garantias são vistas como declarações, exibidas nos sítios web dos repositório, relativas aos dados preservação e / ou sustentabilidade da organização. No âmbito da ISO 16363:2012, embora a selecção, a metainformação e o processamento de dados, sejam funções de repositório, considera-se que a preservação e a sustentabilidade são mecanismos de garantia estrutural, na medida em que aumentam a sensação de segurança e a formação de redes de segurança.[571]

Em resumo, dois dos factores de confiança directa - a identificação com os interesses das partes interessadas, e a transparência - parecem estar alinhadas com a ISO 16363:2012. Além disso, espera-se que os aspectos de segurança estrutural (certificados emitidos por entidades externas e as garantias derivadas da preservação e sustentabilidade), que dizem respeito à ISO 16363:2012 e ao processo de certificação possam estimular a confiança nos repositórios digitais.[572]

O Catálogo de Critérios Alemão: NESTOR e o Certificado DINI

Como já se referiu, o NESTOR foi desenvolvido com o objectivo de ser catálogo de critérios de fidedignidade e preparar a certificação de repositórios digitais de acordo com procedimentos nacionais e internacionais. No âmbito nacional, os critérios considerados cruciais situam-se no âmbito do quadro jurídico, na existência de recursos financeiros e humanos adequados nos organismos públicos, nas estruturas organizacionais nacionais e no estado de desenvolvimento em matéria de preservação digital a longo prazo a nível nacional. A tradução das várias versões tem como objectivo ser abordado e normalizado também no contexto internacional.

[567] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 145
[568] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book, p. 2-1
[569] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 147
[570] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book, p. 2-2
[571] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 147
[572] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 148

A produção dos critérios do NESTOR baseou-se em princípios como a abstracção, para poderem ser válidos para utilização num maior espectro de repositórios, e a conformidade com a terminologia OAIS, de onde emana a maioria dos termos utilizados no âmbito dos repositórios digitais.[573] Becker chama a atenção para os aspectos ligado ao planeamento a longo prazo, mecanismos ligados à mudança, e ainda a definição das propriedades significativas dos objectos digitais a preservar.[574] Para além destes princípios, Dobratz e Schoger[575] sistematizam outros como é o caso da necessidade de existência de documentação adequada aos objectivos, especificações e implementação dos repositórios; o incentivo à transparência, através da publicação de documentação dirigida às partes interessadas internas ou externas ao repositório, sem pôr em causa a confidencialidade de determinadas informações; a adequação dos critérios aos casos concretos dos repositórios; e a mensurabilidade não apenas no aspecto quantitativo, mas também de qualidade.

No âmbito destes princípios, o catálogo proposto pelo NESTOR estrutura-se em torno de três dimensões:

- O quadro organizacional do repositório;
- A gestão dos objectos; e
- A infraestrutura e segurança tecnológicas.[576]

Para além do NESTOR, foram também desenvolvidos outros projectos no quadro de certificação de repositórios digitais na Alemanha. Como se verificou anteriormente, o grupo de trabalho de *Electronic Publishing* do DINI desenvolveu, a partir de 2002, um processo de certificação no âmbito dos repositórios institucionais, partindo de critérios como a qualidade de serviço, a visibilidade, interoperabilidade e recurso a normas. Esta certificação estabeleceu um conjunto de requisitos mínimos para os repositórios e instituições de que estes fazem parte, abrangendo aspectos como políticas de servidor, questões legais, disponibilidade e sustentabilidade a longo prazo.[577] Este processo de certificação inicia-se com o preenchimento do formulário/questionário de auditoria, cujas respostas eram posteriormente avaliadas por um especialista da informação e um perito em tecnologia, que verificavam se a certificação podia ser concedida. A verificação engloba a análise da documentação institucional e dos serviços, a existência de compromissos assumidos em termos da sua política, missão e definição de objectivos, da manutenção das características dos objectos a preservar, e ainda das questões legais como as permissões de utilização. Adicionalmente verificam a existência de preocupação em apoiar os autores, em investir numa política de indexação, não esquecendo também a disponibilização e acesso a longo prazo. O certificado DINI teve três edições, em 2004, 2007 e 2010.[578] A implementação deste certificado pretende promover o

[573] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 7.
[574] BECKER, Christoph - Trustworthy preservation planning.
[575] DOBRATZ, Susanne; SCHOGER, Astrid - Trustworthy digital long-term repositories: the NESTOR approach in the context of international developments.
[576] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 10-37.
[577] DOBRATZ, Susanne; SCHOLZE, Frank. - DINI institutional repository certification and beyond.
[578] ALEMANHA. DINI Working Group "Electronic Publishing" - DINI-certificatedocument and publication services; BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 7; RECKER, Astrid - The preservation of digital objects in german repositories: three case studies.

aumento da visibilidade, o reconhecimento e importância dos serviços prestados por estes repositórios, e simultaneamente incentivar o acesso livre.[579]

A distinção entre o certificado DINI e projectos como NESTOR ou o TRAC prende-se, na perspectiva de Dobratz, pelo facto destes estarem mais focados no estabelecimento de critérios para a certificação da confiabilidade dos repositórios digitais no contexto da preservação digital a longo prazo, pelo facto de pretender sobretudo especificar requisitos e padrões mínimos a cumprir pelas instituições, ao nível dos documentos e publicações institucionais, estando mais focado na qualidade dos próprios serviços, na sua visibilidade e interoperabilidade.

No entanto, e após a produção da segunda versão do NESTOR, o grupo de trabalho *DIN Working Group "Trusted Archives - Certification"* desenvolveu, em colaboração com o DIN Institute, a norma *DIN 31644 "Information and documentation- Criteria for trustworthy digital archives*" publicada em 2012 [580]*,* que fixou os critérios para o estabelecimento da confiança em arquivos digitais.[581] Tal norma o que permitiu o desenvolvimento *do Nestor Seal for Trustworthy Digital Archives.*[582]

A norma é composta por 34 critérios baseados em quatro princípios: Documentação das actividades do repositório, transparência, adequação às necessidades das partes interessadas, e mensurabilidade dos critérios. Estes critérios dividem-se igualmente em três grupos:

- Organização do Repositório digital;
- Gestão de objectos a preservar;
- Infrastrutura e segurança.[583]

Para a obtenção do *Nestor Seal for Trustworthy Digital Archives,* o repositório deve requerer a avaliação por parte do NESTOR, e cada um das partes nomeará representantes para contactos. O NESTOR define a calendarização do processo, e o repositório começa por fazer a auto-avaliação, utilizando o formulário de verificação e as instruções para cada critério. A aplicação de cada critério deve ser verificada para o caso em questão, podendo excluir-se alguns critérios desde que tal exclusão seja justificada devidamente. Depois de determinar quais os critérios aplicáveis, o repositório deve dar resposta de forma aprofundada e comprovada documentalmente, e é classificada com base numa escala de 4 níveis referente ao grau de cumprimento:

- 0 (ainda não foi accionado);
- 3 (planeado);

[579] DOBRATZ, Susanne; SCHOLZE, Frank. - DINI institutional repository certification and beyond.
[580] ALLIANCE FOR PERMANENT ACCESS TO THE RECORDS OF SCIENCE NETWORK (APARSEN) - Report on peer review of digital repositories, p. 10; KEITEL, Christian - DIN Standard 31644 and NESTOR certification.
[581] KEITEL, Christian - DIN Standard 31644 and NESTOR certification.
[582] HARMSEN, Henk [et al.] - Explanatory notes on the NESTOR seal for trustworthy digital archives; KEITEL, Christian - DIN Standard 31644 and NESTOR certification.
[583] KEITEL, Christian - DIN Standard 31644 and NESTOR certification.

- 6 (planeado em detalhe);
- 10 (implementado).

Após a auto-avaliação, a documentação é entregue ao responsável do NESTOR pelo processo, que verificará se a informação fornecida corresponde aos critérios, se é consistente, e se as soluções oferecidas são apropriadas para as tarefas e objectivos do repositório. Caso não haja questões, este emitirá um relatório, que será verificado pelo segundo revisor do NESTOR, que decidirá a atribuição do Certificado. De seguida o gabinete NESTOR e o repositório são informados, e caso este último não concorde com a decisão, pode apelar ao grupo de trabalho de certificação do NESTOR. O Selo tem validade aquando da publicação do relatório, das respostas e dos documentos no seu sítio web e após o NESTOR o acrescentar ao registo de repositórios certificados. O Selo indica o ano em que foi emitido e formalmente, a sua validade é indefinida, dependendo de futuras revisões e reavaliações.[584]

Os 10 Princípios

Uma das primeiras tentativas de conseguir um compromisso entre várias entidades ligadas à definição de critérios ou requisitos comuns que os repositórios digitais deveriam identificar como objectivos a atingir para serem considerados confiáveis, levou a que em Janeiro de 2007, o *Center for Research Libraries* (CRL) organizasse uma reunião de projectos de desenvolvimento de normas e mecanismos de apoio à auditoria, certificação e acreditação de repositórios. Esta reunião, em que também participaram o *Digital Curation Center* (DCC), o *Digital Preservation Europe* (DPE) e o NESTOR resultou no desenvolvimento de um conjunto comum de critérios a que todos os repositórios de preservação digital, independentemente da sua missão, modelo de negócio e fonte de financiamento, devem seguir[585]:

1. Compromete-se com a manutenção continuada de objectos digitais para a(s) sua(s) comunidade(s) identificada (s);
2. Demonstra aptidão organizacional (financeira, de pessoal, de estrutura, de processos) para cumprir o seu compromisso;
3. Adquire e mantém os direitos contratuais e legais necessários e cumpre com as suas responsabilidades;
4. Tem um quadro de política eficaz e eficiente;
5. Adquire e ingere objectos digitais com base em critérios enunciados que correspondem aos seus compromissos e capacidades;

[584] HARMSEN, Henk [et al.] - Explanatory notes on the NESTOR seal for trustworthy digital archives, p. 3-6.
[585] CENTER FOR RESEARCH LIBRARIES (CRL) - Ten principles; MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment – DRAMBORA, p. 16; BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 53.

6. Mantém / garante a integridade, a autenticidade e a usabilidade dos objectos digitais que detém ao longo do tempo;

7. Cria e mantém metainformação necessária acerca das acções tomadas sobre os objectos digitais durante a preservação, e acerca do contexto dos processos de produção, suporte ao acesso e utilização anteriores à preservação;

8. Cumpre com os requisitos de disseminação exigidos;

9. Tem um programa estratégico de planeamento e acções de preservação;

10. Tem uma infrastrutura técnica adequada para a manutenção e segurança continuadas dos objectos digitais;

Becker nota que apenas um dos dez princípios refere-se directamente ao equipamento puramente técnico, ilustrando que, para os signatários destes dez princípios, a confiança tem de ser alcançada a vários níveis, que se estendem desde questões organizacionais e de planeamento estratégico até aos modelos de informação e aos requisitos de utilização.[586]

Avaliação de Repositórios: *Data Seal of Approval*

Em 2010 o instituto *Data Archiving and Networked Services* (DANS), fundado pelo *Netherlands Academy of Arts and Sciences* (KNAW) *e Netherlands Organization for Scientific Research* (NWO), publicou as orientações que servem de base para obtenção *do Digital Seal of Approval* (DSA) por parte dos repositórios, e que é concedido pelo *Data Seal of Approval Board*.[587]

Este *Data Seal of Approval* pretende fornecer garantias aos produtores e financiadores de que os dados e materiais associados estão armazenados de forma confiável e que permanecerão disponíveis para reutilização e o seu investimento não se perderá. Permite ainda que os consumidores de dados possam avaliar os repositórios onde são mantidos os dados, e apoia os repositórios de dados no armazenamento e distribuição de dados eficientes.[588]

O DSA está assim orientado para a avaliação de repositórios na sua especificidade, e não para a auditoria e certificação de organizações, sendo a avaliação totalmente realizada à distância, sem a necessidade da visita de qualquer auditoria externa.[589] Estas orientações, que foram actualizadas em 2013, contêm 16 requisitos para auto-avaliação e verificação pelos pares escolhidos pelo *Data Seal of Approval Board*, relacionados com a criação, armazenamento e (re)utilização de dados digitais.[590] Tal requere que os candidatos apresentem documentação que comprove publicamente o cumprimento de cada um dos requisitos.[591] Os pares que fazem a verificação são escolhidos pelo *Data Seal of Approval Board*, terão que comentar as

[586] BECKER, Christoph - Trustworthy preservation planning, p. 17-18.
[587] MITCHAM, Jenny; HARMAN, Catherine - ADS and the Data Seal of Approval – case study for the DCC.
[588] DATA SEAL OF APPROVAL BOARD – DSA Website http://datasealofapproval.org/en/information/about/.
[589] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital; SCHUMANN, Natascha - Tried and trusted: experiences with certification processes at the GESIS data archive.
[590] DATA SEAL OF APPROVAL BOARD – DSA guidelines 2014-2015, p. 5.
[591] DATA SEAL OF APPROVAL BOARD – DSA guidelines 2014-2015, p. 6.

respostas, confirmando os documentos apresentados como elemento de prova e o nível de cumprimento ou rejeitá-lo justificando as suas razões. O processo de comentário / resposta continuará até que os pares que fazem a verificação decidam positivamente. Em caso de litígio, o requerente pode interpor recurso ao *Data Seal of Approval Board.*[592]

De acordo com Mithcham e Harman[593], dos 16 requisitos, três referem-se aos produtores de dados, dez à qualidade do próprio repositório de dados, e os restantes três à utilização (e utilizadores) dos dados digitais no arquivo. Cada um dos requisitos deve ser avaliado numa escala de 0 (zero) a 4 (quatro), em que a primeira traduz-se em requisito «não aplicável» e o último significa que "o requisito foi totalmente implementado no âmbito das necessidades do repositório" em apreço.[594]

European Framework for Audit and Certification of Digital Repositories

Uma outra tentativa de compromisso para desenvolvimento de um quadro amplamente aceite de requisitos básicos relevantes para todos os repositórios confiáveis, ocorreu em 2010 com a assinatura de um memorando de entendimento pelos seguintes grupos de trabalho ligados à certificação de repositórios digitais: *CCSDS/ISO Repository Audit and Certification Working Group* (RAC); *Data Seal of Approval Board* (DSA); e *DIN Working Group "Trusted Archives - Certification"* ligados ao NESTOR. Este memorando deu origem ao *European Framework for Audit and Certification of Digital Repositories.*[595]

O quadro pretende apoiar as organizações na obtenção de certificação adequada como repositórios digitais confiável e estabelece três níveis de exigência no âmbito da avaliação:

- Certificação Básica: auto-avaliação com base nos 16 requisitos do *Data Seal of Approval* (DSA);
- Certificação avançada: Certificação Básica e auto-avaliação adicional verificada externamente com base nos requisitos da norma ISO 16363:2012 ou DIN 31644;
- Certificação Formal: Validação da auto-certificação com uma auditoria externa oficial com base na ISO 16363:2012 ou DIN 31644.[596]

A atribuição destes certificados permitirá que os repositórios apresentem um dos três símbolos (a acordar) nas suas páginas web e noutros documentos, para além de quaisquer outras marcas de certificação do DSA, DIN ou ISO.[597]

---

[592] DATA SEAL OF APPROVAL BOARD – DSA guidelines 2014-2015, p. 5.
[593] MITCHAM, Jenny; HARMAN, Catherine - ADS and the Data Seal of Approval – case study for the DCC.
[594] DATA SEAL OF APPROVAL BOARD – DSA guidelines 2014-2015, p. 8.
[595] GIARETTA, David; HARMSEN, Henk; KEITEL, Christian – Memorandum of understanding to create a european framework for audit and certification of digital repositories.
[596] ALLIANCE FOR PERMANENT ACCESS TO THE RECORDS OF SCIENCE NETWORK (APARSEN) - Report on peer review of digital repositories, p. 10.
[597] GIARETTA, David; HARMSEN, Henk; KEITEL, Christian – Memorandum of understanding to create a european framework for audit and certification of digital repositories.

No entanto, nada impede que os repositórios realizem auditorias internas ou até externas, devendo ter procedimentos documentados sobre todas as actividades realizadas em torno do repositório, possuir registos e evidências de todas as actividades realizadas, identificar potenciais riscos e delinear planos de contingência caso esses riscos não possam ser evitados, e finalmente, monitorizar o meio ambiente e definir planos de preservação digital (i.e. ser pró-activo e não reactivo).[598]

Aplicação de Critérios e Certificação

Tanto o TRAC como o NESTOR apresentam um conjunto de aspectos relacionados com a aplicação dos seus critérios no âmbito de uma auditoria e/ou num processo de certificação.

O TRAC aconselha a utilização da lista de verificação para Auditoria e Certificação como uma ferramenta para a avaliação objectiva, seja ela feita internamente ou por um auditor externo e objectivo, e independentemente de saber se é realizada para a recolha e avaliação de informação ou como parte de um processo de certificação. A Auditoria é a base para a comparação das capacidades de um repositório digital confiável face a um conjunto de critérios fundamentais. A certificação é mais um passo que alguns repositórios tomam para o reconhecimento formal e objectivo no plano internacional ou de rede. O resultado de uma auditoria deve ser considerado no contexto em que foi realizada.[599]

Segundo este documento, a aplicação dos critérios deve ter em conta o contexto da instituição, sua missão, prioridades e compromissos assumidos,[600] e deve articular os princípios de aplicação de quaisquer critérios: documentação, como evidência dos objectivos, do projecto, das especificações e da implementação do repositório; a transparência interna e externa para aumentar a fidedignidade; a adequação da auditoria à realidade a avaliar; e mensurabilidade com base em indicadores de confiança.[601]

Ainda de acordo com o TRAC, um processo de certificação deve fornecer ferramentas para permitir o planeamento, a auto-avaliação e auditoria externa. Deve reconhecer normas e boas práticas pertinentes para a comunidade do repositório, e os sectores da gestão de informação e da gestão da segurança.[602] É importante ter uma norma internacional que especifique critérios face aos quais serão avaliados os repositórios, mas os processos de auditoria e certificação serão provavelmente implementado de maneiras diferentes para satisfazer as necessidades ou o contexto legal nacionais.[603]

[598] FERREIRA, Miguel - Certificação de repositórios digitais in Seminário (r)evolução da informação pública : preservar, certificar e acessibilizar.
[599] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 5.
[600] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 6.
[601] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 6-7.
[602] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 7.
[603] AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p. 7.

Para o NESTOR a aplicação dos critérios deve ser documentada, para poder ser avaliada, transparente, para aumentar o nível de confiança, adequada à realidade das tarefas, objectivos do repositório digital, e mensurável, com a referência dos indicadores[604].

Avaliação de Riscos: DRAMBORA

A questão acerca do risco transparece em Portugal pela mão de Saramago (2003) que refere que o repositório digital deve gerir os riscos que ameaçam os recursos digitais, sejam eles derivados de "calamidades naturais" [sic] e sabotagens, da vulnerabilidade dos suportes, ou ainda dos riscos decorrentes das estratégias de preservação.[605]

Nesse âmbito, em 2007, o *Digital Curation Centre* (DCC) e o *Digital Preservation Europe* (DPE) criam a ferramenta *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA). Baseando-se nas listas e catálogos de critérios já existentes[606], permite a identificação das competências, pontos fortes e fracos do sistema, através da análise dos objectivos e tarefas, e também dos riscos, cuja execução é medida em termos de ameaças de ocorrências [impacto negativo] e oportunidades [Risco de não ocorrências][607], e ainda das medidas implementadas para a gestão desses riscos no âmbito de um repositório digital.

O documento DRAMBORA refere que:

> *"(…) Work has continued over the past several years to define attributes of such Trusted (or Trustworthy) Digital Repositories, and the criteria that might be used to audit them. Note that trustworthy here is used in a specialist sense."*[608]

Este documento confirma a importância dada anteriormente, pelo relatório da CPA/RLG de 1996 e pelo documento da RLG/OCLC de 2002, no que diz respeito à certificação de confiança e fiabilidade dos repositórios para preservação a longo prazo, e admite que a maioria dos repositórios não têm as responsabilidades orientadas para o acesso e utilização a longo prazo.

Ross e McHugh (2006) consideram que a pretensão deste documento era evidenciar, com base em demonstrações práticas, a existência de atributos que indicassem e medissem a qualidade dos repositórios, através de um processo de auditoria baseado na análise da documentação organizacional, na observação e no testemunho.[609]

O DRAMBORA assume que a Preservação Digital é um exercício de gestão de risco para converter a incerteza da manutenção da usabilidade dos objectos digitais autênticos em riscos quantificáveis. Tal implica fazer tudo para mitigar os riscos que impedem a sua capacidade de

[604] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 7-8.
[605] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais p. 75.
[606] DALE, Robin; GORE, Emily - Process models and the development of trustworthy digital repositories, p. 17.
[607] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 11-12.
[608] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 10.
[609] ROSS, Seamus; HUGH, Andrew - The role of evidence in establishing trusting repositories.

fornecer acesso à informação digital autêntica, sendo que a medida de sucesso do trabalho de um repositório é a "qualidade" da informação que dissemina aos seus utilizadores.[610]

Sendo o risco algo intrínseco ao que o repositório digital faz, a análise de risco e as técnicas de gestão de risco darão suporte à gestão em geral e também às suas actividades fundamentais de preservação e conservação.[611]

O DRAMBORA, como ferramenta de auditoria, pretende ser um complemento aos esforços de avaliação do repositório do TRAC e do NESTOR, guiar os auditores por uma série de tarefas categorizadas de acordo com as características e actividades da organização. Pretende incentivar os repositório a:

1. Identificar contexto de gestão de risco;
2. Identificar e classificar riscos com implicações mais profundas à continuidade do negócio em cada uma das suas actividades;
3. Verificar possibilidades de ocorrência e potencial impacto;
4. Determinar o sucesso de antecipar, evitar, mitigar e tratar riscos;
5. Definir medidas para responder e gerir riscos;
6. Avaliar as respostas ao risco.[612]

Estas fases implicam sempre a manutenção da documentação de prova (evidencial) para assegurar que as conclusões da avaliação[613] são verificáveis no âmbito de uma estratégia de gestão de risco, com o objectivo de determinar se o repositório fez todos os esforços para evitar e conter os riscos que possam impedir a sua capacidade de receber, preservar e fornecer acesso a informação digital autêntica, e contextualmente compreensível, sintáctica e semanticamente, com o fim último de prevenir perdas, melhorar o desempenho, a qualidade dos serviços e a segurança.[614]

A conclusão da auditoria vai traduzir-se numa compreensão documentada/fundamentada da sua missão, fins, objectivos e actividades e bens intrínsecos a eles. Tal incluirá a produção de um catálogo de riscos pertinentes, categorizados de acordo com o tipo e relação entre eles e que permitirá uma identificação interna dos sucessos e lacunas da organização, para permitir a alocação ou redireccionamento de recursos para responder às situações mais problemáticas. Tudo isto permitirá a preparação do organismo para auditoria externa, seja pelo TRAC, NESTOR ou CCSDS.[615]

De acordo com o DRAMBORA, uma premissa fundamental subjacente nos Dez Princípios, já abordados anteriormente, é que os requisitos de preservação devem ser adaptados às

[610] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 20.
[611] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 21.
[612] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 17.
[613] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 24.
[614] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 18.
[615] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 25.

necessidades e meios da comunidade do repositório, pelo facto de estes não serem todos iguais em termos de finalidades e dimensão.[616] Por outro lado, tem que ser feita uma distinção entre repositórios que são entidades próprias daqueles que fazem parte de uma organização maior, no sentido de definir (ou mesmo delegar) responsabilidades e funções no âmbito da gestão dos riscos.[617] A fim de apoiar estas diferentes situações na prática de auditoria, o *kit* de ferramentas de auto-avaliação definiu 8 classes funcionais de actividades de um repositório digital agrupado em Actividades operacionais [Core] e actividades de suporte [Suporte]: para representar as funções básicas de um repositório digital: aquisição e ingestão, conservação e armazenamento, descrição e gestão de metainformação, acesso e disseminação; e as funções que podem ser encontrados em qualquer organização: organização e gestão, recursos humanos, gestão de finanças, apoio tecnológico e segurança. De acordo com o DRAMBORA, a definição das principais actividades, bens/recursos e a identificação dos riscos relacionados com estes, traz uma maior flexibilidade para os auditores escolherem a área do trabalho do repositório onde detêm responsabilidades.[618]

O DRAMBORA afirma ainda que as categorias ou classes ligadas à Segurança da infrastrutura técnica têm um significado relativamente maior para os repositórios digitais, na medida em que os principais bens/recursos do negócio do repositório - a informação digital que preserva - são fortemente dependentes de uma infrastrutura técnica sólida e segura.[619]

O DRAMBORA permite uma autoconsciência documentada de objectivos, actividades e recursos, verificando se os recursos estão bem investidos e posicionados para o sucesso; uma compreensão documentada dos riscos, o que facilita a gestão e alocação de recursos e conhecimento da gravidade dos riscos; a definição de meios de gestão de risco e sua implementação, através de estratégias apropriadas para prevenção, o tratamento, transferência e tolerância, bem como a mecânica da sua implementação. Este processo, que deve ser repetido com regularidade, fornecerá oportunidades para estabelecer e alcançar metas quantificáveis, facilitando o desenvolvimento contínuo de todos os aspectos da actividade organizacional; e, finalmente, uma base para auditoria externas, para futura acreditação e certificação.

McHugh, Ross e Innocenti (2008) referem que o DRAMBORA pretende uma abordagem do tipo base-topo, no sentido de permitir aos repositórios adaptarem a avaliação interna ao seu contexto específico, ao passo que as propostas do TRAC e do NESTOR partem de abordagens topo-base, com o objectivo de estabelecer consensos quanto aos requisitos a cumprir por um repositório digital que pretenda ser considerado confiável, revelando uma adaptabilidade mais difícil tendo em conta a grande variedade de repositórios existente. Para estes autores, tanto o TRAC como o NESTOR não distinguem claramente a auditoria da certificação – na medida em que a primeira, podendo ser precursora da segunda, tem características distintas –, e também

[616] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 16.
[617] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 16-17.
[618] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 17.
[619] MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment, p. 17.

não definem claramente as responsabilidades que devem ser atribuídas aos elementos envolvidos nestes processos.[620]

Ou seja, e de acordo com o PLATTER (2010), enquanto os grupos de trabalho do TRAC e do NESTOR produziram listas de requisitos com critérios específicos que os repositórios deveriam cumprir e comprovar documentalmente com o fim de obter certificação, a ferramenta DRAMBORA guia os repositórios durante um exercício de avaliação de risco que lhes permite auto-avaliar a sua capacidade para cumprir os seus objectivos. Cada método tem aspectos fortes e fracos. As listas de requisitos são mais concretas e específicas, logo mais apropriadas para o processo de certificação, mas são algo rígidas e pode revelar-se difícil de serem aplicadas à totalidade dos repositórios digitais que pretendem obter o estatuto de fidedignidade. Por seu lado, a ferramenta DRAMBORA é extremamente flexível porque avalia um repositório relativamente aos objectivos autodefinidos, e não a requisitos definidos externamente. No entanto isto significa que a sua fidedignidade está dependente da qualidade desses mesmos objectivos.[621].

Um compromisso adequado seria permitir que os repositórios identificassem os seus próprios objectivos dentro de um quadro amplamente aceite de requisitos básicos relevantes para todos os repositórios confiáveis.[622] Como já se abordou anteriormente, esse compromisso resultou no desenvolvimento de um conjunto de 10 critérios comuns pelo CRL, o DCC, o DPE e o NESTOR[623], e mais recentemente, no *European Framework for Audit and Certification of Digital Repositories.*[624]

No âmbito da ferramenta DRAMBORA, esses princípios determinam uma classificação dos riscos identificados pelo processo de avaliação. Para as listas de requisitos representam um esquema de classificação acordado para os requisitos a serem verificados.[625]

Concepção e Planeamento de Repositórios: o PLATTER

O interesse na incorporação dos Dez Princípios[626] ou requisitos na concepção e planeamento de um repositório que se pretende confiável logo de início deu origem, em 2010, ao *Planning Tool for Trusted Electronic Repositories (*PLATTER). O ciclo de planeamento PLATTER descreve um conjunto semi-formalizado de etapas destinadas a facilitar os processos de definição e apresentação dos objectivos organizacionais, e a implementação e avaliação das medidas

[620] MCHUGH, Andrew [et al.] - Bringing self-assessment home: repository profiling and key lines of enquiry within DRAMBORA.
[621] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 8.
[622] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 9.
[623] CENTER FOR RESEARCH LIBRARIES (CRL) - Ten principles; MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment – DRAMBORA, p. 16; BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 53.
[624] GIARETTA, David; HARMSEN, Henk; KEITEL, Christian – Memorandum of understanding to create a european framework for audit and certification of digital repositories.
[625] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 9.
[626] CENTER FOR RESEARCH LIBRARIES (CRL) - Ten principles; MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment – DRAMBORA, p. 16; BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 53.

destinadas a conhecê-los. O PLATTER foi concebido para apoiar abordagens tanto através de lista de requisitos, como uma auditoria com base na análise de risco.[627]

O processo é cíclico, e as secções individuais correspondem em muitos aspectos, a etapas do processo de análise de risco DRAMBORA. As etapas do PLATTER são:

- Planeamento estratégico;
- Definição de objectivos ou princípios - planeamento operacional;
- Implementar o planeamento;
- Apresentar, rever e reformular implementação.[628]

O processo definido no PLATTER leva à produção de nove Planos Objectivos Estratégicos: o Plano de Negócio, o Plano de Recursos Humanos, o Plano de Dados (especificações de objectos de dados, metainformação, estruturas dos macroprocessos), o Plano de Aquisição (relação com os fornecedores e depositadores), Plano de Acessos, Plano de Preservação, Plano do sistema Tecnológico, Plano de Sucessão, Plano de Emergência.[629]

A ferramenta PLATTER está preocupada exclusivamente com a gestão dos objectivos e metas do repositório. Não é considerada como ferramenta para estabelecer a confiança e não se destina a competir com outras iniciativas nessa área.[630]

Em resumo, pode-se afirmar que, enquanto os catálogos de critérios TRAC e NESTOR estão orientadas para serem uma lista de requisitos para a certificação, as ferramentas PLATTER e DRAMBORA orientam os planeadores do repositório e apoiam-nos com mecanismos de avaliação e melhoria de alto-nível.[631]

O ponto de vista dos utilizadores

Perante esta panóplia de instrumentos, falta perguntar como é que utilizadores, da Comunidade Designada, das partes interessadas, vão adquirindo/ganhando confiança nos repositórios, e ainda se estes consideram que as acções executadas pelos repositórios digitais, no âmbito de auditorias e certificações de fidedignidade, lhes conferem fiabilidade. Autores como Ross e McHugh (2006) [632], Prieto[633] e mais recentemente, Elizabeth Yakel, Ixchel Faniel,

[627] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 44.
[628] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - Repository planning checklist and guidance, p. 17.
[629] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - repository planning checklist and guidance, p. 20.
[630] DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. HATII - repository planning checklist and guidance, p. 44.
[631] BECKER, Christoph - Trustworthy preservation planning, p. 24 .
[632] ROSS, Seamus; HUGH, Andrew - The role of evidence in establishing trusting repositories.
[633] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories.

Adam Kriesberg, Ayoung Yoon[634], referem a necessidade de estudar a [percepção de] confiança dos utilizadores no que se refere aos repositórios digitais.

Como já se teve oportunidade de verificar, para Prieto, os repositórios digitais confiáveis podem ser classificados como'' de confiança'' no âmbito do processo de certificação principalmente porque eles cumprem ou excedem as expectativas e as necessidades das comunidades de utilizadores para os quais foram projectados e pelo reconhecimento das normas e boas práticas relevantes para a sua comunidade.[635]

Este autor conclui assim que é importante, então, a estudar as percepções de confiança das comunidades de utilizadores como factores essenciais para o sucesso dos repositórios digitais. Os mecanismos e protocolos devem ter em conta o papel central que desempenham no sucesso do repositório digital, seja ele criado como repositório institucional, biblioteca digital, arquivo digital, ou qualquer outro modelo. Ao aumentar e fortalecer as percepções de confiança detidas pela comunidade de utilizadores, o conceito e o potencial do repositório digital confiável pode se tornar uma realidade ainda maior.

Yakel, ao abordar a questão da confiança das partes interessadas externas na organização, ao analisar a ISO 16363:2012, afirma que, muito embora esta norma tenha a ver claramente com as acções do repositório, exige, em muitos casos, que a Comunidade Designada reconheça que são acções fidedignas conducentes à criação de confiança (critérios 3.3.2 e 4.2.5.2), e também que confirme que são respeitados princípios subjacentes ao repositório, como a transparência (critérios 3.1.3 e 4.1.1).[636]

Nos factores considerados por esta autora, os quais já foram referidos neste capítulo, ela identifica que, no âmbito do factor da confiança das partes interessadas, a dimensão da identificação é verificada nesta norma no requisito referente à compreensão da Comunidade Designada[637], e a dimensão da transparência se verifica nos requisitos referentes à partilha de resultados de auditoria.[638] Para o segundo factor (garantias de estrutura), ela dá como exemplo da aprovação/certificação dada por terceiros, o *Data Seal of Approval* e a certificação ISO da norma ISO 16363:2012, citando mesmo esta norma quando refere que é importante reconhecer que existe valor em saber se uma instituição é certificada de acordo com as normas ou cumpre com outros controlos que podem ser relevantes para uma auditoria.[639]

Esta autora também sugere que a Identificação, ou compreensão da Comunidade Designada, pode ser considerada uma métrica de verificação para a Comunidade Designada perceber o quão bem o repositório compreende suas necessidades.[640] No entanto refere que o

[634] YAKEL, Elizabeth [et al.] - Trust in digital repositories.
[635] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 593.
[636] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 145.
[637] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 146. Cft. AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist, p.21-22; EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book, p. 3-5 e 3-6.
[638] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 146. Cft. AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist p. 25-26; EUA. CCSDS - Audit and certification of trustworthy digital repositorie: magenta book, p. 2-1; 3-6; 3-9 - 3-10.
[639] EUA. CCSDS - Audit and certification of trustworthy digital repositories: magenta book, p. 2-2.
[640] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 150.

estabelecimento de métricas para o objectivo de compreensão da Comunidade DesignadaC da ISO 16363:2012 pode ser muito complexo e cheia de *nuances*. É importante compreender como as partes interessadas constroem confiança, na medida em que tal pode ajudar a reforçar as iniciativas de repositórios para estabelecer a confiança e é um factor para o repositório atingir a meta de ser considerado confiável.[641]

Ayoung Yoon [642], ao investigar como os utilizadores definem'' confiança'' em relação aos repositórios digitais, e quais os factores que influenciam utilizadores na construção de confiança e / ou mantê-la. A autora defende que a definição de confiança por parte dos utilizadores é em grande medida baseada numa falta de decepção, ou veracidade[643] quando se trata do contexto específico de repositórios de dados.

Em relação aos factores que influenciam o desenvolvimento de confiança nos repositórios por parte dos utilizadores, foram identificados os seguintes: características organizacionais, comunidades de utilizadores (recomendações e uso frequente), experiências passadas, os processos de repositório (documentação, limpeza de dados e verificação de qualidade), e a percepção que os utilizadores têm dos papéis do repositório.[644]

Para a autora, os esforços de identificação de atributos e de desenvolvimento de ferramentas de certificação reconheceram sempre o papel da comunidade de utilizadores e sugeriram formas de os envolver no processo de criação de repositórios digitais fidedignos.[645] No entanto os estudos nesta área são reduzidos.

A autora conclui que se o primeiro passo é perceber a confiança dos utilizadores, o passo seguinte envolve o desenvolvimento de uma métrica para medir a confiança que os utilizadores depositam nos repositórios. A confiança é um conceito complexo de medir, mas a existência de uma medição normalizada da confiança dos utilizadores pode ajudar a demonstrar como é que o repositório ganhou a confiança dos utilizadores e também como são considerados fontes confiáveis de informação. A autora sugere ainda que se deva estudar a confiança dos utilizadores nos dados.[646]

Para concluir o estado da arte em Certificação de Repositórios Digitais

De acordo com Miguel Ferreira[647], o recurso a ferramentas como o TRAC permite identificar pontos fortes, pontos fracos e formas de mitigar riscos e potenciais pontos de falha A publicação dos resultados das auditorias (internas ou externas) e restante documentação,

[641] YAKEL, Elizabeth [et al.] - Trust in digital repositories, p. 154.
[642] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development.
[643] Truthfulness no original; cft truthfulness In Infopédia [Em linha]. Porto: Porto Editora, 2003-2014. [Consult. 2014-05-03]. Disponível na www: <URL: http://www.infopedia.pt/ingles-portugues/truthfulness>.1. Veracidade; 2. Autenticidade; 3. boa fé ;4. exatidão; 5. Fidelidade; 6. Autenticidade
[644] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development, p. 31.
[645] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development, p. 21.
[646] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development, p. 32.
[647] FERREIRA, Miguel - Certificação de repositórios digitais.

confere maior confiabilidade ao repositório aos olhos de terceiros, indo ao encontro do princípio da transparência.

Actualmente não existem entidades certificadoras de repositórios pela ISO 16363:2012, estando somente o DSA e o DINI a dar os primeiros passos como entidades certificadoras com os seus conjuntos de critérios de certificação.

Os instrumentos de suporte à certificação analisados neste capítulo têm motivado o desenvolvimento de várias outras ferramentas, e a adaptação de aplicações informáticas, com o objectivo de auxiliar as organizações no planeamento dos seus repositórios, principalmente no que concerne ao estabelecimento e incremento da confiança entre a comunidade de interesse. São disso exemplo a ferramenta PLATO, que será abordada no âmbito do capítulo 6, ou o projecto DCAPE-*Distributed Custodial Archival Preservation Environments*[648], que não teve posteriores desenvolvimentos.

No caso de Portugal, a comunidade académica tem acompanhado as tendências internacionais no desenvolvimento e implementação de repositórios institucionais. Apesar de não estarem ainda em prática medidas concretas para a realização de auditorias e certificação desses repositórios, há consciência, por parte da comunidade envolvida, da necessidade de estabelecimento de políticas formais de preservação, assegurando as características de autenticidade, integridade, e acessibilidade dos documentos digitais, e simultaneamente desenvolvendo elementos que permitam o incremento da confiabilidade dos repositórios, abrindo o caminho para futuros processos de certificação.[649]

A manutenção da assinatura digital.

Adicionalmente aventa-se aqui a possibilidade da certificação de repositórios digitais permitir uma evolução positiva nas situações ligadas ao risco que acarreta a utilização de documentos de arquivo electrónico com assinatura electrónica como elemento probatório a longo prazo. A assinatura electrónica qualificada constitui um meio de autenticação digital equiparável à autenticação através da assinatura convencional (escrita), mas, ao contrário desta, tem um prazo de validade limitado, de acordo com as especificações e critérios de cada entidade certificadora.[650] Ora estando a leitura da assinatura electrónica dependente de um sistema intermediário, é possível que a evolução tecnológica leve à obsolescência do *software* e *hardware* que interpreta a assinatura, o que retira validade probatória ao documento.[651] Por outro lado os certificados digitais que suportam a assinatura digital[652], e que são emitidos por uma entidade certificadora[653] que garante não só a associação de uma assinatura digital com um determinado individuo como a autenticidade e inviolabilidade da assinatura digital, assumem a manutenção da autenticidade do documento através da inalterabilidade da

[648] HOU, Chien-Yi; WOJCIK, Caryn; MARCIANO, Richard - Trusted digital repository design: a policy-driven approach.
[649] FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital.
[650] DECRETO-LEI 290D/99 de 2 de Agosto; DECRETO-LEI 68/2003 de 3 de Abril; DECRETO-LEI 165/2004 de 6 de Julho; DECRETO-LEI 116-A/2006 de 16 de Junho; DECRETO-LEI 88/2009 de 9 de Abril.
[651] MARTINS, Francisco – Preservação digital: novos desafios na justiça.
[652] DECRETO REGULAMENTAR 25/2004 de 15 de Julho.
[653] DECRETO-LEI 116-A/2006 de 16 de Junho.

informação a nível lógico. Como a obsolescência tecnológica pode tornar o objecto ininterpretável e mesmo inacessível, será necessário aplicar medidas de preservação digital, medidas essas que, não alterando o objecto digital a nível conceptual, produzem alterações a nível lógico, o que constitui uma quebra da garantia fornecida pela assinatura digital.

É da nossa opinião que apenas através da sistematização das medidas de preservação digital em sede de um plano de preservação digital, apoiando-se em repositórios digitais certificados que assegurem a evidência do valor probatório dos documentos, será possível resolver o conflito entre a obsolescência dos certificados das assinaturas digitais e o valor evidencial a longo prazo dos documentos que contêm essas assinaturas digitais. Neste âmbito verifica-se a necessidade de reformular e repensar o conceito de autenticidade e integridade que está na base da legislação sobre a assinatura electrónica, na medida em que, de acordo com Miguel Ferreira:

> *"num contexto digital, a autenticidade não terá tanto que ver com o demonstrar que um objecto é original, mas sim, que está conforme o original."*[654]

A solução proposta requer igualmente legislação que confirme e legitime a existência de um repositório digital certificado com responsabilidades na custódia e emissão de cópias certificadas dos documentos nele ingeridos e geridos. Nesse âmbito a Direcção-Geral de Arquivos, actual Direcção-Geral do Livro, dos Arquivos e das Bibliotecas, apresentou em 2011 uma proposta para Serviços de Arquivo Confiáveis: preservação de informação digital autêntica e autenticada, que implicaria a possibilidade de certificar repositórios de acordo com referenciais normativos internacionais e incluí-los no texto da lei de forma a criar opções efectivas para preservação digital, a possibilidade de credenciar instituições certificadoras, de acordo com normativos internacionais, de forma a terem competências para reconhecer repositórios como certificados, a aceitação de cópias certificadas como documentos com valor probatório idêntico a "originais" desde que custodiados por um repositório certificado, a possibilidade de assinatura digital ser extraída no momento da ingestão do documento no repositório certificado através de um processo totalmente documentado através da criação de metainformação emitida pelo repositório (mantendo o documento "original" com a assinatura digital, embora sem preservação associada), e a regulamentação como solução (adicional) de preservação digital a longo prazo para documentos assinados digitalmente dos TAS – Serviços de Arquivo Confiáveis, de acordo com o indicado pelo grupo de trabalho *European Electronic Signature Standardization Initiative (EESSI)* [655]

[654] FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico, p. 37.
[655] NILSSON, Hans [et al.] - Final report of the EESSI expert team.

6 - Repositório de Objectos Digitais Autênticos (RODA)

O Repositório de Objectos Digitais Autênticos tem origem no projecto homónimo, e do qual fizemos parte, desenvolvido entre 2006-2008, pelo Instituto de Arquivos Nacionais/Torre do Tombo (IAN/TT), depois elevado a Direcção-Geral de Arquivos (DGARQ), que foi fundido mais recentemente na Direcção-Geral do Livro, Arquivos e Biblioteca (DGLAB). A missão desta instituição inclui responsabilidade pela identificação e preservação de documentação de valor histórico como meio de garantir e fomentar a memória individual e colectiva nacional e assegurar o valor evidencial da documentação produzida pela Administração Pública. Tal documentação inclui informação digital produzida no âmbito das iniciativas do Governo Electrónico para agilizar e assegurar um serviço mais rápido, completo e transparente para os cidadãos. Por esse motivo o IAN/TT considerava necessário desenvolver processos, ferramentas e recursos capazes de dar resposta às necessidades de preservação dessa informação digital, num processo sustentado e pró-activo que permitisse dar resposta às solicitações governamentais e comunitárias no sentido do governo electrónico. Os financiadores originais do RODA foram o POAP (Programa Operacional da Administração Pública), um instrumento financeiro nacional, financiado pela União Europeia (75%), e a Direcção-Geral de Arquivos (25%). O POAP visava a inovação organizacional, a simplificação dos procedimentos administrativos, melhorando a qualidade dos serviços públicos e formação de pessoal na administração central.

O Projecto

O projecto RODA, que contou com a colaboração informática da Universidade do Minho, tinha como finalidade desenvolver e promover uma solução tecnológica, ultimada na construção de um protótipo de repositório digital que desse origem a ideias e a um conhecimento mais concreto de como construir um repositório de preservação digital real[656] capaz de incorporar, descrever e dar acesso a todo o tipo de informação digital produzida no contexto da Administração Pública.[657] Foram planeadas três macro-fases, a saber Análise e Planeamento, Prototipagem e, Teste e Disseminação, cada uma composta por várias tarefas.[658]

O projecto considerou como objectivos primários o desenvolvimento e a definição de: requisitos funcionais para um arquivo digital, clientes e aplicações a integrar; modelos conceptuais, lógicos e de dados de um arquivo digital; Identificação e selecção de esquemas de metainformação para as diferentes camadas de metainformação; Requisitos técnicos e organizacionais; protótipo dum arquivo digital para preservar objectos digitais susceptíveis de conservação definitiva; elaboração de uma ferramenta, enquanto módulo da anterior, capaz de se "acoplar" com sistemas de gestão documental existentes na AP e assegurar funções de preservação digital numa perspectiva de gestão administrativa.

Foram também identificados objectivos secundários, como a definição de uma política de arquivo para os objectos digitais produzidos pela Administração Pública nacional (avaliação e

[656] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade, p. 5.
[657] BARBEDO Francisco [et al.] – RODA: Repositório de Objectos Digitais Autênticos.
[658] FARIA, Luis e CASTRO, Luis – RODA Repositório de Objectos Digitais Autênticos – relatório final,p. 5.

selecção); a definição de uma política de preservação para o arquivo digital; a criação ou identificação de modelos de financiamento viáveis para suportar o Arquivo Digital; a definição de uma taxionomia de propriedades significativas para cada uma das classes de objectos consideradas.

O protótipo foi planeado tendo por base as funcionalidades indicadas no modelo de referência OAIS, e em conformidade com a METS (*Metadata Encoding & Transmition Standard*), a EAD (*Encoded Archival Description*), a PREMIS (*PREservation Metadata: Implementation Strategies*), e as recomendações do *InterPares.*[659]

Posteriormente à produção do protótipo foi desenvolvido um sistema de repositório, de acordo com os princípios e requisitos refinados na fase anterior.

Foram consideradas três classes de objectos digitais: documentos de texto estruturado, imagens estáticas bidimensionais e bases de dados relacionais (MS SQL Server, MS Access, PostgreSQL, MySQL e ODBC genérico), para os quais foram definidos formatos de preservação, respectivamente o PDF/A-1[660], o TIFF[661] e o DBML.[662] O estudo das taxonomias também permitiu verificar que a preservação de bases de dados implica a separação lógica e física dos dados relativamente ao sistema que os gere, pelo que é necessário metainformação acerca dos formulários e relatórios existentes no sistema que continha os dados da base de dados.

Metainformação no RODA

A metainformação escolhida no âmbito do projecto dizia respeito às camadas de metainformação descritiva, que cumpre o propósito de os materiais estarem bem organizados e facilmente localizáveis, estando assim ligada à função de acesso, a metainformação técnica, para detectar eventuais falhas no processo de preservação e auxiliar a tomada de decisão quanto à estratégia de preservação a implementar, metainformação estrutural, ligada ao processamento e interpretação do objecto de forma coerente e correcta, e metainformação de preservação, referente à garantia de autenticidade. Os esquemas de metainformação identificam-se com o EAD versão de 2002[663], para a metainformação descritiva, o PREMIS 1.0 (*PREservation Metadata: Implementation Strategies*)[664] para a metainformação de preservação, o Esquema NISO Z39.86[665] para a metainformação técnica para caracterizar imagens digitais, e o esquema METS (*Metadata Encoding & Transmition Standard*)[666] e ainda o esquema RDF (*Resource Description Framework*)[667] para a metainformação estrutural.

---

[659] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade, p. 5 e p. 7.
[660] ISO 19005-1:2005, Document management – Electronic document file format for long-term preservation: Part 1: Use of PDF 1.4 (PDF/A-1).
[661] ADOBE - TIFF developer information site.
[662] HENRIQUES, Marta [et al.] - Bidirectional conversion between XML documents and relational data bases.
[663] Encoded Archival Description.
[664] CAPLAN, Priscilla [et al.] - Data dictionary for preservation metadata: final report of the PREMIS working group.
[665] ANSI/NISO Z39.87-2006, Data Dictionary - Technical metadata for digital still images.
[666] METS - Metadata Encoding and Transmission Standard.
[667] RDF - Resource Description Framework.

Assim, o RODA considera como esquemas de metainformação primários o EAD e o PREMIS. O EAD permite descrever as Entidades Intelectuais, isto é, as representações, e as relações hierárquicas, sustentadas nos respectivos planos de classificação, sendo o nível mais baixo de descrição permitido o documento composto ou documento simples. Por sua vez o PREMIS, guarda metainformação relativa à preservação digital, descrevendo representações, agregado de ficheiros necessários para renderizar a entidade intelectual, e ainda os ficheiros que constituem essa entidade Intelectual, e que são o verdadeiro alvo dos processos de preservação. O PREMIS inclui ainda dados acerca dos Eventos, que registam as acções que ocorrem sobre os objectos e o resultado dessas mesmas acções, mas também sobre os Agentes responsáveis pela execução das acções que produzem os referidos Eventos. Mas uma vez que o PREMIS é um esquema generalista que não guarda metainformação técnica específica acerca de qualquer tipo de ficheiro, é necessário utilizar um esquema de metainformação técnico específico para cada tipo de ficheiros alvo de preservação, o que no caso das imagens digitais estáticas é o esquema NISO Z39.87. De igual forma, é usado ainda outro tipo de metainformação estrutural para objectos digitais constituídos por vários ficheiros que devem estar organizados por uma determinada ordem e/ou agrupamento. Neste caso, o esquema METS guarda a informação sobre a ordem das imagens (páginas) e também sobre a divisão em subgrupos (organização interna) dos ficheiros de uma representação, tendo a função de ponto de acesso a esta representação, permitindo a navegação pelos vários ficheiros da representação de uma forma ordenada. Este esquema transparece como um envelope que acompanha pacotes de submissão de informação (SIP). O RDF é utilizado para criação de relações entre objectos de descrição, preservação e representações.

Baseando-se no projecto INTERPARES, definiu-se a migração como estratégia fundamental de preservação, utilizando conversores para migrar os formatos em perigo de obsolescência. Tal assume que a autenticidade dos objectos digitais não se possa basear na sua originalidade, mas na sua fidelidade relativamente ao original. Tal implica que a garantia de fidelidade requeira a avaliação dos objectos digitais aquando de cada migração, devendo estas migrações ser bem documentadas, nomeadamente no que diz respeito a perdas, por forma a manter a sua autenticidade. O registo das tarefas ligadas à preservação fica guardado no RODA, seguindo o esquema PREMIS.[668]

Plataforma de Desenvolvimento

A selecção da plataforma de desenvolvimento levou a uma análise de projectos de arquitecturas de repositórios que fossem *open-source*, destacando-se o DSpace e o Fedora. Estes candidatos foram avaliados e comparados tendo por base os requisitos funcionais do RODA. Estes requisitos estão divididos em três tipos distintos, ligados aos macroprocessos identificados no Modelo de Referência OAIS - Ingestão, Gestão, Disseminação – e cada um deles indicava um componente do RODA que comprovaria a cumprimento do requisito. A avaliação e comparação verificaram que o DSpace implementa mais requisitos do que o Fedora, o que levou a pensar que seria o mais apropriado. No entanto, verificou-se que o DSpace apresentava uma estrutura de dados interna demasiado específica que dificultava a

[668] FARIA, Luis e CASTRO, Luis – RODA Repositório de Objectos Digitais Autênticos – relatório final, p. 20-21.

possibilidade de o adequar às necessidades do RODA, como a inclusão dos esquemas de metainformação escolhidos. Tal rigidez, oposta à flexibilidade do Fedora, derivada da ausência de ferramentas ou serviços, levou a que a equipa do RODA opta-se pela segunda opção. A escolha do Fedora obrigou a um maior trabalho de implementação das funcionalidades a adicionar, quando em comparação com uma solução menos genérica.

Assim, o RODA está organizado em várias entidades funcionais de acordo com o modelo de referência OAIS, e a sua arquitectura interna baseia-se na arquitectura do *FEDORA Commons*, uma plataforma de código-aberto que disponibiliza um conjunto de serviços básicos que permitem o desenvolvimento de repositórios digitais altamente parametrizáveis. Os serviços disponibilizados pelo *Fedora Commons* são responsáveis por tarefas elementares ao nível das entidades funcionais de Gestão de Dados e de Armazenamento de arquivo, e incluem a capacidade de ingerir, aceder e eliminar objectos digitais, bem como estabelecer relações entre estes através de mecanismos ontológicos baseados em RDF. O Fedora inclui um motor de pesquisa capaz de indexar o conteúdo dos vários objectos armazenados permitindo assim a sua posterior localização e recuperação. O RODA guarda um registo de todas as acções desenvolvidas em torno do repositório. Essa informação é armazenada numa base de dados e em ficheiros armazenados no sistema de ficheiros. Toda esta camada de componentes é apelidada de Serviços de Dados RODA (*RODA Data Services*).

Sobre os serviços anteriormente descritos foram desenvolvidos métodos remotos mais complexos que implementam a lógica de negócio do repositório, como *o RODA Core Services*. O *RODA Core Services* é responsável pela execução de tarefas como lidar com o fluxo do processo de ingestão, formas avançadas de consulta ao repositório e execução de funções administrativas no repositório. Estes métodos encontram-se acessíveis através de vários Web services organizados de acordo com o modelo de referência OAIS. Isso permite integração de sistemas já existentes na organização, que poderão depositar ou consultar informação disponível no repositório. Além disso, esta API permite a criação de novas ferramentas de ingestão que criam e depositam SIPs de forma automática no RODA.

A interface com o utilizador é assegurada pelo componente *RODA Web User Interface* (RODA WUI). Este componente faz uso dos serviços disponibilizados pelo RODA Core e apresenta uma interface gráfica que permite aos produtores, consumidores, arquivistas, e administradores de sistema interagir com o repositório. Os subcomponentes que constituem RODA WUI são baseados no *Google Web Toolkit*.

O mecanismo de autenticação implementado pelo RODA assenta no recurso a um servidor LDAP (*Lightweight Directory Access Protocol*).

Paralelamente ao *RODA Core Services* existe um conjunto de serviços de migração e serviços relacionados com as acções de preservação e manutenção, como a normalização de formatos, verificação de integridade, despiste de vírus, tarefas administrativas, activação de alertas, cálculo de estatísticas, etc. As ferramentas de preservação digital permitem a validação e caracterização dos objectos digitais, comparação entre objectos originais e os derivados da sua conversão, processos de migração para vários formatos, que incluem a identificação do formato e outras propriedades do objecto digital.

A Gestão da Preservação dentro do RODA é gerida por uma agenda de tarefas em que um utilizador especial, ou seja, o especialista de preservação, pode definir o conjunto de regras que desencadeiam acções de preservação específicas. As acções de preservação respeitam uma API comum, por isso a criação e instalação de novas acções no repositório é tão simples como copiar o ficheiro de programa para pasta correta no servidor. Estas acções podem invocar serviços remotos, mas devem ser implementados localmente por uma questão de conformidade com os requisitos. Estas acções devem lidar com todos os pedidos de serviços remotos e lidar com todas as possíveis excepções que possam ocorrer.

A agenda de tarefas permite que o perito de preservação configure as regras que irão seleccionar objectos relevantes para uma intervenção de preservação, bem como o agendamento da própria intervenção.

Uma das características do RODA como sistema distribuído é a possibilidade de ser implantado de diferentes maneiras, desde correr todos os componentes num servidor, até correr cada componente num sistema diferente. A implantação do RODA em diversos sistemas aumenta o seu desempenho e segurança.

Pacotes de Informação

Assim, o FEDORA considera a unidade de informação como o objecto, pelo que toda a informação, incluindo a metainformação, terá que fazer parte de um ou mais objectos. Um objecto está estruturado em 4 partes: o PID, ou identificador único e persistente; a Descrição, necessária para a gestão interna dos objectos, e que inclui as propriedades do Objecto e a metainformação acerca das suas Relações; Itens, o conjunto de metainformação contido no objecto e Serviços, as funcionalidades associadas ao objecto, nomeadamente o serviço de disseminação, que disponibiliza o acesso às propriedades e aos objectos.[669]

Com base nesta estrutura, cada SIP que o RODA ingere é composto por uma ou mais representações, um registo de metainformação descritiva por cada representação[670] e restante metainformação de preservação e técnica (se existente). Todos esses ficheiros são acompanhados de um envelope METS para lhes dar ordem e estrutura. Todos esses ficheiros são comprimidos num ficheiro ZIP, que constitui o SIP.[671]

Antes do SIP ser incorporado no RODA, passa por uma série de teste depois de ser descomprimido, e que incluem o despiste de vírus, validação sintáctica e estrutural, verificação de completude do SIP e integridade dos ficheiros, validação da metainformação descritiva e de preservação, verificação de existência das representações, verificação de permissões do produtor, normalização dos formatos.

---

[669] FARIA, Luis e CASTRO, Luis – RODA Repositório de Objectos Digitais Autênticos – relatório final, p. 32-34.

[670] Uma vez que o esquema EAD é utilizado para descrever uma colecção inteira de representações, verifica-se que cada registro EAD não descreve somente uma representação. Assim a equipa do RODA optou por um subconjunto do esquema EAD, o EAD-C, suficiente para descrever uma representação, ou seja, um elemento <c> e todos os seus sub-elementos.

[671] FERREIRA, Miguel - RODA: descrição do sistema, p34; FARIA, Luis [et al.] - RODA : a service-oriented repository to preserve authentic digital objects, p. 3-4.

Após ser validado, o SIP é então desmontado e cada um dos seus componentes é integrado no repositório. Findo este procedimento, o SIP torna-se um AIP e está pronto para ser disseminado para potenciais consumidores que têm autorização para aceder a essa informação.

O consumidor tem a possibilidade de pesquisar as colecções disponíveis para visualizar ou descarregar as representações digitais custodiadas no repositório. Com esse fim, são utilizados diferentes módulos aplicacionais para visualização ou disseminação, tendo em conta o tipo do objecto digital.

Modelo de Dados

O modelo de Dados do RODA distingue três tipos de objectos: Objectos de Descrição (OD), Objectos de Representação (OR) e Objectos de Preservação (OP).

O AIP é ilustrativo do modelo de dados do RODA, verificando-se ser atomístico e baseado no modelo definido pelo PREMIS. Com efeito, cada Entidade Intelectual é descrita por um registo de metainformação EAD-C, designado por objecto de descrição. Estes objectos de descrição relacionam-se hierarquicamente entre si de forma a constituir uma descrição completa de um Fundo de arquivo, mas são mantidos separadamente dentro do modelo de conteúdo *Fedora Commons*. Estas relações são criadas usando o mecanismo de ligação RDF fornecido pelo Fedora.

Adicionalmente, cada objecto de descrição do tipo documento ou documento composto possui relações com um ou mais objectos de representação. Um objecto de representação é um objecto Fedora que incorpora todos os ficheiros e sequências binárias que constituem uma representação digital.

Finalmente, cada um destes objectos encontra-se relacionado com um terceiro tipo de objectos designados por objectos de preservação. Estes têm como objectivo documentar a proveniência da representação digital e o historial de eventos de preservação que ocorreram no interior do repositório. Os objectos de preservação podem ser de quatro tipos distintos: objecto, evento, evento com relacionamento, e agente.

Os objectos de preservação do tipo objecto registam a estrutura da representação e informação técnica sobre os ficheiros que as constituem. Os objectos do tipo agente descrevem qualquer pessoa, organização ou aplicação de *software* que tenha sido responsável pela realização de um evento. Por sua vez, um evento agrega toda a informação relativa a uma acção de preservação (e.g. verificação de integridade, migração, etc.), bem como o resultado da mesma (e.g. sucesso, insucesso, etc.).

Os objectos do tipo evento com relacionamento são utilizados para documentar eventos que originam as novas representações. Exemplos disto são os eventos de migração. Trata-se de eventos que são aplicados a uma representação e cujo resultado é uma nova representação derivada da primeira.

Verifica-se assim que o RODA implementa totalmente o macroprocesso de Ingestão que não só valida SIPs, mas também cuida de todo o processo de negociação entre o arquivo e os produtores da informação. O RODA também é responsável pelo Acesso, fornecendo diferentes formas de pesquisa e navegação sobre a metainformação disponível, bem como visualização / transferência de objectos digitais armazenados. Também foram desenvolvidos componentes de Administração que permitem que os arquivistas alterem a metainformação descritiva e definam regras para as intervenções de preservação, como agendamento de verificação de integridade de todos os objectos digitais armazenados, iniciar o processo de migração de determinadas classes/ formatos de representação, ou controlar quais utilizadores ou grupos estão autorizados a realizar certas acções dentro do repositório.[672]

Planeamento de Preservação: o CRiB

Embora o RODA cubra a maior parte dos componentes funcionais descritas no modelo de referência OAIS, ainda faltava um componente muito importante, o Planeamento de Preservação.[673]

Assim a equipa do RODA tomou proveito do projecto CRiB (*Conversion and Recommendation of Digital Object Formats*), desenvolvido na Universidade do Minho com a intenção de ajudar organizações no planeamento e execução de operações de preservação baseada na migração.[674] Trata-se de uma Arquitectura Orientada ao Serviço (SOA) suportada por *Web Service*s que permite aos actuais repositórios realizar migrações de formatos, determinar a quantidade de informação perdida numa migração, documentar a intervenção de preservação e obter sugestões de alternativas de migração adequadas ao problema de preservação em causa.[675] O Planeamento da Preservação é suportado por um serviço de recomendação que toma decisões informadas sobre as melhores opções de migração disponíveis e toma em consideração as necessidades individuais de cada instituição cliente. O componente de execução de preservação é tratado por um grande conjunto de serviços de migração que pode ser constituído para gerar fluxos de migração mais complexos.[676] Apresentamos resumidamente os seus componentes constituintes:

- O *Identifier Format*, que é um serviço capaz de identificar a codificação subjacente a uma representação digital, garantindo que as aplicações clientes responsáveis pela preservação de objectos digitais sejam capazes de identificar, caracterizar e validar a integridade dos seus objectos sem intervenção humana. Além disso, permite que as descrições de formato sejam uniformizadas em todos os componentes do CRiB de acordo com o vocabulário controlado

[672] RAMALHO, José Carlos [et al.] - RODA and CRiB a service-oriented digital repositor; BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade, p. 7.
[673] RAMALHO, José Carlos [et al.] - RODA and CRiB a service-oriented digital repositor.
[674] FERREIRA, Miguel; BAPTISTA, Ana Alice; RAMALHO, José Carlos - A foundation for automatic digital preservation.
[675] FERREIRA, Miguel, BAPTISTA, Ana Alice, RAMALHO, José Carlos - CRIB : a service oriented architecture for digital preservation outsourcing.
[676] RAMALHO, José Carlos [et al.] - RODA and CRiB a service-oriented digital repositor.

definido pelo registro de formatos PRONOM desenvolvido pelos Arquivos Nacionais do Reino Unido;[677]

O *Obsolescence Notifier* é responsável pela monitorização do nível de (falta de) utilização dos formatos reconhecidos. Quando um determinado formato está em risco de se tornar obsoleto (por exemplo, quando é publicada uma nova versão de um formato), este componente fará accionar os eventos de preservação adequados.

O Service Registry gere a metainformação de suporte à descoberta de serviços, baseada na norma UDDI (*Universal Description, Discovery and Integration*), informando o CRiB dos serviços de migração disponíveis e prontos a serem utilizados.

O *Migration Broker* está responsável pela invocação de serviços de migração e pela medição da performance de cada um desses serviços em termos de disponibilidade, estabilidade, escalabilidade, débito e custo.

O *Object Evaluator* verifica a quantidade de informação perdida na migração, tendo por base múltiplos critérios de avaliação e propriedades significativas, como por exemplo, o conteúdo textual, dimensões da página, número de páginas, *layout* gráfico, tamanho da fonte, etc. Este componente emite de relatórios para o cliente, baseados no *PREMIS Data Dictionary* (*Event Entity*), indicando a data e hora da intervenção, descrição dos agentes envolvidos, tipo de evento (e.g. migração) e o resultado da intervenção.

O *Format Evaluator* informa o sistema sobre o estado dos formatos digitais ao nível de cota de mercado, nível de suporte, existência de especificação aberta, etc., para o *Migration Advisor* decidir quais os formatos mais adequados para a preservação a longo prazo. Utiliza como fontes de informação bases de dados com factos sobre formatos e outras fontes dinâmicas de informação como o *PRONOM Registry* ou o *Google Trends*.

O *Migration Advisor* é o responsável pelo planeamento da preservação. Para tal gera sugestões de alternativas de migração, combina os requisitos de cada organização cliente (como a importância atribuída a cada propriedade significativa) com o conhecimento que acumula sobre a qualidade de cada conversor usado para migração, em termos de desempenho, perda de informação associada e estado de cada formato.

O CRiB apresenta-se como uma plataforma de avaliação, recomendação e selecção de alternativas de migração, que presta serviços de conversão/migração e avaliação dos resultados dessa conversões/migrações. Adicionalmente, produz relatórios para anexação à metainformação de preservação, que servem como documentação da intervenção e garantem a autenticidade. Permite a redução de custos, sugerindo alternativas de migração e efectuando a avaliação automática das intervenções de preservação. Permite ser extensível através da utilização de novos serviços de conversão e avaliação, e fornece serviços que vão desde a publicação e venda de serviços de conversão/migração até *benchmarking* de conversores/migradores. Em suma, o CRiB oferece um grande conjunto de serviços de preservação que podem ser utilizados por qualquer instituição, aplicação ou utilizador individual cliente, com o fim de manter as suas colecções de objectos digitais em codificações

[677] REINO UNIDO. National Archives – PRONOM: The technical registry.

interpretáveis e actuais garantindo que o risco de perda das características representacionais importantes é mínimo.

Presentemente: Desafios e Oportunidades

Terminado o financiamento do POAP, o projecto foi adaptado para se tornar um verdadeiro projecto *open source*, do qual fazemos parte no âmbito do Conselho de Disseminação Formação, no sentido de oferecer aos utilizadores uma solução fácil de instalar e de testar (máquina virtual), listas de discussão e documentação de suporte, modalidades de apoio gratuito ou pago. Para os desenvolvedores, fornece orientações sobre o desenvolvimento e tradução, construção fácil, disponibilidade no *GitHub*, listas de discussão de apoio, muita documentação e um sítio web da comunidade.[678]

Actualmente o RODA apresenta-se em conformidade com o OAIS e a TRAC e com normas abertas (EAD, PREMIS, METS, NISO Z39.87, etc,). Este repositório permite a preservação a longo prazo da legibilidade e acessibilidade de forma independente de qualquer *software* ou *hardware* específico, garantindo a Fidedignidade e autenticidade dos registos digitais na migração através de gerações sucessivas de tecnologias de informação. A sua arquitectura é escalável, na medida em que o sistema de *plug-in* e agendamento permite acrescentar e alterar funcionalidades ao sistema. Tal permite acomodar uma crescente ingestão de informação, incorporar e preservar informação digital específica, nomeadamente áudio e vídeo digital (cujos formatos de preservação definidos foram WAV[679] e MPEG2[680], respectivamente), informação herdada de sistemas obsoletos, bases de dados de grande porte, e com flexibilidade para gerir diversos formatos de ficheiros e acomodar a complexidade de registos criados por várias aplicações e para lidar com a evolução contínua da tecnologia. Outras características incluem a capacidade de assegurar que os utilizadores podem aceder à informação digital que estão autorizados a ver e que a informação de acesso restrito só se encontra disponível para os utilizadores com direitos e privilégios de acesso adequados, a capacidade de se integrar com sistemas externos, e a de permitir a ingestão de informação digital de quatro formas diferentes: em linha, fora de linha, por FTP e integração com *software* de gestão documental de terceiros.[681]

Os actuais problemas aos quais a equipa e a comunidade do RODA estão sensíveis, prendem-se com as questões de escalabilidade, derivada da quantidade de informação que cresce exponencialmente; da monitorização do mundo, no sentido de sistematizar e automatizar a aquisição de informação para detectar obsolescência; da sistematização do planeamento, ligada à responsabilização e a provar no futuro que foram tomadas as melhores decisões possíveis; da automatização dos processos, tendo em conta o número, heterogeneidade e complexidade dos objectos tornam todas as tarefas morosas e o suporte reduzido[682].

[678] RODA Community.
[679] EUA. Library of Congress - WAVE Audio File Format.
[680] EUA. Library of Congress - MPEG-2 Encoding Family.
[681] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade, p. 7-8.
[682] FARIA, Luís - Desafios práticos à preservação digital: RODA e SCAPE.

O Projecto SCAPE

Com vista a encontrar soluções para estas questões, o RODA foi integrado no projecto SCAPE, projecto europeu do 7º programa-quadro, que começou em 2011 e termina em 2014. No âmbito deste projecto pretende-se, no que se refere ao RODA, desenvolver infrastrutura e ferramentas escaláveis, criar uma *framework* para *workflows* de preservação e integrar com um sistema de planeamento e monitorização.[683]

Tal permitirá que no futuro sejam possíveis processos de Ingestão por colecções, permitindo assim a optimização de tarefas para executar numa plataforma escalável, a integração com ferramentas de planeamento de preservação em que a Ingestão accionará o planeamento e levará à execução automática do plano de preservação; também permitirá a monitorização contínua, em que a Ingestão será uma fonte de informação do Macroprocesso de Vigilância[684], e monitorizar os eventos que podem desencadear mudanças no planeamento.[685]

O SCAPE Preservation Environment

O *SCAPE* definiu uma arquitectura para a gestão de armazenamento e de gestão de dados, e o planeamento, monitorização e operações (ou acções) de preservação, chamada *SCAPE Preservation Environment* (SPE). Esta arquitectura permite a preservação da informação digital a longo prazo através da monitorização contínua de elementos internos e externos que influem na preservação e definir as melhores acções a tomar para a preservação dos objectos digitais custodiados.[686]

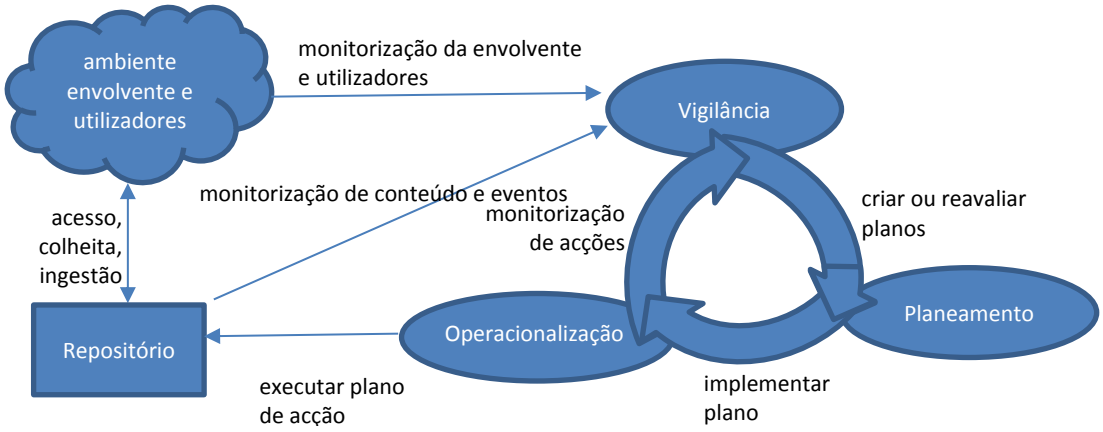

Figura 9 - Ciclo de Vida da Preservação Digital (SCAPE)

Nesta lógica, e baseando-se num ciclo de vida da preservação apresentado na figura 9, o repositório (o RODA), relaciona-se com o ambiente envolvente e os seus utilizadores através das funcionalidades de acesso, colheita [harvest], e ingestão de informação. Neste âmbito verificam-se dois tipos de monitorização que vão alimentar o Macroprocesso de Vigilância, e que são a monitorização da envolvente e utilizadores e a monitorização de conteúdo e eventos no repositório. Este dados recolhidos pelo Macroprocesso de Vigilância permitem criar ou

[683] FARIA, Luís - Desafios práticos à preservação digital: RODA e SCAPE.
[684] Macroprocesso de Vigilância - *Watch* no original.
[685] FARIA, Luis - Ingest with RODA : the present and the future of repository ingest.
[686] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 2.

reavaliar os planos existentes no Macroprocesso de Planeamento[687], planos esses que são implementados no Macroprocesso de Operacionalização[688], que executará o plano de acção. No meio destes três macroprocessos influem as Políticas.

Com base neste ciclo de vida, o *SCAPE Preservation Environment* apresenta um conjunto de serviços para a monitorização do conteúdo, nomeadamente a ferramenta de *software C3PO* (*Clever, Crafty, Content Profiling of Objects*), que usa metainformação extraída a partir de ficheiros de um acervo digital, agregando-os e analisando-os para gerar perfis de conteúdo[689], ou seja, uma visão agregada das características de conteúdo, necessário para apoiar o Macroprocesso de Vigilância. Além disso, a ferramenta analisa o conteúdo e permite a selecção de conteúdos (*datasets*) representativos, que são necessários para o Macroprocesso de Planeamento.[690]

No âmbito do Macroprocesso de Vigilância apresenta o *SCOUT*, um sistema de observação de preservação digital que fornece uma base de conhecimento ontológica para centralizar todas as informações necessárias para detectar riscos e oportunidades de preservação[691] e notifica sempre que algum evento significativo no mundo lhe puder trazer danos ou oportunidades. As fontes de informação do *SCOUT* incluem os registos de Formatos e catálogos de *software*, repositórios digitais e arquivos web, objectivos e políticas organizacionais, experiências, simulações e o conhecimento humano adquirido.[692] Ao ser notificado sobre os riscos e oportunidades, o responsável pelo planeamento da preservação define um plano de preservação para os resolver, e envia-o para o repositório para ser executado. O progresso da execução do plano é monitorizado pelo *SCOUT.*[693]

Para o Macroprocesso de Planeamento, é utilizado o *PLATO 4*, uma ferramenta para o planeamento de preservação de forma sistemática. Ele permite a definição de objectivos de preservação, critérios e restrições necessárias para a tomada de decisão e ajuda na avaliação de todas as alternativas de acção, alcançando a melhor solução bem definida, documentando todo o raciocínio por trás das decisões, e proporcionando a rastreabilidade, uma das bases para manter a autenticidade de recursos digitais[694] que permite produzir os planos de preservação fidedignos.[695] O *PLATO* define os requisitos de planeamento com base na informação do Macroprocesso de Vigilância, nos perfis de conteúdo, políticas, riscos e oportunidades, informação da envolvente, e avalia alternativas, baseando-se nos dados acerca de acções alternativas e amostras representativas de conteúdo. Após esta fase, faz a avaliação

[687] Macroprocesso de Planeamento – *Planning* no original.
[688] Macroprocesso de Operacionalização – *Operations* no original.
[689] KULMUKHAMETOV, Artur; PETROV, Petar - C3PO Clever, Crafty Content Profiling of Objects; PETROV, Petar; BECKER, Christoph - Large-scale content profiling for preservation analysis.
[690] FARIA, Luis - Supporting the preservation lifecycle in repositories.
[691] FARIA, Luis - Supporting the preservation lifecycle in repositories.
[692] FARIA, Luis [et al.] - Automatic preservation watch using information extraction on the Web : a case study on semantic extraction of natural language for digital preservation.
[693] KRAXNER, Michael [et al.] - The SCAPE planning and watch suite: supporting the preservation lifecycle in repositories.
[694] FARIA, Luis - Supporting the preservation lifecycle in repositories.
[695] KRAXNER, Michael [et al.] - The SCAPE planning and watch suite: supporting the preservation lifecycle in repositories.

dos resultados e produz o plano de preservação.[696] O plano de preservação documenta todas as evidências que levam à adopção da estratégia escolhida para preservar o conteúdo, incluindo um fluxo de trabalho que pode ser executado pelo repositório numa plataforma escolhida.[697]

O resultado do planeamento de preservação é um plano de acção que, além de documentar o processo em si, define as acções necessárias a executar no conteúdo. Caso as acções a executar nos conteúdos levantem preocupações de viabilidade devido ao volume de conteúdo ou a intensidade de acção de computação, será necessário ter em consideração as plataformas escaláveis. A plataforma *SCAPE*[698] fornece orientações sobre como implementar essa plataforma para apoiar a execução de acções de preservação em larga escala.[699]

No que respeita ao Macroprocesso de Operacionalização, responsável pela alteração dos conteúdos do repositório de acordo com os planos de preservação resultantes da actividade do Macroprocesso de Planeamento[700], ele é suportado por um sistema de gestão de *workflow* bastante utilizado na área científica da biologia, o *Taverna*. Este sistema permite a execução de *workflows* complexos que reúnem componentes de preservação, como é o caso das ferramentas de descrição/caracterização, migração e garantia de qualidade. A pesquisa feita no âmbito do SCAPE permitiu verificar como executar *workflows* complexos em larga escala[701], sendo que a escolha como implementação de referência recaiu no *Taverna* por ser mais fácil de reproduzir do que os sistemas complexos necessários para execução em larga escala.[702]

A figura seguinte esquematiza como funcionam os componentes entre si.

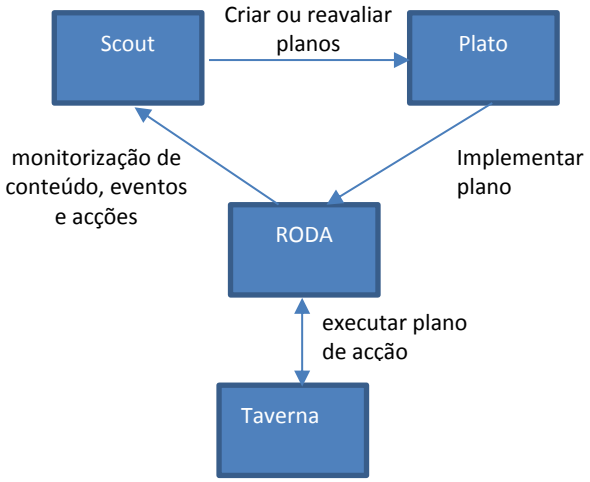

Figura 10 - Implementação de referência do SCAPE Preservation Environment

[696] BECKER, Christoph; KULOVITS, Hannes; RAUBER, Andreas - Trustworthy preservation planning with Plato.
[697] FARIA, Luis - Supporting the preservation lifecycle in repositories.
[698] SCHMIDT, Rainer - An architectural overview of the SCAPE preservation platform.
[699] FARIA, Luis - Supporting the preservation lifecycle in repositories.
[700] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 2.
[701] SCHMIDT, Rainer - An architectural overview of the SCAPE preservation platform.
[702] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 5.

Para além destes componentes funcionais, o SCAPE produziu um conjunto de documentos, que considera parte do *SCAPE Preservation Environment*, nomeadamente as Políticas, sejam estas passíveis de ser compreendidas por humanos ou políticas de controlo para as máquinas, e que servem de suporte às actividades automatizadas de monitorização; orientações para Boas Práticas no âmbito da migração de repositórios de longo prazo em larga escala, da preservação de dados de investigação científica e da preservação ao nível do *bit*, e que são relevantes no contexto da ISO 16363:2012, do *Data Seal of Approval* e do NESTOR; Relatórios SCAPE que abordam aprofundadamente cada um dos componentes funcionais do *SCAPE Preservation Environment*, e que podem ajudar as organizações no processo de implementação do sistema.[703]

[703] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 5.

7 - Comparação e aplicação de Documentos Certificação

O Quadro Comparativo

O quadro comparativo, que se apresenta no fim deste trabalho e que se encontra dividido em três anexos, inspirou-se conceptualmente no esboço de mapeamento de comparação entre o TRAC, o NESTOR, DRAMBORA, ISO27001 e as orientações da OCDE para a segurança dos sistemas de informação elaborado por Katia Thomaz.[704] No entanto, tendo em conta o aviso no âmbito do projecto SHAMAN, de que tal trabalho continha algumas imprecisões[705], e ainda o facto de tal avaliação não incluir a ISO 16363:2012 e última versão do NESTOR, o quadro comparativo foi elaborado de raíz. Assim sendo, esta comparação é uma proposta, sujeita a crítica e aperfeiçoamentos posteriores, mas que pretende trazer economias, e um trabalho de auditoria mais eficiente, e talvez partir para um documento com recomendações e requisitos para auditoria e certificação de repositórios digitais que integre os melhores aspectos dos documentos alvo de comparação.

Comparação dos requisitos/ critérios TRAC, ISO, NESTOR

O TRAC é uma lista de requisitos para auditoria, orientada para a auditoria interna e externa. Pode ser usado para o estabelecimento de metas, planeamento, construção de políticas, e avaliação. Foca-se nos repositórios de preservação.

A ISO 16363:2012, ao contrário do TRAC, permite às organizações obterem uma certificação de confiança dos seus repositórios a nível internacional. Com o estabelecimento desta nova norma, os arquivos passam a ter objectivos mensuráveis para alcançar a confiança dos seus repositórios e os utilizadores possuem uma forma para determinar se um arquivo em particular corresponde às suas necessidades.

O NESTOR é um catálogo com referências e notas, desenvolvido a partir de uma perspectiva e prioridades e motivos específicos derivados do contexto alemão em termos de restrições legais, o funcionamento das instituições públicas (em termos de recursos financeiros e humanos), as decisões organizacionais a nível nacional. Pode ser usado para o planeamento, construção/montagem e avaliação. O NESTOR 1 e 2 são semelhantes em termos de cobertura e nível de detalhe. Não fornecem detalhes de implementação. Com base em Hofstede, pode-se supor que a maior necessidade de controlo de incerteza e redução de ambiguidade por parte da Alemanha[706], a estatuição de regras como fonte de autoridade impessoal[707] e a uniformização de procedimentos como mecanismo de coordenação das actividades da

[704] Katia Thomaz A draft TRAC-DRAMBORA mapping RLG/NARA TRAC with NESTOR CCTDR, DCC/DPE DRAMBORA, ISO27001 and OECD guidelines.
[705] INNOCENTI, Perla [et al.] - SHAMAN requirements analysis report (public version) and specification of the SHAMAN assessment framework and protocol, p. 61, nota de rodapé 19.
[706] HOFSTEDE, Geert – Culturas e organizações, p. 139.
[707] HOFSTEDE, Geert – Culturas e organizações, p. 173-174.

organização[708] será a explicação para a necessidade da Alemanha produzir um documento diferente dos produzidos internacionalmente.

Um elemento a ressalvar é a existência do requisito de gestão de qualidade, ao nível do Enquadramento Organizacional, nas duas versões do NESTOR (ponto 5), que não aparece explicitado nos outros documentos. Curiosamente, a primeira versão deste documento incluía neste ponto o requisito de que o repositório teria que reagir a alterações substanciais, que no entanto passa para o ponto 4 (como 4.5), que se refere adequação organizacional ao repositório digital. Outra diferença entre as versões do NESTOR é a explicitação dos aspectos que integram o âmbito da Gestão de Objectos, na primeira versão[709] (integridade, autenticidade, disponibilização, confidencialidade e metainformação destes elementos). A sustentabilidade destes aspectos, em conjunto com a rastreabilidade e capacidade de referenciação dos objectos e ainda a facilidade de interpretação a longo prazo, requer um acompanhamento para além do que é normalmente entendido por segurança de TI.

O TRAC, a ISO 16363:2012 e o NESTOR

Comparativamente ao TRAC, a ISO 16363:2012 apresenta, em alguns aspectos, uma maior granularidade, fazendo com que alguns requisitos TRAC tenham dado origem a mais critérios.

A nível de topo apresentam ambos a mesma subdivisão em 3 secções, e dentro das duas primeiras secções, as subsecções são também idênticas. Tal só não acontece na última secção, porque a ISO 16363:2012 integra agora o conceito de gestão de risco (*5 Infrastructure And Security Risk Management*) e reúne numa só subsecção (*5.1 Technical Infrastructure Risk Management)* os critérios que o TRAC apresentava em duas subsecções (*C1. System Infrastructure* e *C.2 Appropriate technologies*).

O TDR/ISO 16363:2012 sugere 109 indicadores enquanto o TRAC fornece apenas 84. Esta discrepância reflecte sobretudo um maior foco, por parte do TDR/ISO 16363:2012, em consolidar os termos adoptados, ao nível da preservação digital, de modo a corresponder aos critérios de uma norma ISO. Assim sendo, alguns indicadores foram englobados dentro de outros ou expandidos (ex.: o indicador TRAC A. 2 é expandido no TDR/ISO 16363:2012 em mais dois indicadores: 3.1.2.1 e 3.1.2.2.); suprimidos (ex.: o indicador TRAC A 4.2) e acrescentados (ex.. o TDR/ISO 16363:2012 acrescenta o indicador 4.3.4)

O NESTOR, por sua vez apresenta a mesma divisão em três secções, mas não utiliza subsecções. Considerámos, para efeitos de análise e de comparação, que os critérios resumem o conjunto de requisitos que agrupam, excepto os critérios 8 e 14 que, não tendo nível inferior, correspondem eles próprio a um requisito. Assim, a título de exemplo, consideramos que o critério 1 resume ou engloba os requisitos 1.1 e 1.2. Desta forma, quando se abordar os critérios, estaremos igualmente a abordar os requisitos que dele fazem parte. Daí que no caso da comparação e da avaliação ela tenha sido feita acima de tudo tendo em conta os requisitos.

[708] HOFSTEDE, Geert – Culturas e organizações, p. 168, 178 e seg.
[709] DOBRATZ, Susanne [et al.] – NESTOR catalogue of criteria for trusted digital repositories, p. 15.

Comparação entre critérios/métricas TRAC e ISO 16363:2012

Na nossa perspectiva, dos 85 requisitos do TRAC, somente 7 não são claramente transportados para a ISO 16363. Comparativamente, a ISO 16363:2012 não transporta do TRAC requisitos específicos sobre a existência de políticas e procedimentos de solicitação e utilização do feedback de produtores e utilizadores (critério A3.5), sobre a revisão e ajustamento anuais do plano de negócio (critério A4.2), sobre a preservação de quaisquer identificadores únicos associados aos objectos digitais antes da ingestão (critério B2.6), sobre a aplicação de estratégias de preservação documentadas (critério B4.1), sobre a implementação de políticas de acesso documentadas que incluem o registo de todas as acções 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 objectos armazenados (critérios B6.2 e B6.4). No que se refere a estes três últimos requisitos, que dizem respeito à aplicação e implementação, a ISO 16363:2012 apenas solicita a existência do plano de estratégia documental preservação digital e a existência de estratégias documentadas (critérios 3.1.2 e 4.3.1) e o cumprimento das políticas de acesso, que, em conjunto com os procedimentos, devem permitir a disseminação de objectos digitais rastreáveis aos originais com provas da sua autenticidade (4.6.1 e 4.6.2), requerendo apenas o registo de falhas e anomalias no acesso e erros nos dados ou respostas aos utilizadores (4.6.1.1 e 4.6.2.1).

Por seu lado, a ISO 16363:2012 apresenta requisitos que não são explicitados no TRAC. Dois desses referentes ao governo e viabilidade organizacional (subsecção 3.1), prendem-se 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 ao 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). Ainda na secção da infrastrutura organizacional, a norma ISO 16363:2012 requer, no que se refere à responsabilidade e responsabilização procedimental e enquadramento da política de preservação (subsecção 3.3), a existência de políticas de preservação que estejam em consonâncias com o cumprimento do Plano de Estratégia de Preservação (3.3.2).

O maior número de requisitos originais da ISO 16363:2012 surge na secção de Gestão de Objectos Digitais (secção 4), muito por virtude da existência de muitos subrequisitos. Assim, quanto à aquisição de conteúdo no âmbito da Ingestão (subsecção 4.1), é requerido 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).

Para efeitos de criação dos AIPs no âmbito da ingestão (subsecção 4.2) a ISO 16363:2012 requer adicionalmente 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), se bem que este último depende de um subrequisito (critério 4.2.3.1) que tem equivalência num requisito mais abrangente do TRAC (critério B2.4). Acerca dos identificadores únicos dos AIPs, é requerido pela ISO 16363, no que respeita a regras para a sua geração, a existência de documentação sobre os processos ligados à alteração, e 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 objecto digital independentemente da sua localização física (4.2.4.2). Quanto aos recursos para garantir a qualidade da autoridade da informação de representação dos objectos digitais, surgem dúvidas quanto à equivalência entre o requisito do TRAC sobre o registo da Informação de Representação ingerida (incluindo formatos) (critério B2.8) e o seu desdobramento nos requisitos da ISO 16363:2012, quanto a ferramentas ou métodos para identificar o tipo de ficheiro de todos os objectos de dados ingeridos e definir qual a informação de Representação necessária para tornar os objectos de dados compreensíveis para a Comunidade Designada (critérios 4.2.5.1 e 4.2.5.2). Ainda no âmbito da qualidade da autoridade da Informação de Representação, a ISO 16363:2012 requer a garantia de acesso à informação de representação necessária e de que ela está persistentemente associada aos objectos de dados relevantes (critérios 4.2.5.3 e 4.2.5.4). No que respeita ao planeamento de preservação (secção 4.3), a ISO 16363:2012 solicita 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). A preservação dos AIPs (subsecção 4.4) fornece algumas dúvidas quanto à equivalência entre o requisito referente às especificações de como os AIPs devem ser armazenados até ao nível dos bits (4.4.1), e o requisito de implementação de estratégias de armazenamento e migração dos AIPs (B4.2), embora o requisito da ISO 16363:2012 se justifique pela necessidade de garantir que a informação contida nos AIPs possa ser extraída a longo prazo. O registo de acções e procedimentos administrativos relevantes para o armazenamento e preservação dos AIPs requer, segundo a ISO 16363:2012 a existência de procedimentos (documentados) para todas as acções tomadas sobre os AIPs, e demonstração de que tais acções estão de acordo com as especificações definidas para essas acções (4.4.2.1 e 4.4.2.2). No âmbito da gestão de acesso (subsecção 4.6), existem dúvidas entre a equivalência do critério referente à necessidade de conformidade com as políticas de acesso (4.6.1) com o critério referente à necessidade de documentar e comunicar à(s) sua(s) comunidade(s) designadas que opções de acesso e de entrega existem (B6.1), apesar não restarem dúvidas quanto à equivalência com o requisito que diz respeito à necessidade do sistema de gestão de acesso implementar totalmente a política de acesso (B6.5).

Para a gestão de risco a nível de infrastruturas e segurança (secção 5), a ISO 16363:2012 obriga à identificação e documentação dos processos críticos que afectam a capacidade de cumprir com as suas responsabilidades obrigatórias no âmbito da gestão dos riscos das operações e objectivos de preservação associados à infra-estrutura do sistema do repositório (5.1.1.6), mas apresenta-nos dúvidas quanto à equivalência total, entre os requisitos da ISO 16363:2012 relativos a procedimentos, compromisso e financiamento para substituir *hardware* e *software*

quando a avaliação indica a necessidade de o fazer (5.1.1.1.4 e 5.1.1.1.8) com os requisitos do TRAC referentes à existência de tecnologias de *hardware* e *software* adequados aos serviços que presta às suas comunidades designadas e de procedimentos para receber notificações e monitorizar e avaliar quando são necessárias mudanças de tecnologia de *hardware* (C2.1 e C2.2), porque a ISO 16363:2012 solicita adicionalmente compromissos e financiamento para pôr em prática a substituição, enquanto o TRAC somente aborda a verificação e avaliação da sua necessidade (ou não.). Na nossa perspectiva, dos 109 requisitos da ISO 16363, somente 18 não são identificados claramente no TRAC.

Comparação entre critérios/métricas TRAC e NESTOR

Comparando o TRAC com o NESTOR, não encontrámos correspondência directa de 44 requisitos do TRAC no NESTOR. A título de exemplo, e no que se refere à estrutura da organização e recursos humanos (subsecção A2), o TRAC requer a existência de programas de desenvolvimento profissional que fornece aos funcionários as habilitações e competências necessárias (A2.3), enquanto o NESTOR só indica a necessidade de recursos humanos com qualificações necessárias (4.2). No âmbito da responsabilidade e responsabilização procedimental e enquadramento da política de preservação (subsecção A3), o TRAC especifica a necessidade da existência de procedimentos e políticas em vigor, e os mecanismos para a sua revisão e actualização, 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). Ainda nesta linha o TRAC 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 auto-avaliação e certificação periódica (critérios A3.6, A3.7, A3.8, A3.9). O NESTOR por comparação, somente requer a definição das finalidades do repositório, o cumprimento da legislação e regras contratualizados e procedimentos ligados à gestão de qualidade (critérios integrados nos grupos 1, 3, 4 e 5 do NESTOR). Na mesma secção, a questão da sustentabilidade financeira (A4), são requerido 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, A4.4, A4.5). O NESTOR requer apenas financiamento assegurado (4.1). No âmbito dos contratos, licenças e passivos (A5), o TRAC requer 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). Em contraposição, o NESTOR somente requer a existência de contratos entre o repositório digital e os produtores, devendo o repositório agir de acordo com o contratualizado e com a legislação em termos de tarefas de arquivo e de utilização (3.1 a 3.3). Surgem-nos dúvidas referentes ao facto do requisito do TRAC para conseguir identificar e administrar quaisquer restrições à utilização de conteúdo do repositório (A5.4), tenha equivalência no critério do NESTOR referente à aquisição de metainformação que registe os direitos e condições de utilização (12.6).

Em termos de Gestão de Objectos Digitais, todas as subsecções do TRAC têm requisitos que não têm equivalência específica com o NESTOR. Assim, relativamente à aquisição de conteúdo no âmbito da Ingestão (subsecção B1), o TRAC requer 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 acções e processos relevantes para a preservação (B1.6, B1.7 e B1.8). O NESTOR só refere a garantia da integridade e autenticidade e aceitação dos objectos digitais de acordo com critérios definidos (6, 7 e 9). Numa perspectiva mais alargada poderíamos englobar todos os requisitos desta subsecção no requisito do NESTOR relativo ao desenvolvimento de critérios para a selecção dos objectos digitais (1.1). No que se refere à criação de AIPs no âmbito da ingestão (subsecção B2) o TRAC apresenta requisitos de 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 exactidão 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). O NESTOR somente requer a garantia de integridade, autenticidade dos objectos digitais, e a definição dos AIPs, do seu processo de criação, de armazenamento, legibilidade, e implementação de estratégias que garantam a sua preservação (6, 7, 10), e a identificação única e permanente dos objectos e as suas relações (12.1). No âmbito do Planeamento da Preservação (secção B3), o TRAC requer 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. (critério B3.2 e B3.4). O NESTOR somente solicita metainformação técnica e a existência de um plano de preservação (12.5 e 8). No que respeita ao Armazenamento de arquivo e à manutenção dos AIPs (subsecção B4) o TRAC requer a utilização de estratégias de preservação documentadas e o registo de todas acções ligadas ao armazenamento de arquivo que sejam relevantes para a preservação (B4.1 e B4.5). O NESTOR somente requer um plano estratégico para as medidas de preservação (8) e não especifica registos para as acções de armazenamento. Para a gestão da Informação (subsecção B5), o TRAC solicita a definição de requisitos mínimos de metainformação que permitam à Comunidade Designada recuperar e identificar os recursos que pretendam (B5.1), enquanto o NESTOR apenas requer o registo de metainformação adequada (12.2, 12.3, 12.4, 12.5, 12.6). Ainda nesta secção, os requisitos do TRAC para a gestão de Acesso (subsecção B6) abordam a necessidade de documentar e informar a Comunidade Designada acerca das opções de acesso disponíveis, de registo de todas acções 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 acessos e que os recursos humanos verifiquem episódios de "negação de acesso" incorrectos, 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). O NESTOR somente requer a definição de critérios para a utilização dos objectos digitais e o acesso adequado aos objectos digitais por parte da Comunidade Designada (11 e 2).

Em termos de tecnologias, infra-estrutura técnica e segurança (secção C) o TRAC requer, em termos de infrastrutura do sistema (subsecção C1), a garantia de funcionamento em sistemas operativos e *software*s infrastruturais bem suportados, suporte esse 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). Assim o repositório tem que gerir o número e localização de cópias de todos os objectos digitais, garantindo a sincronização dessas cópias, tem que reportar todos os casos de corrupção ou perda de dados, e as medidas tomadas de correcção/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 apenas requer a adequação da infrastrutura tecnológica às necessidades de gestão dos objectos e de segurança, com o fim de proteger o repositório e objectos digitais (13.1, 13.2 e 14), não abordando questões ligadas ao suporte da infrastrutura, de gestão de cópias, medidas para corrupção ou perda de dados, ou mesmo mudança de tecnologia. Quanto às questões da segurança (subsecção C3), o TRAC requer 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 desastres, que incluam no mínimo, cópias fora do sistema (C3.3 e C3.4). O NESTOR apenas aborda a implementação de requisitos de segurança no âmbito do sistema de segurança e a protecção do repositório e dos objectos digitais (13.2 e 14).

Em relação ao NESTOR, alguns critérios parecem estar englobados em todos os requisitos de uma subsecção do TRAC. É o caso da definição de critérios para a selecção de objectos digitais (1.1) que parece incluir todos requisitos da gestão de conteúdo no âmbito da ingestão (B1), da garantia de acesso da Comunidade Designada aos objectos digitais (2.1) e a definição dos DIPs e a garantia da transformação dos AIPs em DIPs (11.1 e 11.2), que integram a generalidade dos requisitos de gestão de acesso (B6), a documentação de todos os seus elementos de acordo com um processo definido (5.2), e os requisitos ligados à implementação dos necessidades de gestão dos objectos por parte da infrastrutura (13.1), ligados à infrastrutura do sistema (C1), a definição dos DIPs e a garantia da transformação dos AIPs em DIPs (11.1 e 11.2). Desta feita, somente a necessidade de um plano estratégico para as medidas de preservação (critério 8) parece não ter equivalência no TRAC, que somente requer estratégias de preservação documentadas (B3.1 e B4.1) e mecanismos de alteração de planos de preservação tendo em contas as acções de monitorização (B3.3).

Comparação entre critérios/métricas NESTOR e ISO 16363:2012

A comparação entre a ISO 16363:2012 e o NESTOR permitiu verificar a existência de 50 em 109 requisitos do ISO 16363:2012 que não aparecem claramente no NESTOR. Quanto à infrastrutura organizacional (secção 3), surgem logo dúvidas que concernem a governança e viabilidade organizacional (subsecção 3.1). Tais dúvidas dizem respeito à equivalência entre os requisitos de relativos à existência de um Plano Estratégico de Preservação que defina a abordagem do repositório para desenvolver a sua missão a longo prazo (3.1.2) e o requisito do NESTOR relativo ao planeamento a longo prazo (4.4), mesmo que, na nossa perspectiva, não haja dúvidas quanto à relação com outro requisito do NESTOR de existência de um plano estratégico para a preservação técnica no repositório (8). Outra equivalência que traz dúvidas é a relativa ao requisito referente à existência de uma política de colecção que estipule o tipo de informação que irá preservar, manter, gerir e fornecer acesso (3.1.3), em relação ao

requisito do NESTOR referente ao desenvolvimento de critérios de selecção dos objectos digitais. No que se refere à estrutura organizacional e recursos humanos (subsecção 3.2), a ISO 16363:2012 requer a existência de programas de desenvolvimento profissional que forneçam aos funcionários as habilitações e competências necessárias (3.2.1.3), enquanto o NESTOR só indica a necessidade de recursos humanos com qualificações necessárias (4.2). No âmbito da responsabilidade e responsabilização procedimental e enquadramento da política de preservação (subsecção 3.3), a ISO 16363:2012 especifica a necessidade da existência de políticas de preservação, de procedimentos e políticas em vigor, e os mecanismos para a sua revisão e actualização 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 auto-avaliação e certificação periódica (critérios 3.3.3, 3.3.4, 3.3.5, 3.36). O NESTOR por comparação, somente requer a definição das finalidades do repositório, o cumprimento da legislação e regras contratualizados e procedimentos ligados à gestão de qualidade e a existência de um plano estratégico para medidas de preservação técnica (critérios integrados nos grupos 1, 3, 4, 5 e 8 do NESTOR). Na mesma secção, a questão da sustentabilidade financeira (subsecção 3.4), são requeridos 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). O NESTOR requer apenas financiamento assegurado (4.1). No âmbito dos contratos, licenças e passivos (subsecção A5), a ISO 16363:2012 requer 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). Em contraposição, o NESTOR somente requer a existência de contratos entre o repositório digital e os produtores, devendo o repositório agir de acordo com o contratualizado e com a legislação em termos de tarefas de arquivo e de utilização (3.1 a 3.3). Surgem-nos dúvidas referentes ao facto do requisito da ISO 16363:2012 para conseguir identificar e administrar quaisquer restrições à utilização de conteúdo do repositório (3.5.2), tenha equivalência no critério do NESTOR referente à aquisição de metainformação que registe os direitos e condições de utilização (12.6).

Em termos de Gestão de Objectos Digitais, todas as subsecções da ISO 16363:2012 têm requisitos que não têm equivalência específica com o NESTOR. Assim, relativamente à aquisição de conteúdo no âmbito da Ingestão (subsecção 4.1), a ISO 16363:2012 requer especificamente 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 registros das acções e processos de administração relevantes para a aquisição de conteúdo (4.1.3, 4.1.7, 4.1.8). O NESTOR somente aborda a necessidade de aceitar objectos digitais com

base em critérios predefinidos e de identificar as características dos objectos digitais que são significativos para a preservação da informação (9 e 9.2) e ainda de registo de metainformação referente aos objectos digitais (12.2, 12.3, 12.5, 12.6). No que se refere à criação de AIPs no âmbito da ingestão (subsecção 4.2), a ISO 16363:2012 requer 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 actuais 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 objecto 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 objectos digitais, por forma a determinar a informação de Representação necessária para tornar os dados do objecto compreensíveis por parte da Comunidade Designada, garantir o acesso à informação de representação necessária, e que esta esteja persistentemente associada aos objectos de dados (4.2.5, 4.2.5.2, 4.2.5.3, 4.2.5.4). A ISO 16363:2012 considera necessário ainda para a criação de AIPs no âmbito da ingestão, a verificação da integralidade e exactidão dos AIPs aquando da sua criação, e o histórico das acções e processos administrativos relevantes para a criação dos AIPs. (4.2.8 e 4.2.10). O NESTOR somente requer a garantia de integridade e autenticidade dos objectos digitais, e a definição dos AIPs, do seu processo de criação, de armazenamento, legibilidade, e implementação de estratégias que garantam a sua preservação (6, 7, 10), e a identificação única e permanente dos objectos e as suas relações (12.1).

No âmbito do Planeamento da Preservação (secção 4.3), a ISO 16363:2012 requer 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). O NESTOR somente solicita metainformação técnica e a existência de um plano de preservação (12.5 e 8) e a garantia que a Comunidade Designada consegue interpretar os objectos digitais (2.2). No que respeita a preservação dos AIPs (subsecção 4.4) a ISO 16363:2012 requer a preservação da informação de conteúdo dos AIPs, o registo de todas acções e processos administrativos que sejam relevantes para o armazenamento e preservação dos AIPs, sendo que deve especificar os procedimentos referentes a essas acções, e comprovativos de que tais acções vão ao encontro dessas especificações (4.4.1.1, 4.4.2, 4.4.2.1 e 4.4.2.2). O NESTOR somente requer um plano estratégico para as medidas de preservação (8) e não especifica registos para as acções de armazenamento, excepto alterações feitas nos objectos digitais pelo repositório (12.4). Para a gestão da Informação (subsecção 4.5), a ISO 16363:2012 solicita a definição de requisitos mínimos de metainformação que permitam à Comunidade Designada recuperar e identificar os recursos que pretendam (4.5.1), enquanto o NESTOR apenas requer o registo de

metainformação adequada (12.2, 12.3, 12.4, 12.5, 12.6). Ainda nesta secção, os requisitos da ISO 16363:2012 para a gestão de Acesso (subsecção B6) 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). O NESTOR somente requer a definição de critérios para a utilização dos objectos digitais e o acesso adequado aos objectos digitais por parte da Comunidade Designada (11 e 2). Numa 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 objectos 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). Em termos de gestão de riscos de infra-estrutura e segurança (secção 5), a ISO 16363:2012 requer, em termos de gestão de risco da infrastrutura técnica (subsecção 5.1), a identificação e gestão dos riscos decorrentes das operações e metas de preservação associadas à infra-estrutura 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 correcção/substituição, processos para registrar e agir, com base numa avaliação do risco-benefício, à disponibilidade de novas actualizações 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 objectos 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). O NESTOR apenas requer a adequação da infrastrutura tecnológica às necessidades de gestão dos objectos e de segurança, com o fim de proteger o repositório e objectos digitais (13.1, 13.2 e 14), não abordando questões ligadas ao suporte da infrastrutura, de gestão de cópias, medidas para corrupção ou perda de dados, ou mesmo mudança de tecnologia. De uma forma geral poderíamos incluir a globalidade dos requisitos desta subsecção nos requisitos do NESTOR relativos à formalização de todos os seus elementos com base num processo definido e a implementação das exigências da gestão de objectos por parte da infrastrutura tecnológica (5.2 e 13.1). Quanto às questões da gestão de riscos de segurança (subsecção 5.3), a ISO 16363:2012 requer 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). O NESTOR apenas aborda a implementação de requisitos de segurança no âmbito do sistema de segurança e a protecção do repositório e dos objectos digitais (13.2 e 14).

Em relação ao NESTOR, alguns critérios parecem estar englobados em todos os requisitos de uma subsecção da ISO 16363. É o caso da definição de critérios para a selecção de objectos digitais (1.1) que parece incluir todos os requisitos da gestão de conteúdo no âmbito da ingestão (4.1 da ISO), da garantia de acesso da Comunidade Designada aos objectos digitais (2.1) e a definição dos DIPs e a garantia da transformação dos AIPs em DIPs (11.1 e 11.2), que integram a generalidade dos requisitos de gestão de acesso (4.6 da ISO), a documentação de todos os seus elementos de acordo com um processo definido (5.2), e os requisitos ligados à implementação das necessidades de gestão dos objectos por parte da infrastrutura (13.1), ligados à infrastrutura do sistema (5.1 da ISO). Por outro lado surgem dúvidas de que o

requisito referente ao registo de metainformação estrutural dos objectos digitais (12.3) tenha equivalência directa nos requisitos da ISO 16363, referentes à necessidade de ferramentas e métodos que definam a informação de Representação necessária para garantir a compreensibilidade dos dados dos objectos pela Comunidade Designada, com o devido acesso à informação de Representação necessária, e resultante garantia de que a informação de Representação está associada aos objectos de dados de forma persistente (4.2.5.2, 4.2.5.3, 4.2.5.4)

Aplicação ao RODA

TRAC

No âmbito do TRAC, e tomando em consideração a avaliação de conformidade com os critérios da lista de verificação referida, e na qual participámos no âmbito do projecto RODA, considera-se que os critérios da secção A (Infrastrutura Organizacional) não se aplicam directamente ao sistema aplicacional do RODA, mas à organização que é o seu detentor.[710] No entanto, tomou-se como exemplo a DGLAB, primeira detentora do RODA, e sendo esta organização uma instituição estatal ligada à área do património, e que tem à sua disposição recursos para garantir a salvaguarda do património arquivístico nacional em formato electrónico, consideramos que cumpre estes requisitos. Tal cumprimento é verificável pelas evidências na legislação nacional, como a Lei orgânica da instituição, a Lei de Bases de Património Cultural e legislação sobre a protecção de dados, segurança do Estado, direitos de autor e conexos, acesso e reutilização de documentos da Administração Pública, acesso ao património arquivístico e outros regimes específicos de acesso, acessibilidades para cidadãos com necessidades especiais, comércio electrónico, assinatura electrónica e valor probatório dos documentos electrónicos, declaração de compromisso com a preservação a longo prazo, com a gestão e com o acesso à informação digital, disponível a todas as partes interessadas. A nível normativo incluem-se as normas e recomendações adoptadas, como por exemplo ISO 14721:2003 (OAIS), ISO 17799:2005 (segurança), ISO 20652:2003 (pré-ingestão), ISO 9000 (qualidade), ISO 27001:2013 (segurança). Outros documentos passam pela Declaração de missão, acordos de depósito, contratos com fornecedores de serviços ao repositório e licenças de *software*. Em termos de documentos de política podemos referir a política de aquisição, política de preservação[711], política de acesso, compromisso de transparência, plano de contingência/recuperação de desastres, plano de sucessão e o plano de *backups* e cópias. De especial relevância são ainda os recursos humanos, com a identificação das competências necessárias para operar o repositório em termos dos compromissos assumidos e a demonstração de que o pessoal detém essas competências, a descrição de funções, definição de papéis e responsabilidades. Neste âmbito inclui-se também a formação. A garantia de recursos financeiros requer planos de negócio a curto e longo prazo sustentados por orçamentos e relatórios financeiros e de auditoria, que incluam exposição a cenários de contingência e desastre. O sistema está também dotado de manuais de procedimentos para

[710] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade.
[711] HENRIQUES, Cecília – RODA: política de preservação digital.

actualização do sistema, procedimentos de ingestão[712], procedimentos de administração[713] que incluem tarefas ligadas à preservação e à metainformação descritiva/pesquisa[714], procedimentos de disseminação[715], procedimento de avaliação da integridade do repositório e resposta a situações de erro/risco e procedimento de avaliação da inteligibilidade (sendo que este são da responsabilidade da entidade funcional de Planeamento de Preservação – CRIB e agora PLATO).

No que respeita a secção B (Gestão de Objectos Digitais) e a secção C (Tecnologias, Infrastrutura Técnica e Segurança) surgem como principais evidências os documentos de exploração e a documentação do sistema. Os documentos de exploração incluem relatórios de auditoria externa e de auto-avaliação, documentação sobre as decisões e/ou acções tomadas, relatórios de ingestão[716], de administração[717] e disseminação[718] (que também estão registados nas rotinas de auditoria do sistema). Do ponto de vista de arquitectura, infrastrutura técnica e segurança, inclui-se a Documentação do sistema, incluindo questões como a caracterização dos AIPs, a conversão de SIPs em AIPs e de AIPs em DIPs, a criação de identificadores únicos e persistentes, a segurança de riscos e de permissões, controlos de acesso, controlo e sincronização de cópias (mesmo que estejam fora do sistema), a documentação dos fornecedores indicadora do ciclo de vida do *hardware*, e finalmente os inventários de *backup*, *software* e *hardware*.

A avaliação feita com base no TRAC considera então que o RODA cumpre todos os requisitos relativos à aquisição de conteúdo, planeamento de preservação, armazenamento de arquivo e preservação/manutenção dos AIPs, e gestão de Informação (subsecções B1, B3, B4, B5). Na subsecção B2, de criação de pacotes de arquivo no âmbito da Ingestão, a avaliação efectuada ao RODA antes do início do Projecto SCAPE considerou que o critério B2.10 não era cumprido porque a rede de informação necessária para documentar o cumprimento do requisito de inteligibilidade do conteúdo da informação e de assegurar o nível contratualizado de inteligibilidade dependia inteiramente da especificidade dos objectos de informação, pelo que necessitava de ser criada e adaptada como parte de um projecto próprio, sendo tal especialmente aplicável a tipos de objecto complexos tais como bases de dados, podendo ser utilizadas ferramentas de análise interna (a não ser que essa informação seja fornecida *à priori* pela metainformação existente).[719] A avaliação actual considera que a actual versão do RODA cumpre este requisito, uma vez que se recorre ao feedback dos utilizadores para verificar se a metainformação descritiva dos conteúdos ingeridos é compreensível, sendo o resultado do processo de validação manual/semântico da metainformação descritiva registado no sistema e ligado à metainformação referente ao SIP, executando-se um processo para teste de cada AIP ingerido e registando o resultado no sistema. Quando se constata que o conteúdo do objecto não consegue ser apresentado de forma compreensível, o SIP é rejeitado e os produtores são

[712] CORUJO, Luis – RODA: manual de procedimentos de ingestão.
[713] CORUJO, Luis – RODA: manual de procedimentos de administração.
[714] CORUJO, Luis – RODA: manual de procedimentos de gestão de planos de classificação.
[715] CORUJO, Luis – RODA: manual de procedimentos de disseminação.
[716] CORUJO, Luis – RODA: manual de procedimentos de ingestão.
[717] CORUJO, Luis – RODA: manual de procedimentos de administração.
[718] CORUJO, Luis – RODA: manual de procedimentos de disseminação.
[719] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade.

notificados, ficando os sistemas a aguardar a ingestão de um novo SIP. De igual forma, mas já no que respeita à gestão de Acesso (subsecção B6), a avaliação efectuada ao RODA antes do início do Projecto SCAPE considerou existirem dois critérios que não são cumpridos, referentes ao registo e análise das falhas de acessos e demonstração de resultados de todos os pedidos de acesso (critérios B6.6 e B6.9), uma vez que essa versão do sistema RODA ainda não implementava integralmente essa funcionalidade.[720] No entanto, o ecossistema SCAPE desenvolveu funcionalidades que permitem o cumprimento dos requisitos de registo e análise das falhas de acesso e outras anomalias (critério B6.6), através do registo de todas as acções de autenticação, sendo tal registo facilmente inspeccionado pelos administradores do sistema, e também de permitir o registo e resolução de problemas relatados pelos utilizadores acerca de erros de respostas ou nos dados (critério B6.9), através da notificação dos administradores do sistema aquando de certas ocorrências e também pela existência de canais de feedback para os utilizadores reportarem quaisquer problemas nos dados ou no repositório.

Em termos de Infrastrutura do sistema (subsecção C1) a avaliação efectuada ao RODA antes do início do Projecto SCAPE considerou que o repositório não tinha as funcionalidades de gestão do número e localização de cópias de todos os objectos digitais, nem os mecanismos para assegurar que as múltiplas cópias dos objectos digitais estão sincronizadas (critérios C1.3 e C1.4), mas que tais tarefas eram desempenhas pela organização fora do sistema, uma vez que guardava as cópias dos objectos digitais e respectiva metainformação. Actualmente estes requisitos são cumpridos directamente pela existência de uma cópia-matriz do objecto digital no sistema, e indirectamente através das cópias feitas pelo sistema de *backup*, que faz a gestão da sua localização. O critério C1.8, referente ao processo de gestão de mudança documentado, é sobretudo um procedimento predominantemente organizacional, que precisa de ser implementado na respectiva instituição, constituindo evidência os documentos ligados à gestão de mudança, como a política de preservação[721], o plano de contingência/recuperação de desastres, o plano de sucessão, o plano de *backups* e cópias, os planos de negócio sustentados por orçamentos e relatórios financeiros e de auditoria, que incluem a exposição a cenários de contingência e desastre, e ainda os procedimentos para actualização, manuais para ingestão[722], e para administração.[723] O critério C.1.9, que diz respeito à existência de um processo para testar o efeito de alterações críticas ao sistema, está dependente da actuação de pessoal operador do sistema para se considerarem aspectos específicos de configuração local, apesar das actualizações do sistema passarem por um rigoroso procedimento de testes para assegurar que não afectam o seu funcionamento. Este procedimento é realizado em parte durante o ciclo de lançamento dos componentes de fonte aberta, mas, de acordo com o estipulado pela organização, precisa de ser repetido no local por pessoal operador do sistema para se considerarem aspectos de configuração local. Também o critério C1.10 sobre a existência de um processo para integrar novas actualizações de segurança do *software* com base numa avaliação de risco/benefício, é cumprido parcialmente, porque tais actualizações são feitas intencionalmente de modo manual, de acordo com os procedimentos para actualização definidos pelo organismo. Estas devem ser primeiro instaladas num sítio de pré-

[720] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade.
[721] HENRIQUES, Cecília – RODA: política de preservação digital.
[722] CORUJO, Luis – RODA: manual de procedimentos de ingestão.
[723] CORUJO, Luis – RODA: manual de procedimentos de administração.

produção antes de se aplicarem à aplicação principal. Adicionalmente os sistemas operativos actuais já produzem notificações e registam quaisquer acções tomadas para melhorar a segurança através de actualizações. A subsecção referente à Tecnologia adequada (subsecção C2) é cumprida totalmente, na medida em que se constata a existência de *hardware* e *software* apropriados para os serviços que fornece, e a tecnologia SCOUT para a vigilância de preservação notifica o utilizador quando ocorrem não-conformidades. O ecossistema SCAPE, através do SCOUT e do PLATO, monitoriza o *hardware* e *software*, verificando o consumo de recursos para verificação de necessidades e alternativas existentes para a actualização. Paralelamente, existe um quadro de referência para o desenvolvimento do RODA. Finalmente, os critérios referentes à subsecção C3 (Segurança) são comprovados através da documentação indicada anteriormente para secção A (Infrastrutura Organizacional).

ISO 16363:2012

A recentíssima (à data da produção deste trabalho) avaliação de conformidade apresentada no âmbito do projecto SCAPE refere-se apenas à perspectiva tecnológica, pelo que existe um conjunto significativo de critérios cuja verificação não pode ser feita fora do contexto da organização responsável pelo repositório ou da infrastrutura tecnológica onde este assenta, pelo que não foi tida em conta na sua avaliação.[724] Para o Projecto SCAPE, tais requisitos precisam de ser abordados pelas entidades que adoptarem o *SCAPE Preservation Environment*, mas referem-se somente a questões organizacionais, não remetendo para o suporte técnico do ecossistema, muito embora sejam tratados nos recursos referentes às questões de Política e de boas práticas.[725] Por ser essencialmente uma avaliação no âmbito do ecossistema de preservação desenvolvido pelo referido projecto europeu, foca-se por um lado, no pacote de *software* que integra não só o RODA, mas também num ambiente de execução, serviços de planeamento e observação, e por outro, nas políticas de controlo de preservação, orientações para boas práticas e relatórios[726], verificando-se que o termo "repositório" utilizado em quase todos os critérios existentes na ISO 16363:2012 (apenas um requisito o não menciona explicitamente, o 4.2.4.1.3) se reporta ao *SCAPE Preservation Environment* e não à organização responsável pelo repositório digital. No entanto, e tal como na avaliação feita no âmbito do TRAC, tomou-se como exemplo a DGLAB, primeira detentora do RODA, pelo que se pretende aventar algumas diferenças de resultados da avaliação feita no âmbito deste trabalho e da avaliação de conformidade no âmbito do projecto SCAPE, e que serão especificados.

Assim a avaliação de conformidade do SCAPE considera que a maioria dos critérios apresentados na secção 3 (Infrastrutura Organizacional) está fora do âmbito da sua análise (todos os critérios referentes às subsecções do Governo e Viabilidade Organizacional (3.1), Estrutura Organizacional e Recursos Humanos (3.2), Sustentabilidade Financeira (3.4), e quatro dos sete requisitos da secção Responsabilidade e Responsabilização[727] Procedimental e Quadro de Política de Preservação (3.3)), existindo três totalmente suportados (referentes à

[724] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 7.
[725] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 23.
[726] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 1, 4, 7, 23.
[727] Responsabilidade e Responsabilização – *Accountability* no original.

políticas de preservação (3.3.2), transparência e Responsabilidade e Responsabilização de todas as acções (3.3.4) e verificações de integridade (3.3.6)), um parcialmente suportado (ligado ao rastreio e gestão de direitos e restrições de propriedade intelectual (3.5.2)), e cinco não suportados (ligados à gestão dos contratos estabelecidos com os produtores (3.5.1 e dentro deste desde o 3.5.1.1 até ao 3.5.2.2)). Na sua perspectiva, a totalidade dos requisitos que consideram estar fora do âmbito da sua análise referem-se a políticas e procedimentos, que são abordados em documentos da sua autoria[728], que podem servir de referência para qualquer organização que pretenda adoptar boas práticas na produção de políticas de preservação.[729] Estes documentos descrevem um enquadramento de política de preservação que consiste em três níveis que vão desde a Política de Orientação de alto nível, passando pela definição e descrição de Políticas de Procedimentos de Preservação, até a instruções concretas de suporte ao *workflow* automatizado definidas nas Políticas de Controlo.[730] Referem também que os requisitos não suportados poderiam ser considerados fora do âmbito da sua análise, uma vez que os acordos ou contratos de depósitos são estabelecidos fora do sistema tecnológico, mas uma vez que existem sistemas de repositório que fornecem suporte para admissão de acordos de depósito, optaram por considerá-los não suportados.[731] Quanto ao requisito parcialmente suportado (3.5.2), o ecossistema SCAPE inclui uma acção que verifica as permissões referentes a cada AIP em relação às restrições definidas na metainformação descritiva, resultando a emissão de um aviso ao proprietário do repositório quando as permissões não estão correctamente definidas.[732]

No âmbito da norma ISO 16363:2012, a nossa avaliação considera que todos os critérios referentes à secção 3 (Infrastrutura Organizacional) são cumpridos, uma vez que a organização apresenta a documentação que o comprova. É o caso específico do Plano de Preservação Digital referente ao critério 3.1.2, a Declaração de missão e documentos de política de preservação[733] e de política de acesso, como declaração de compromisso com a preservação a longo prazo, com a gestão e com o acesso à informação digital, disponível a todas as partes interessadas e que inclui a declaração global das propriedades do objecto digital/classe de objecto digital a preservar, referentes aos critérios 3.1.3 e 3.3.2. Assim, consideramos que os requisitos que a análise produzida no âmbito do projecto SCAPE considerou como fora do âmbito, parcialmente suportadas (3.5.2) e não suportadas (3.5.1 e dentro deste desde o 3.5.1.1 até ao 3.5.2.2), são inteiramente suportados se tivermos em conta a avaliação do RODA no seio da organização.

No que se refere à secção 4 da norma, ligada à gestão dos objectos digitais, o SCAPE considera que o seu ecossistema suporta todos os requisitos com excepção de um requisito que consideraram não suportado e de outro considerado fora do âmbito da análise. O requisito não suportado refere-se à descrição de como os AIPs são construídos a partir dos SIPs (4.2.2), ligado à subsecção da criação do AIP no âmbito da Ingestão (4.2), na medida em que somente

[728] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 22.
[729] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 23.
[730] BECHHOFER, Sean [et al.] – SCAPE Final version of policy specification model; SIERMAN, Barbara; JONES, Catherine; ELSTRØM, Gry – SCAPE Catalogue of preservation policy elements.
[731] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 11 e 22.
[732] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 11.
[733] HENRIQUES, Cecília – RODA: política de preservação digital.

fornece tal informação ao nível do código-fonte do RODA, notando que é necessário produzir tal documentação.[734] O requisito considerado fora do âmbito diz respeito à existência de procedimentos para todas as acções tomadas sobre os AIPs (4.4.2.1), ligado à subsecção referente à Preservação de AIPs (4.2.4), na medida em que teria a ver com questões de documentos de procedimentos e variam de organismo para organismo.[735]

Quanto à secção referente à gestão dos objectos digitais, a nossa avaliação considera que o RODA cumpre plenamente com os requisitos no âmbito da aquisição de conteúdo, planeamento de preservação, preservação dos AIPs, e gestão da informação (secções 4.1, 4.3, 4.4 e 4.5). A título de exemplo, são apresentados os documentos referentes aos esquemas de metainformação, à política de preservação[736], os acordos de depósito e documentação acerca do *workflow*, o plano de preservação e os relatórios de rotina de auditoria, como evidências dos critérios referentes aos procedimentos e registos ligados às Propriedades da Informação e Informação de Conteúdo critérios 4.1.1.1 e 4.1.1.2), documentação técnica acerca dos formatos e acerca dos elementos que constituem o SIP, como o relatório do RODA[737], para o critério referente ao reconhecimento e análise dos SIPs (critério 4.1.3), o Plano de Preservação Digital com a referenciação de utilização de serviços de registo de formatos e de monitorização da evolução tecnológica, para suprir necessidades de Informação de Representação adicional (critério 4.3.3.1), documentação com indicação de todas acções possíveis de executar sobre os AIPs e rotinas de auditoria que demonstrem a execução e os resultados dessas acções (como é o caso do Documento de política de preservação digital[738] e do manual de procedimentos de administração[739]) (critérios 4.4.2.1 e 4.4.2.2).

No que se refere à criação do AIP no âmbito da ingestão (subsecção 4.2), evidencia-se a política de preservação[740] que garante a recuperação, identificação e gestão dos AIPs a longo prazo (critério 4.2.1), a descrição das convenções para atribuição de identificadores únicos e persistentes, prova da sua aplicação (ex. relatórios automáticos do sistema), compromisso de produção de relatórios que descrevam o processo de implementação de alterações ao sistema de identificadores (quando tal se verifique, documentação que especifique a estratégia usada para fazer o mapeamento entre o ID original (como a metainformação de proveniência) e o atribuído pelo repositório, quando o SIP já traz um identificador único (critérios 4.2.4.1.3, 4.2.4.1.4, 4.2.4.1.5 e 4.2.4.2), os documentos de política de ingestão, o manual de procedimentos de ingestão[741] e a documentação técnica do sistema que permita definir a informação de representação necessária para a sua compreensão, acesso e ligação persistente ao objecto ao qual diz respeito (critérios 4.2.5.2, 4.2.5.3, 4.2.5.4). No que respeita ao requisito referente à descrição de como os AIPs são construídos a partir dos SIPs (4.2.2), consideramos que a documentação técnica produzida no âmbito do desenvolvimento inicial do RODA, como a descrição do sistema, inclui questões como a caracterização dos AIPs, a conversão de SIPs em

[734] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 14 e 23.
[735] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 18 e 23.
[736] HENRIQUES, Cecília – RODA: política de preservação digital.
[737] FARIA, Luis, CASTRO, Luis – RODA Repositório de Objectos Digitais Autênticos – relatório final.
[738] HENRIQUES, Cecília – RODA: política de preservação digital.
[739] CORUJO, Luis – RODA: manual de procedimentos de administração.
[740] HENRIQUES, Cecília – RODA: política de preservação digital.
[741] CORUJO, Luis – RODA: manual de procedimentos de ingestão.

AIPs e de AIPs em DIPs, constituindo evidência de conformidade com o referido requisito. Podemos mesmo aventar que o código-fonte constitui ele próprio um documento evidencial de descrição da construção de AIPs a partir dos SIPs. Ainda dentro desta secção, e ao contrário do que se verificou na avaliação efectuada ao RODA antes do início do Projecto SCAPE[742], verifica-se o cumprimento dos requisitos referentes à garantia de compreensão da informação de conteúdo (critérios 4.2.7, 4.2.7.1, 4.2.7.2, 4.2.7.3), uma vez que se recorre ao *feedback* dos utilizadores para verificar se a metainformação descritiva dos conteúdos ingeridos é compreensível (4.2.7), sendo o resultado do processo de validação manual/semântico da metainformação descritiva registado no sistema e ligado à metainformação referente ao SIP (4.2.7.1), executando-se e registando no sistema o resultado de um processo para teste de cada AIP ingerido (4.2.7.2). Caso se verifique que a Informação de Conteúdo não consegue ser renderizada (isto é, apresentada de forma compreensível), o SIP é rejeitado e os produtores são notificados, ficando os sistema a aguardar a ingestão de um novo SIP (4.2.7.3). De igual forma, mas já no âmbito dos requisitos de gestão de acesso (subsecção 4.6), constata-se que após a avaliação efectuada ao RODA antes do início do Projecto SCAPE[743], foram implementadas medidas no sentido do RODA cumprir plenamente com os critérios de registo e análise das falhas de acesso e outras anomalias (critério 4.6.1.1), através do registo de todas as acções de autenticação, sendo tal registo facilmente inspeccionado pelos administradores do sistema, e também permitir o registo e resolução de problemas relatados pelos utilizadores, referente a erros de respostas ou nos dados (critério 4.6.2.1), através da notificação dos administradores do sistema aquando de certas ocorrências e também pela existência de canais de *feedback* para os utilizadores reportarem quaisquer problemas nos dados ou no repositório.

A avaliação do SCAPE no âmbito da ISO 16363:2012 considerou que a maioria dos requisitos integrados na secção 5, referente à gestão de risco a nível de infrastrutura e de segurança, está fora do âmbito da análise, particularmente a totalidade dos quatro requisitos da subsecção de Gestão de Risco de Segurança (5.2). Assim, na subsecção ligada à Gestão de Risco da Infrastrutura Técnica, consideraram a existência de um requisito parcialmente suportado (ligado à gestão de riscos das suas operações e finalidades de preservação ligadas à infrastrutura do sistema (5.1.1), e de novo fora do âmbito de análise (ligados à utilização de *hardware* adequado para os serviços que fornece (5.1.1.1.1), procedimentos, compromissos e recursos para substituição de hardware e de software (critérios 5.1.1.1.4 e 5.1.1.1.8), registo e produção de relatórios para a administração acerca de todas as ocorrências de corrupção de dados (5.1.1.3.1), processo para integrar novas actualizações de segurança do software com base numa avaliação de risco/benefício (critério 5.1.1.4), definição de processos para substituição de suportes de armazenamento e *hardware* (5.1.1.5), identificação e documentação de processos críticos que afectam a capacidade de cumprir com as responsabilidades obrigatórias (5.1.1.6), formalização do processo de mudança (5.1.1.6.1), e existência de processos para teste e aferição dos efeitos da mudança (5.1.1.6.2)) sendo os restantes dez requisitos totalmente suportados.

[742] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade.
[743] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade.

O requisito 5.1.1 foi considerado parcialmente suportado pelo facto de alguns dos seus subrequisitos estarem fora do âmbito do análise, por dizerem respeito a questões ligadas com o hardware utilizado, com a organização e financiamento[744], como é o caso dos critérios 5.1.1.1.4, 5.1.1.1.8. Quanto ao requisito 5.1.1.3.1 o SCAPE admite que o sistema é capaz de notificar os administradores por correio electrónico, quando ocorrem erros, e o registo de ocorrências é feito numa plataforma que é independente do repositório.[745] Quanto ao requisito 5.1.1.4, referem estar relacionado com a existência de procedimentos escritos, embora a generalidade dos sistemas operativos actuais notifique e registe quaisquer acções tomadas para melhorar a segurança através de actualizações.[746] Os restantes requisitos da subsecção 5.1 são considerados fora do âmbito da análise por, na opinião do SCAPE, não estarem relacionados com o sistema. Quanto aos requisitos totalmente suportados que se encontram na subsecção 5.1, o SCAPE sublinha o papel do SCOUT, software abordado anteriormente, porque alarga a capacidade de monitorização do repositório de preservação no que respeita às mudanças de tecnologia[747], mas também surgem menções ao *Plato* (5.1.1.1.3, 5.1.1.1.6, 5.1.1.1.7) e ao plano de desenvolvimento do RODA (5.1.1.1.5). No que se refere aos requisitos da subsecção 5.2, o SCAPE considera estarem todos fora do âmbito da análise, mas refere que a implementação da ISO27001:2013[748] favorece grandemente a garantia de conformidade com os requisitos ligados à gestão de riscos de segurança, e no caso específico do critério 5.2.3 refere que o ecossistema SCAPE suporta a gestão de permissões, funções, grupos e utilizadores com grande nível de granularidade, pelo que qualquer política de autorizações pode ser facilmente implementada.[749]

No que diz respeito à secção de gestão de risco a nível de infrastrutura e de segurança (secção 5), a nossa avaliação evidencia a existência, no âmbito da organizão em apreço, de *hardware* apropriado para os serviços que fornece (5.1.1.1.1), de documentação como planos de investimentos, inventários de *software* e *hardware*, documentação de fornecedores, de procedimentos, compromissos e recursos para substituição de *hardware* e de *software* (critérios 5.1.1.1.4 e 5.1.1.1.8), documentação que constata as obrigações do repositório e as tarefas necessárias para o seu cumprimento, definindo os procedimentos considerados vitais para o repositório (critério 5.1.1.6). Para além disso constata-se que o sistema envia notificações de ocorrência de erros aos administradores por correio electrónico e o registo de ocorrências é feito numa plataforma que é independente do repositório (5.1.1.3.1). O requisito identificado com a definição de processos para mudança de *hardware* e suportes de armazenamento (5.1.1.5) integra-se nos procedimentos definidos para a actualização do parque informático da organização. No entanto, é de referir que o RODA não contém especificamente um processo automático para integrar novas actualizações de segurança do *software* com base numa avaliação de risco/benefício (critério 5.1.1.4), porque tal tarefa é executada intencionalmente, de acordo com os procedimentos para actualização definidos pelo organismo, de modo manual, sendo primeiro instaladas num sítio web de pré-produção

[744] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 19.
[745] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 20.
[746] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 20.
[747] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 23.
[748] ISO 27001:2013, Information technology - Security techniques - Information security management systems – Requirements.
[749] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 21.

antes de se aplicarem à aplicação principal. Adicionalmente os sistemas operativos actuais já produzem notificações e registam quaisquer acções tomadas para melhorar a segurança através de actualizações. O requisito referente à identificação e formalização de processos críticos que afectam a capacidade de cumprir com as responsabilidades obrigatórias (5.1.1.6) tem como evidências os documentos de procedimentos de ingestão[750], de administração[751], de disseminação[752], avaliação da integridade do repositório e resposta a situações de erro/risco, e procedimento de avaliação da inteligibilidade, aos quais se acrescentam os relatórios com registos de acções produzidos pelo sistema. O requisito referente ao processo de gestão de mudança documentado que identifica todas as alterações em processos críticos que possam afectar a capacidade do repositório de cumprir com as suas obrigações (critério 5.1.1.6.1) diz respeito a um procedimento predominantemente organizacional que precisa de ser implementado na respectiva instituição, constituindo evidência documentos ligados à gestão de mudança, como a política de preservação[753], o plano de contingência/recuperação de desastres, o plano de sucessão, o plano de *backups* e cópias, os planos de negócio sustentados por orçamentos e relatórios financeiros e de auditoria, que incluem a exposição a cenários de contingência e desastre, e ainda os procedimentos para actualização, manuais para ingestão[754], e para administração.[755]

O cumprimento do requisito relativo à avaliação do efeito de alterações aos processos críticos do repositório (critério 5.1.1.6.2) está dependente da actuação de pessoal operador do sistema para se considerarem aspectos específicos de configuração local, apesar das actualizações do sistema passarem por um rigoroso procedimento de testes para assegurar que não afectam o seu funcionamento, e de tal procedimento ser realizado parcialmente durante o ciclo de lançamento dos componentes de fonte aberta. Finalmente, as funcionalidades que dizem respeito aos requisitos de gestão do número e localização de cópias de todos os objectos digitais e aos mecanismos para assegurar que quaisquer múltiplas cópias dos objectos digitais estão sincronizadas (critérios 5.1.2 e 5.1.2.1), e que não tinham sido implementadas na versão do RODA[756] anterior ao projecto SCAPE, são agora cumpridas directamente pela existência de uma cópia-matriz do objecto digital no sistema, e indirectamente através das cópias feitas pelo sistema de *backup*, que faz a gestão da sua localização. Quanto à gestão de risco de segurança (5.2), o cumprimento dos requisitos é evidenciado pela existência de documentação normativa que passa pelas normas e recomendações adoptadas, como por exemplo ISO 17799:2005 (segurança) e ISO 27001:2013 (segurança). Outra documentação que constitui evidência inclui o plano de contingência/recuperação de desastres, plano de sucessão, plano de *backups* e cópias, documentação acerca dos recursos humanos, com a identificação das competências necessárias para operar o repositório em termos dos compromissos assumidos e a demonstração que o pessoal detém essas competências, a descrição de funções, definição de papéis e responsabilidades. Finalmente, é digna de menção a documentação referente a

[750] CORUJO, Luis – RODA: manual de procedimentos de ingestão.
[751] CORUJO, Luis – RODA: manual de procedimentos de administração.
[752] CORUJO, Luis – RODA: manual de procedimentos de disseminação.
[753] HENRIQUES, Cecília – RODA: política de preservação digital.
[754] CORUJO, Luis – RODA: manual de procedimentos de ingestão.
[755] CORUJO, Luis – RODA: manual de procedimentos de administração.
[756] BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade.

recursos financeiros, como planos de negócio a curto e longo prazo sustentados por orçamentos e relatórios financeiros e de auditoria, que incluam exposição a cenários de contingência e desastre, e manuais de procedimentos para actualização do sistema, procedimento de avaliação da integridade do repositório e resposta a situações de erro/risco, e procedimento de avaliação da inteligibilidade.

Resumindo, e de acordo com a avaliação feita no âmbito do projecto SCAPE[757], o RODA suporta totalmente 69 (sessenta e nove) requisitos da ISO 16363:2012, considerando que 31 (trinta e um) requisitos estão fora do âmbito da avaliação por dizerem respeito a questões ligadas à instituição, e que não podem ser cumpridas somente do ponto de vista tecnológico nem verificáveis fora do quadro organizacional. Paralelamente a isto, consideram que 2 (dois) requisitos são parcialmente suportados pelo RODA, que somente não suporta 6 (seis) requisitos, o que dá um nível de conformidade sensivelmente na ordem nos 90 por cento (não contabilizando os requisitos da norma que consideram ser referentes à organização).

Tal levou a que o projecto SCAPE identificasse os pontos fracos do RODA a abordar para garantir que este repositório atinga a conformidade total no âmbito de um processo de certificação com base na ISO 16363:2012. Esses elementos são:

- Capacidade e gerir e manter os contratos ou acordos de depósito através dos interfaces de utilizador do repositório;
- Suporte para rastreamento dos direitos de propriedade intelectual;
- Melhorar a documentação técnica, especialmente a que concerne à conversão de SIPs para AIPs;
- Capacidade de auxiliar o gestor do repositório na realização de uma melhor gestão de risco.[758]

NESTOR

No âmbito do NESTOR, a avaliação verifica que o RODA cobre a totalidade dos requisitos indicados, muito por causa da documentação produzida em termos de objectivo (critério 1) requisitos mínimos de garantia de acesso (critério 2), compilação de legislação e de compromissos contratuais (critério 3), documentação sobre recurso humanos e financeiros, planeamento a longo prazo e gestão de mudança (critérios 4 e 8), normas, recomendações e manuais de procedimentos (critério 5), procedimentos que garantem a integridade e autenticidade dos objectos digitais (critérios 6 e 7), documentos de política de aquisição (critério 9), política de armazenamento/preservação (critério 10) e política de acessos (critério 11), documentação técnica do sistema, segurança do sistema e esquemas de metainformação (critérios 12, 13, 14). Os relatórios, rotinas de auditoria, documentos de auto-avaliação, registos de aquisições, resultados de monitorização, em suma, os documentos produzidos no âmbito da exploração do sistema, permitem confirmar que o RODA cumpre os requisitos do NESTOR no funcionamento do dia-a-dia.

[757] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. IV e 21-24.
[758] FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation, p. 23-24.

Conclusão à comparação e à aplicação

A classificação de um repositório como confiável passa necessariamente pela análise da percepção da sua comunidade de interesse, já que a missão dos repositórios é servir um grupo particular ou a Comunidade Designada, como aponta Yoon (2014).[759] Todavia, a autora salienta que a medição dessa percepção é muito complexa, constituindo ainda um campo aberto a estudos futuros, para o qual a generalidade dos projectos de estabelecimento de programas de auditoria e certificação ainda não encontraram critérios claramente definidos.

Por outro lado, ainda que seja possível identificar pontos comuns aos vários projectos para a certificação de repositórios digitais confiáveis, ainda não foi possível estabelecer um conjunto de requisitos para um único programa de auditoria e certificação, sob as mesmas regras. Como se verificou, as tentativas de comparação internacional entre os critérios e métodos propostos pelo DCC/DPE, RLG/NARA e NESTOR, em 2007 e em 2011 pelo *CCSDS/ISO*; *Data Seal of Approval Board* (DSA); e *DIN NESTOR,* apenas foi possível estabelecer um consenso quanto a um conjunto de dez princípios básicos para a confiabilidade dos repositórios e os níveis de certificação no âmbito de um *European Framework for Audit and Certification of Digital Repositories*. Contam-se como constrangimentos os quadros jurídico-legais de cada país, os sistemas institucionais, os estados de desenvolvimento de cada um, entre outros, que levam a que, actualmente, seja ainda difícil desenvolver e aplicar uma norma internacional comum.

Com o presente trabalho pretendemos fazer uma brevíssima comparação entre os critérios do TRAC, NESTOR e ISO 16363:2012, destacando os elos de contacto e as diferenças entre eles, embora sem pretensões de assentar "os critérios básicos" para a confiabilidade dos repositórios tal como foi tentado executar em 2007, como atrás referido. Ainda assim, partilha-se algumas ideias quanto à formulação geral de cada documento.

Assim, a nosso ver, o TRAC e a ISO 16363:2012 valorizam a necessidade de comprovar documentalmente os mais variados procedimentos – o que se reflecte no apelo à redacção de políticas - de modo a que estejam reunidas as condições para uma auditoria externa imediata, ou seja, que haja mecanismos independentes de verificação, indicando várias vezes que essa deve ser uma das preocupações dos repositórios digitais. Outra finalidade da necessidade de provar documentalmente todos os processos é a protecção legal, na medida em que o repositório demonstra que agiu conforme os procedimentos definidos pelos planos existentes, actuando no cúmulo das suas competências. Já no NESTOR, em contrapartida, embora tenha sido elaborado com vista à auditoria e certificação, raras vezes surge a consciência desse fim.

Por outro lado, é visível que o TRAC e a ISO 16363:2012 enfatizam a necessidade de prever situações de erro e de falha a vários níveis, desde as características físicas do objecto ao sistema do repositório, como modo de prevenir e evitar os perigos, garantindo sempre que o repositório constitui uma fonte segura e confiável de depósito e obtenção de informação e que os serviços podem ser assegurados por um longo prazo.

Por último, o TRAC e a ISO 16363:2012 são frequentemente mais pormenorizados do que o NESTOR, uma vez que o grau de granularidade é maior. Exemplo disso é a identificação dos

[759] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development.

requisitos relativos às infrastruturas e à segurança tecnológica, em que o NESTOR trata somente de enumerar as ideias gerais deste âmbito que devem presidir a um repositório, de onde resultam apenas quatro critérios, enquanto que o TRAC e a ISO 16363:2012 fornecem uma explicitação mais detalhada de como devem ser cumpridas essas ideias que, não sendo directamente formuladas, constituem a base de acção (vinte e quatro critérios no caso da ISO 16363:2012).

Deve contudo, ser salientado que o TRAC e a ISO 16363:2012, por si só, não são suficientes para assegurar a aplicação prática de programas de auditoria e certificação. É ainda necessário aprofundar questões relacionadas com as práticas desses processos, nomeadamente definir competências e responsabilidades das entidades que neles deverão ser envolvidas, como é o caso dos auditores, estando para esse efeito em produção a ISO 16919, que pretende fixar os requisitos dos membros das futuras equipas a integrarem programas de certificação de repositórios digitais confiáveis.

Assim, e apesar de alguns testes feitos à aplicação da ISO 16363:2012, pode considerar-se que o processo de certificação é apenas ainda informal. Deve também ser pensada a forma de articulação destas normas com outras já existentes ligadas à gestão da qualidade, nomeadamente a ISO 9001.

Há, portanto, um trabalho a desenvolver nesta área no futuro, pois os processos de auditoria e certificação constituem, apesar das diferentes abordagens e projectos em curso, uma ferramenta de desenvolvimento e aumento da confiança nos repositórios digitais. A certificação passa por análise de questões tanto técnicas como qualitativas, envolvendo aspectos como a responsabilidade das organizações, a sua viabilidade e sustentabilidade em meios humanos e financeiros, a permanente adequação e desenvolvimento tecnológico, a segurança nos acessos e na preservação a longo prazo, o estabelecimento de procedimentos fiáveis para assegurar a manutenção das características e valores intrínsecos aos documentos, bem como a qualidade e adequação dos serviços prestados.

Além de encorajar a competição entre instituições, no sentido da constante melhoria, a certificação produz evidência de qualidade para utilizadores e instituições, e induz a maior confiança na capacidade das organizações tomarem medidas para minimizar os riscos inerentes aos sistemas tecnológicos e digitais.

8 – Conclusão

A pesquisa e este trabalho deram a oportunidade de abordar e apresentar um conjunto de pontos que estão intimamente ligados à informação digital, documentos digitais, objectos digitais e sua preservação, mas também aos repositórios e sua confiabilidade e confiança neles depositada.

Aparenta ser progressivamente do conhecimento geral que a informação digital, pela sua dependência de sistemas intermediários (compostos por software e hardware), e características de versatilidade e complexidade, derivadas da sua composição em diversos componentes, e diferentes formas de registo e armazenamento, é ameaçada por problemas que vão desde:

- a ausência da percepção social/organizacional de posse ou, pelo contrário, excessivo sentido de individualização;
- a perda de informação operacional e de informação-memória e perda de valor evidencial, conduzindo a que a responsabilização de conduta e actividades fiquem comprometidas;
- dificuldades de gestão a nível de armazenamento, identificação, recuperação, localização, e controlo;
- rápida obsolescência tecnológica, seja nos formatos, no software, ou nos suportes, constatável pela ilegibilidade, impossibilidade de acesso e mesmo desaparecimento físico, incerteza de retrocompatibilidade das aplicações informáticas, concorrência comercial;
- a instabilidade dos materiais, condições ambientais de armazenamento, os efeitos de manuseamento e utilização, desastres naturais, falhas de infrastrutura, manutenção inadequada;
- avanços tecnológicos que obrigam à rápida substituição de *hardware*, e que advém da competição entre fabricantes, da diminuição do tamanho e do custo das unidades de armazenamento, do aumento da capacidade de armazenamento, e das tendências em termos de fragilidade, estabilidade, segurança e duração antes da obsolescência.

Face a estes problemas apresentam-se soluções, que vão desde a inacção à gestão documental tradicional baseada no papel, mas que não são soluções credíveis, e por outro lado temos um conjunto de respostas credíveis, que se centram na gestão dos documentos electrónicos como documentos principais em ambiente electrónico.

A gestão da informação digital requer assim medidas, estratégias consignadas num plano de preservação que responsabilize e implique todos os elementos da organização que promove a sua gestão.

Ao contrário da conservação dos documentos em suportes ditos tradicionais ou analógicos, e que tem como objectivo que os documentos permaneçam sem quaisquer alterações, recorrendo ao restauro e à prevenção e recuperação dos suportes deteriorados, a preservação digital pretende garantir o acesso à informação electrónica e a sua autenticidade independentemente do formato, *software* e *hardware* usados na sua produção ou utilização

para que foi concebida de origem, para que ela possa ser utilizada a longo prazo, sem qualquer constrangimento físico de plataforma, legal, patrimonial, etc.

No entanto a preservação digital implica um trabalho de definição das características dos documentos electrónicos e de sistematização *a priori* à sua produção. Para além das questões intelectuais, organizacionais, sociais, etc. ligadas às necessidades ou intenções que conduziram à sua produção, é necessário definir as suas características significativas a nível técnico, semântico e de eficácia de comunicação, ligadas essencialmente à parte física, parte lógica, e parte conceptual do objecto.

Para melhor seleccionar a estratégia de preservação a ser aplicada, é preciso ter em conta os critérios de exequibilidade, a sustentabilidade, a viabilidade e a pertinência, e ainda elementos como a análise de riscos, o registo de formatos e a metainformação.

Tudo isto conduz-nos para a definição de um modelo sistémico de preservação digital, tal como indicado por Thomaz.[760] Esse modelo, ou as finalidades e objectivos do mesmo, são identificáveis com os repositórios digitais que têm como objectivo e finalidade a preservação e fornecimento de acesso a informação digital a longo prazo, e que se apelidam de Arquivos Digitais.

Ou seja, instituições com responsabilidades na manutenção do Património digital[761] e que garantem o seu acesso e utilização[762], utilizam mecanismos/ferramentas (tecnologia) para efectivar a gestão e armazenamento dos conteúdos digitais.[763] Essas ferramentas são usadas pelos produtores, disseminadores e utilizadores dos documentos digitais.

Se um Sistema Aberto de Informação de Arquivo (OAIS) (e sem nos esquecermos das considerações de von Bertalanffy[764] e Luhmann[765], Checkland[766] acerca dos sistemas abertos) é conceptualizado como um arquivo que consiste num conjunto de pessoas e sistemas, e que tem como responsabilidade de preservar informação e disponibilizá-la à Comunidade Designada[767], esta definição é suficiente aberta para agregar qualquer repositório ou arquivo, independentemente da tecnologia utilizada e do tipo de informação (analógica ou digital) que gere.[768]

[760] THOMAZ, Katia P - Critical factors for digital records preservation.
[761] OWEN, John Mackenzie – Preserving the digital heritage: roles and responsibilities for heritage repositories. p. 49.
[762] BEAGRIE, Neil et al - Trusted digital repositories: attributes and responsibilities, p. 59.
[763] JISC – What is a repository? In Repositories Support Project (RSP); DOBRATZ, Susanne et al. – NESTOR catalogue of criteria for trusted digital repositories, p. 2.
[764] BERTALANFFY, Ludwig von – General system theory.
[765] LUHMANN, Niklas – Introduction to systems theory.
[766] CHECKLAND, Peter; HOLWELL, Sue – Information, systems and information systems.
[767] WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. III.
[768] BERGMEYER, Winfried - NESTOR criteria catalogue of criteria for trusted digital repositories, p. 4.

Assim, no caso específico da informação digital, constata-se a existência do binómio mecanismo (tecnologia de informação) ←→ sistema (de informação)[769], em que este último é mais abrangente. Dito de outra forma, o repositório digital com funções de Arquivo Digital é um sistema de informação que é constituído por "*uma estrutura que compreende tecnologia, recursos humanos e um conjunto de políticas para incorporar, gerir e acessibilizar numa perspectiva, continuada objectos digitais de natureza arquivística*[770]", sendo isto que a distingue de repositórios digitais com outras finalidades e objectivos.

Neste âmbito surge o RODA como arquivo nacional digital, através do qual a entidade coordenadora e auditora da política arquivística nacional, a Direcção-Geral de Arquivo, actual DGLAB pretende ter capacidade para incorporar documentos electrónicos de forma controlada assegurando a sua gestão ao longo do tempo e a sua acessibilização aos utilizadores, dando assim resposta efectiva a necessidades de depósito, gestão e autenticidade de informação electrónica. Sendo desenvolvido pela DGLAB (então Direcção-Geral de Arquivos), com a colaboração informática da Universidade do Minho, este projecto acarretou o desenvolvimento progressivo de funcionalidades básicas e sólidas e ir progressivamente aumentando estas funcionalidades de forma a receber maiores tipologias de objectos digitais e futuramente, dar resposta e apoio directo a organizações que possuam objectos digitais mas não disponham de recursos especializados nesta área. Este repositório digital foi construído tendo como base o OAIS e documentos técnicos produzidos no âmbito do projecto InterPARES. A base do repositório RODA assenta na plataforma FEDORA, utilizando vários esquemas de metainformação como o EAD, PREMIS, METS e NISO Z39.87. O RODA é hoje em dia um projecto *open source*, dotado de arquitectura escalável e que permite a integração, gestão, preservação e acessibilização de bases de dados relacionais, texto estruturado, imagens fixas, áudio e vídeo digital. Com uma comunidade crescente, principalmente a nível internacional, o RODA é considerado o repositório digital *open source* mais avançado do mundo, podendo tal ser constatado pela forma como foi integrado e utilizado num projecto europeu do 7º programa-quadro, o SCAPE, e do qual se pretende desenvolver infrastrutura e ferramentas escaláveis, criar uma *framework* para *workflows* de preservação e integrar com um sistema de planeamento e monitorização.[771]

Face ao exposto no magistral Modelo de Referência OAIS, verifica-se uma total identificação entre o RODA e os Modelos conceptualizados nesta norma, a saber, Modelo de Ambiente Externo, Modelo Funcional, e Modelo de Informação.

Assim, é fácil de identificar os intervenientes e as entidades funcionais e interfaces relacionadas propostas na norma OAIS com as definidas e desenvolvidas no âmbito no RODA, nomeadamente a entidade funcional de Planeamento de Preservação.

Ao mesmo tempo, é analogamente verificável a existência no RODA dos conteúdos e metainformação (descritiva, administrativa, estrutural, técnica, de preservação) que está identificada no Modelo de Informação do OAIS, e que se referem às diversas classes de

[769] JISC – What is a repository?. In Repositories Support Project (RSP); FERREIRA, Miguel - Introdução à preservação digital, p-71; VERHEUL, Ingeborg - Networking for digital preservation, p. 21.
[770] BARBEDO, Francisco – Arquivos digitais: da origem à maturidade, p. 12.
[771] FARIA, Luís - Desafios práticos à preservação digital: RODA e SCAPE.

objectos, à taxonomia dos objectos de informação e os Pacotes de Informação (SIP, AIP, DIP) por eles constituídos.

E se o espectro de aplicação do Modelo OAIS extravasou o objecto de informação de arquivo[772], podemos considerar que tal se deveu ao facto do trabalho desenvolvido em torno deste Modelo de Referência, em termos de Metainformação estrutural[773] e de preservação[774], de especificação das Interfaces[775] e para auditoria e certificação[776] têm como fim o desenvolvimento de todo uma estrutura de normalização com o fito de aumentar a confiabilidade e as garantias de confiança nos repositórios digitais.

Esta necessidade de afirmar que o repositório digital é de confiança surge como tentativa de fazer o contraponto aos perigos e riscos derivados da especificidade da informação digital. Implica portanto anteceder-se a estes, identificá-los e medi-los, para que não haja desvios dos resultados expectados, e devem estar baseados no âmbito do risco calculado e "aceitável", como elemento de minimização do perigo.[777]

A confiança baseia-se em expectativas em relação às intenções ou comportamento de outros, seja ela fornecida pela interacção continuada entre as partes, seja pelo sentimento de segurança derivado das estruturas que sustentam uma instituição, seja ela derivada da informação credível que se constitui pela reputação demonstrável/certificação.[778]

No caso específico dos repositórios digitais aplicam-se assim três níveis de confiança, referentes à forma como conquistam a confiança das suas comunidades designadas, como confiam nos fornecedores externos, e como os utilizadores confiam na informação fornecida pelo repositório[779].

Assim, para atingir os seus objectivos, 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, que aceite a responsabilidade da manutenção dos recursos digitais a longo prazo de acordo com os interesses dos depositantes e dos actuais e futuros utilizadores, que demonstre a responsabilidade e sustentação financeira, que o seu planeamento seja de acordo com as recomendações e normas internacionais referentes à gestão, acesso e segurança a longo prazo dos recurso digitais depositados, que defina metodologias para avaliação da qualidade dos

[772] BARBEDO, Francisco - Arquivos digitais: da origem à maturidade, p. 11-12.
[773] METS - Metadata Encoding and Transmission Standard.
[774] GUENTHER, Rebecca et al. - PREMIS Data Dictionary for Preservation Metadata, v 2.2.
[775] ISO 20652:2006, Space data and information transfer systems - Producer-archive interface: methodology abstract standard.
[776] AMBACHER, Bruce et al. - Trustworthy repositories audit & certification: criteria and checklist; ISO 16363:2012, Space data and information transfer systems - Audit and certification of trustworthy digital; ISO/PRF 16919, Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories; DOBRATZ, Susanne [et al.] – NESTOR catalogue of criteria for trusted digital repositories.
[777] GIDDENS, Anthony - As consequëncias da modernidade, p. 35-37.
[778] YOON, Ayoung - End-users' trust in data repositories: definition and influences on trust development, p. 22-23; ROUSSEAU, Denise et al. - Not so different after all: across-discipline view of trust, p. 395.
[779] BEAGRIE, Neil et al - Trusted digital repositories: attributes and responsibilities, p. 9.

sistemas de acordo com as expectativas de confiabilidade da comunidade, e que mantenha políticas, práticas e desempenhos auditáveis e aferidas por entidades independentes.[780]

Tudo isto desemboca num processo de auditoria e certificação, baseadas normas tecnológicas, práticas aceites e mecanismos para autenticação de autoria e precisão do seu conteúdo[781], para a qual deve ser desenvolvidos critérios e/ou requisitos cujo cumprimento seja fonte de confiança.

Para estes processos de auditoria, certificação e análise de risco, têm concorrido uma série de documentos, que em geral, enquadram as características expectáveis dos repositórios digitais em :

- Conformidade com o Modelo de Referência OAIS;
- Responsabilidade administrativa;
- Viabilidade Organizacional;
- Sustentabilidade financeira;
- Adequação tecnológica e procedimental;
- Segurança do sistema
- Prestação de contas procedimental (ligada à certificação.

São assim exemplos, o TRAC e a ISO 16363:2012, o NESTOR; os 10 Princípios, o *Data Seal of Approval*, o *European Framework for Audit and Certification of Digital Repositories,* todos estes no âmbito da certificação, o DRAMBORA referente à avaliação de risco, e o PLATTER, como ferramenta para planificação de repositórios digitais de confiança.

E se no âmbito da certificação emergem tantos documentos com requisitos para auditoria e certificação, que, malgrado as tentativas de compromisso entre as entidades dos quais emanam, acabam por ser concorrenciais. Daí termos considerado importante aventurarmo-nos numa comparação entre os documentos que ponderámos serem os mais utilizados, ou mais amplamente anunciados: o TRAC, a ISO 16363:2012 e o NESTOR. Esta comparação permitiu apurar que o TRAC é um trabalho de charneira, que sistematizou as recomendações mais significativas fornecidas pelos estudos académicos produzidos até então, e contem um conjunto de requisitos a serem usados no âmbito de auditorias. A ISO 16363:2012 revela-se um digno sucessor do TRAC, estendendo o número de requisitos, tendo sido desenvolvido por meio de análises técnicas a repositórios, que entretanto verifica ter uma expansão tanto no número, como nas funcionalidades. Este documento foi produzido como norma internacional a ser utilizada para obtenção, por parte das organizações detentoras de repositórios digitais,

[780] SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais, p. 71. Cft. BEAGRIE, Neil et al - Trusted digital repositories: attributes and responsibilities, p. 5.
[781] PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories, p. 596 e p.603.

de certificação de confiança a nível internacional, requerendo a existência de mecanismos independentes de verificação e de prova documental de todos os procedimentos. Por seu lado, o NESTOR é produto das especificidades do contexto alemão, principalmente no âmbito explícito da gestão de qualidade e da segurança TI. Comparativamente, o NESTOR é menos pormenorizado que o TRAC e a ISO 16363:2012, e, na nossa opinião, estes documentos aparentam englobar implicitamente a maioria dos requisitos no documento alemão. Com base nessa opinião, consideramos que seria possível evoluir para uma situação de consenso que desse origem a uma nova norma internacional que integrasse as disposições de ambos, no sentido de superar os constrangimentos derivados da especificidade jurídico-legal de cada país.

Foi também nesse sentido que se procedeu à avaliação do RODA, aplicando nesse processo esses documentos, com o fito de verificar se o RODA seria digno de confiança para quem o utiliza de acordo com os fins a que este repositório se propõe cumprir.

No entanto, e apesar do que a pesquisa e este trabalho verificaram, é difícil garantir que o cumprimento dos requisitos, acompanhado por processos de auditorias internas e externas tendo como fim a certificação, leve a que, de forma automática, os utilizadores confiem nos repositórios digitais. São conhecidos exemplos de certificação que redundam em procedimentos cristalizados, e que, por vezes, a sua formalização nada tem a ver com as práticas exercidas. E dada a evolução tecnológica, seja em termos de sistema intermediário, seja em termos de formatos e tipologias de informação electrónica, é difícil garantir que o nível de cumprimento dos requisitos se mantenha. Para que tal se verifique, é necessário que haja um investimento constante em Pesquisa, Desenvolvimento e Inovação, na renovação do parque tecnológico e na formação dos recursos humanos que gerem o sistema. Tudo isto implica sustentabilidade financeira e vontade da gestão de topo. E, obviamente, de auditorias internas e externas constantes, e com resultados transparentes. Tudo isto permitirá que a qualidade das práticas e do serviço prestados aos vários utilizadores, clientes, Comunidade Designada (os resultados) iguale, ou mesmo supere, a reputação existente. E assim permitir que o nome do repositório, do organismo responsável e a informação que ele recebe, gere, mantem e fornece possam ser eles próprios considerados sinónimos de confiança.

Referências Bibliográficas

ADOBE - TIFF developer information site [Em linha]. Adobe Systems Incorporated, 2002 [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://partners.adobe.com/public/developer/tiff>

ALLIANCE FOR PERMANENT ACCESS TO THE RECORDS OF SCIENCE NETWORK (APARSEN) - Report on peer review of digital repositories [Em linha]. V.1.0. [S.l.]: APARSEN, 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/04/APARSEN-REP-D33_1B-01-1_0.pdf>

ALEMANHA. Deutsche Initiative für NetzwerkInformation (DINI) Working Group "Electronic Publishing" – DINI certificate document and publication services [Em linha]. v.3.0. Göttingen. DINI: Niedersächsische Staats: Universitätsbibliothek Göttingen, 2010. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://edoc.hu-berlin.de/series/dini-schriften/2010-3-en/PDF/dini-zertifikat-2010-3-en.pdf >

ALLINSON, Julie - OAIS as a reference model for repositories: an evaluation [Em linha]. v 0.5. [S.l.]: UKOLN: JISC, 2006. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.ukoln.ac.uk/repositories/publications/oais-evaluation-200607/Drs-OAIS-evaluation-0.5.pdf>

ALVES, Ivone [et al.] - Dicionário de terminologia arquivística. Lisboa: Instituto da Biblioteca Nacional e do Livro, 1993. ISBN 972-565-146-4

AMBACHER, Bruce [et al.] - An audit checklist for the certification of trusted digital repositories: draft for public comment [Em linha]. Mountain View, Calif.: RLG-NARA Task Force on Digital Repository and Certification; 2005. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://library.oclc.org/cdm/ref/collection/p267701coll33/id/408>

AMBACHER, Bruce [et al.] - Trustworthy repositories audit & certification: criteria and checklist [Em linha]. [S.l.]: RLG-NARA Task Force on Digital Repository and Certification: CRL: OCLC, 2007. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf>

ANSI/NISO Z39.87: 2006, Data Dictionary - Technical metadata for digital still images. ANSI/NISO

ANTÓNIO, Júlio - O sistema de gestão documental: oportunidade do *software* livre nos municípios portugueses [Em linha]. Lisboa: [s.n.], 2008. Tese para obtenção do grau de Mestrado em Ciências da Documentação e Informação pela Faculdade de Letras da Universidade de Lisboa. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://hdl.handle.net/10451/1739>.

ARCHIVAL WORKSHOP PROGRAM COMMITTEE - Archival Workshop on Ingest, Identification, and Certification Standards (AWIICS) draft report [Em linha]. College Park, Md.: NARA, 1999;

rev. 20 Abr. 2004. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://nssdc.gsfc.nasa.gov/nost/isoas/awiics/>

ARCHIVAL WORKSHOP PROGRAM COMMITTEE - Certification of digital archives and preservation methodology: certification input document. In Archival Workshop on Ingest, Identification, and Certification Standards (AWIICS) draft report [Em linha]. College Park, Md.: NARA, 1999; rev. 20 Abr. 2004. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://nssdc.gsfc.nasa.gov/nost/isoas/awiics/CertifBase.ppt>

ARMS, William - Digital libraries [Em linha]. [S.l.]. M.I.T. Press, 2000. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.cs.cornell.edu/wya/diglib/MS1999/index.html>. ISBN 0-262-01180-8

AUSTRÁLIA. National Library of Australia - Preservation metadata for digital collections [Em linha]. [S.l.]: NLA: PANDORA Australia's Web Archive, 1999. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://pandora.nla.gov.au/pan/25498/20020625-0000/www.nla.gov.au/preserve/pmeta.html>

BANAT-BERGER, Françoise [et al.] – L'archivage numérique à long terme. les débuts de la maturité. Paris: Direction des Archives de France; La Documentation française, 2009. ISBN 978-2-11-006942-9

BARBEDO, Francisco - Arquivos digitais: da origem à maturidade. Cadernos BAD. [Em linha]. Nº 2 (2005) p. 6 – 18 [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.bad.pt/publicacoes/index.php/cadernos/article/view/810>. ISSN 0007-9421

BARBEDO, Francisco - RODA+: estratégia para a formação de uma comunidade. Lisboa: DGLAB, 2012. Acessível na Direcção-Geral do Livro, dos Arquivos e das Bibliotecas, Lisboa, Portugal.

BARBEDO, Francisco; CORUJO, Luis; SANT'ANA, Mário – Recomendações para a produção de planos de preservação digital [Em linha]. V2.1. Lisboa: Direcção-Geral de Arquivos, 2011, [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2014/02/Recomend_producao_PPD_V2.1.pdf>.

BARBEDO Francisco [et al.] – RODA: Repositório de Objectos Digitais Autênticos. In Actas do 9º Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas [Em linha]. Ponta Delgada: APBAD, 2007. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/535>

BARBEDO, Francisco; GOMES, Eugénia; HENRIQUES, Cecília - Recomendações para a gestão de documentos de arquivo electrónicos – SIADE 1: contexto de suporte [Em linha]. Lisboa: Instituto dos Arquivos Nacionais/Torre do Tombo: Instituto de Informática, 2000, [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/siade_caderno1.pdf>. ISBN 972-8107-59-5

BARBEDO, Francisco; MARTINS, Sílvia – Preservação digital. Nação e Defesa. Lisboa: Instituto de Defesa Nacional. ISSN 0870-757X. 5ª série, nº133 (2012) p. 167-177.

BARBEDO, Francisco [et al.] – Recomendações para a produção de planos de preservação digital [Em linha]. V1.0. Lisboa: Direcção-Geral de Arquivos, 2008, [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.adporto.pt/ficheiros_a_descarregar/PlanoPreservacaoDigital_v1.0.pdf>.

BEAGRIE, Neil; GREENSTEIN, Daniel – A strategic policy for creating and preserving digital collections : a report to the Digital Archiving Working Group. London: British Library Research and Innovation Centre, 1998. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.ukoln.ac.uk/services/elib/papers/supporting/pdf/framework.pdf>. ISBN 0-7123-9714-0

BEAGRIE, Neil ; JONES, Maggie – Preservation management of digital materials: a handbook [Em linha]. [s.l]: DPC, 2008, [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.dpconline.org/advice/preservationhandbook>. ISBN 978-0712308861

BEAGRIE, Neil, [et al.] - Trusted digital repositories: attributes and responsibilities, an RLG-OCLC report [Em linha]. Mountain View, Calif.: RLG, 2002, [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://oclc.org/content/dam/research/activities/trustedrep/repositories.pdf>.

BEARMAN, David - Collecting software: a new challenge for archives & museums. Archival Informatics Technical Report [Em linha]. Vol. 1, nº 2 (1987). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.archimuse.com/publishing/bearman_col_soft.html>. ISSN 1042-1459

BECHHOFER, Sean [et al.] – SCAPE Final version of policy specification model [Em linha]. [S.l.:s.n.], 2013. [Consult. 16 Set. 2014]. Disponível na Internet: <URL: http://www.scape-project.eu/wp-content/uploads/2013/08/SCAPE_D13.1_UNIMAN_V1.0.pdf >

BECKER, Christoph - Trustworthy preservation planning [Em linha]. Vienna: [s.n], 2010. Tese para obtenção do grau de Doutor em Ciências Técnicas pela Faculdade de Informática da Universidade Técnica de Viena. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://nbn-resolving.de/urn/resolver.pl?urn=urn:nbn:de:0008-2011061603>

BECKER, Christoph; KULOVITS, Hannes; RAUBER, Andreas - Trustworthy preservation planning with Plato. ERCIM news [Em linha]. [S.l.] Nº 80 (2010), p.24-25 [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://ercim-news.ercim.eu/images/stories/EN80/EN80-web.pdf>. ISSN 0926-4981

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>.

BERTALANFFY, Ludwig von – General system theory: foundations, development, applications. New York: George Braziller, 1969. ISBN 978-0-8076-0453-3

BLAU, Peter; SCOTT, W Richard - Formal organizations: a comparative approach. Stanford, Calif.: Stanford University Press, 2003. ISBN 978-0-8047-4890-2

BORBINHA, José – Depósito e preservação na Biblioteca Nacional Digital. In 8º Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas – Nas encruzilhadas da informação e da cultura: (re)inventar a profissão: actas [Em linha]. Lisboa: APBAD, 2004. [Consult. 2013-09-24] Disponível na Internet : <URL: http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/645/642>.

BOWDITCH, James; BUONO, Anthony; STEWART, Marcus - A primer on organizational behavior. 7ª ed. New York: John Wiley & Sons, 2007. ISBN 978-0-4700-8695-7

BRADLEY, Kevin – Defining digital sustainability. Library Trends [Em linha]. Vol. 56, nº 1 (2007), p. 148-163. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL:https://www.ideals.illinois.edu/bitstream/handle/2142/3772/Bradley561.pdf?sequence=2>. ISSN 1559-0682

BRADLEY, Kevin; LEI, Junran; BLACKALL, Chris - Towards an open source repository and preservation system [Em linha]. Paris: UNESCO, 2007. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://unesdoc.unesco.org/images/0015/001547/154761e.pdf>

BRAND, Stewart - Escaping the digital dark. Library Journal [Em linha]. Vol. 124, Nº2 (1999), p. 46-48. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.rense.com/general38/escap.htm>

BULLOCK, Alison - Preservation of digital information: issues and current status. Network Notes [Em linha]. Nº 60 (1999). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://epe.lac-bac.gc.ca/100/202/301/netnotes/netnotes-h/notes60.htm>. ISSN 1201-4338.

BUSH, Vannevar - As we may think. The Atlantic Monthly [Em linha]. Jul. (1945). [Consult. 14 Mar. 2013]. Disponível na Internet: <URL: http://www.theatlantic.com/magazine/print/1945/07/as-we-may-think/303881/>

CABRAL, Maria Luísa - Amanhã é sempre longe demais: crónicas de preservação & conservação. Lisboa: Gabinete de Estudos A&B, 2002. ISBN 972-98827-1-1

CAFÉ, L. [et al.] - Repositórios institucionais: nova estratégia para publicação científica na rede. In Anais do XXVI Congresso brasileiro de ciências da comunicação [Em linha]. Belo Horizonte: INTERCOM. 2003. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.intercom.org.br/papers/nacionais/2003/www/pdf/2003_ENDOCOM_TRABALHO_cafe.pdf >

CANDELA, Leonardo; CASTELLI, Donatella; PAGANO, Pasquale - History, evolution and impact of digital libraries. In IGLEZAKIS, Ioannis, ed. lit.; SYNODINOU, Tatiana-Eleni, ed. lit.; KAPIDAKIS, Sarantos, ed. lit. - E-Publishing and digital libraries: legal and organizational issues.[Em linha]. Hershey, Pa.: IGI Global, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.researchgate.net/publication/229422428_History_Evolution_and_Impact_of_Digital_Libraries/links/09e415110d91b1c40f000000>. ISBN 978-1-60960-031-0

CANDELA, Leonardo [et al.] - The digital library reference model. [Em linha]. V1.0. [S.l.]: DL.org, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://bscw.research-infrastructures.eu/pub/bscw.cgi/d222816/D3.2b%20Digital%20Library%20Reference%20Model.pdf>

CAPLAN, Priscilla [et al.] - Data dictionary for preservation metadata: final report of the PREMIS Working Group [Em linha]. [S.l.]: OCLC/RLG PREMIS Working Group: LOC, 2005. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.loc.gov/standards/premis/v1/premis-dd_1.0_2005_May.pdf>

CASE, Donald – Looking for information. 2ª ed. London: Academic Press: Elsevier, 2007. ISBN 978-0-12-369430-0

CASE, Mary – Framing the issue: open access. ARL: a bimonthly report [Em linha]. Nº 226 (Fev. 2003), pp 8-11. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.arl.org/component/content/article/6/1229>. ISSN 1050-6098

CENTER FOR RESEARCH LIBRARIES (CRL) - Ten principles [Em linha]. Chicago: Center for Research Libraries (CRL), (2007?) [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/core-re>.

CHAMPION, Dean - Sociology of organizations. New York: McGraw-Hill, 1975. ISBN 978-0-07-010492-1

CHECKLAND, Peter; HOLWELL, Sue – Information, systems and information systems: making sense of the field. Chichester: Wiley, 2005. ISBN 978-0471-95820-8

CHEN, Su-Shing - The paradox of digital preservation. Computer [Em linha]. Vol. 34, nº. 3 (Mar. 2001), p. 2-6. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.fpdigital.com/resources/306-the-paradox-of-digital-preservation>. ISSN 0018-9162

CHIAVENATO, Idalberto – Teoria geral da administração. 6ª ed. Rio de Janeiro: Ed. Campus, 2006. ISBN 978-85-352-0849-8

CONWAY, Paul - Preservation in the digital world. [Em linha]. [S.l.]: Council on Library and Information Resources, 1996. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/conway2/>. ISBN 1-887334-49-1

CONWAY, Paul - Preservation in the age of google: digitization, digital preservation, and dilemmas. The library quarterly [Em linha] Vol. 80, nº 1 (2010), p.61–79 [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://deepblue.lib.umich.edu/handle/2027.42/85223>. ISSN 0024-2519

CORNELL UNIVERSITY LIBRARY; INTER-UNIVERSITY CONSORTIUM FOR POLITICAL AND SOCIAL RESEARCH (ICPSR); MIT LIBRARIES - Digital preservation management: implementing short-term strategies for long-term problems (digital preservation management workshops and

tutorial) [Em linha]. Cambridge, Ma.: MIT Libraries, 2003, actual. 2014. [Consult. 6 Mar. 2014]. Disponível na Internet: <URL: http://www.dpworkshop.org/>

CORUJO, Luis – RODA: manual de procedimentos de disseminação. V. 1.1. [S.l.]: Direcção-Geral de Arquivos, 2009

CORUJO, Luis – RODA: manual de procedimentos de ingestão. V. 1.0. [S.l.]: Direcção-Geral de Arquivos, 2009

CORUJO, Luis – RODA: manual de procedimentos de administração. V. 1.0. [S.l.]: Direcção-Geral de Arquivos, 2009

CORUJO, Luis – RODA: manual de procedimentos de gestão de planos de classificação. V. 1.0. [S.l.]: Direcção-Geral de Arquivos, 2009

CROW, Raym - The case for institutional repositories: a SPARC position paper [Em linha]. Washington, DC.: Scholarly Publishing & Academic Resources Coalition, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.sparc.arl.org/sites/default/files/ir_final_release_102.pdf>

DALE, Robin [et al.] - Preservation metadata for digital objects : a review of the state of the art : a white paper [Em linha]. [S.l.]: OCLC/RLG Working Group on preservation metadata, 2001. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.oclc.org/content/dam/research/activities/pmwg/presmeta_wp.pdf?urlm=161396 >

DALE, Robin; GORE, Emily - Process models and the development of trustworthy digital repositories. Information standards quarterly [Em linha]. Vol. 22, nº 2, (2010): p.14-19. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.niso.org/apps/group_public/download.php/4247/FE_Dale_Gore_Trustworthy_Repositories_isqv22no2.pdf>. ISSN 1041-0031

DATA SEAL OF APPROVAL BOARD – DSA Website [Em linha]. [S.l.]: DSA, [2013?]. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://datasealofapproval.org/>

DATA SEAL OF APPROVAL BOARD – DSA guidellines 2014-2015 [Em linha]. v.2. [S.l.]: DSA, 2013. Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://datasealofapproval.org/media/filer_public/2013/09/27/guidelines_2014-2015.pdf>

DATA SEAL OF APPROVAL; ESTADOS UNIDOS. CCDSDS Repository Audit and Certification Working Group; ALEMANHA. DIN Working Group "Trustworthy Archives – Certification" – European framework for audit and certification of digital repositories [Em linha]. [S.l.]: DAS: CCSDS: DIN. [2010?]. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.trusteddigitalrepository.eu/>

DAY, Michael - CEDARS guide to preservation metadata [Em linha]. Leeds: CEDARS, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.webarchive.org.uk/wayback/archive/20050410120000/http://www.leeds.ac.uk/cedars/guideto/metadata/guidetometadata.pdf>.

DECRETO-LEI nº 290-D/99. D.R. I Série. 176 Suplemento (1999-08-02) 4990 (2-10)

DECRETO-LEI nº 62/2003. D.R. I Série. 79 (2003-04-03) 2170-2185

DECRETO-LEI nº 165/2004. D.R. I Série. 157 (2004-07-06) 4072-4073

DECRETO-LEI nº 116-A/2006. D.R. I Série. 115 2º Suplemento (2006-06-16) 4330 (4-8)

DECRETO-LEI nº 88/2009. D.R. I Série. 70 (2009-04-9) 2159-2175

DECRETO REGULAMENTAR nº 25/2004. D.R. I Série. 165 (2004-07-15) 4269-4278

DELOS ASSOCIATION - Digital libraries: future directions for a european research programme: DELOS brainstorming report [Em linha]. San Cassiano: DELOS Network of Excelence. 2001. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://delos-noe.isti.cnr.it/activities/researchforum/Brainstorming/1st-ws.html>

DINAMARCA. Statsbiblioteket; UNIVERSITY OF GLASGOW. Humanities Advanced Technology and Information Institute (HATII) - Repository planning checklist and guidance (Planning tool for trusted electronic repositories - PLATTER) [Em linha]. [S.l.]: DPE: HATII, 2008. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.digitalpreservationeurope.eu/platter.pdf>

DLM Forum - European Commission introduction: the DLM-Forum, MoReq and the European Commission [Em linha]. [S.l.]: DLM-Forum, [2005?]. Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://dlmforum.typepad.com/History_of_DLM_Forum_and_MoReq.pdf>

DOBRATZ, Susanne [et al.] – NESTOR catalogue of criteria for trusted digital repositories [Em linha]. v.1. Frankfurt am Main: Network of Expertise for Long-Term STORage and Long-Term Availability of Digital Resources in Germany, 2006. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://files.d-nb.de/nestor/materialien/nestor_mat_08-eng.pdf>.

DOBRATZ, Susanne; SCHOGER, Astrid; STRATHMANN, Stefan - The NESTOR catalogue of criteria for trusted digital repository evaluation and certification. JODI: journal of digital information [Em linha]. Vol. 8, nº 2. (2007). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://journals.tdl.org/jodi/index.php/jodi/article/view/199/180>. ISSN 1368-7506

DOBRATZ, Susanne; SCHOGER, Astrid - Trustworthy digital long-term repositories: the NESTOR approach in the context of international developments. Research and advanced technology for digital libraries [Em linha]. Vol. 4675, (2007), p. 210–222. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://link.springer.com/chapter/10.1007%2F978-3-540-74851-9_18>. ISSN 978-3-540-74850-2

DOBRATZ, Susanne; SCHOLZE, Frank. - DINI institutional repository certification and beyond. Library hi tech [Em linha]. Vol 24, nº 4 (2006), p. 583-594. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.emeraldinsight.com/journals.htm?articleid=1583893>. ISSN 0737-8831

DUNN, John - Trust and political agency. In GAMBETTA, Diego, ed. lit. - Trust: making and breaking cooperative relations. [Em linha] Oxford: Basil Blackwell, 1988. [Consult. 24 Nov.

2013]. Disponível em WWW: <URL: http://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf>. ISBN 0-631-15506-6

DURANTI, Luciana - The long-term preservation of authentic electronic records. In Proceedings of the 27th very large data bases conference [Em linha]. Roma: Morgan Kaufmann. 2001. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.vldb.org/conf/2001/P625.pdf>. ISBN 1-55860-804-4

DURANTI, Luciana, ed. lit.; PRESTON, Randy, ed. lit. - International research on permanent authentic records in electronic systems (InterPARES) 2: experiential, interactive and dynamic records [Em linha]. Padova: Associazione Nazionale Archivistica Italiana, 2008. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.interpares.org/display_file.cfm?doc=ip2_book_complete.pdf>.

DUREAU, J.M.; CLEMENS D. W. G. - Princípios para a preservação e conservação de espécies bibliográficas. Lisboa: Biblioteca Nacional, 1992. ISBN 972-565-155-3

Encoded Archival Description [Em linha] [S.l.]: Library of Congress, 2002 [Consult. 11 Nov. 2013]. Disponível na Internet: < http://www.loc.gov/ead>

ESTADOS UNIDOS DA AMÉRICA. Consultative Committee for Space Data Systems - Audit and certification of trustworthy digital repositories - magenta book [Em linha]. Washington, DC.: National Aeronautics and Space Administration, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: < http://public.ccsds.org/publications/archive/652x0m1.pdf>.

ESTADOS UNIDOS DA AMÉRICA. Consultative Committee for Space Data Systems - Producer-archive interface methodology abstract standard - magenta book [Em linha]. Washington, DC.: National Aeronautics and Space Administration, 2004. [Consult. 11 Nov. 2013]. Disponível na Internet: < http://public.ccsds.org/publications/archive/651x0m1.pdf >.

ESTADOS UNIDOS DA AMÉRICA. Consultative Committee for Space Data Systems - Reference model for an open archival information system (OAIS) - blue book [Em linha]. Washington, DC.: National Aeronautics and Space Administration, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <http://public.ccsds.org/publications/archive/650x0b1s.pdf>.

ESTADOS UNIDOS DA AMÉRICA. Consultative Committee for Space Data Systems - Reference model for an open archival information system (OAIS) - magenta book [Em linha]. Washington, DC.: National Aeronautics and Space Administration, 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://public.ccsds.org/publications/archive/650x0m2.pdf>

ESTADOS UNIDOS DA AMÉRICA. Consultative Committee for Space Data Systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories - magenta book [Em linha]. V. 1. Washington, DC.: National Aeronautics and Space Administration, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://public.ccsds.org/publications/archive/652x1m1s.pdf >

ESTADOS UNIDOS DA AMÉRICA. Consultative Committee for Space Data Systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories - magenta book [Em linha]. V. 2. Washington, DC.: National Aeronautics and Space Administration, 2014. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://public.ccsds.org/publications/archive/652x1m2.pdf >

ESTADOS UNIDOS DA AMÉRICA. Library of Congress - MPEG-2 encoding family. In Sustainability of digital formats planning for Library of Congress collections [Em linha]. [S.l.]: Library of Congress, 2012, rev. 13 Fev. 2014. [Consult. 11 Mar. 2014. Disponível na Internet: <URL: http://www.digitalpreservation.gov/formats/fdd/fdd000335.shtml>

ESTADOS UNIDOS DA AMÉRICA. Library of Congress - WAVE audio file format. In Sustainability of digital formats planning for Library of Congress collections [Em linha]. [S.l.]: Library of Congress, 2012, rev. 17 Out. 2013. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.digitalpreservation.gov/formats/fdd/fdd000001.shtml>

FARIA, Luís - Desafios práticos à preservação digital: RODA e SCAPE. In Seminário o ambiente digital aberto : desafios e impactos [Em linha]. Braga: Biblioteca Lúcio Craveiro da Silva, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorium.sdum.uminho.pt/handle/1822/17853>

FARIA, Luis - Ingest with RODA : the present and the future of repository ingest. In Digital preservation summit 2011 [Em linha]. Hamburg, Alemanha. ,2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorium.sdum.uminho.pt/handle/1822/17847>

FARIA, Luis - Supporting the preservation lifecycle in repositories. In International conference on open repositories [Em linha]. [S.l.], 2013. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://or2013.net/sessions/supporting-preservation-lifecycle-repositories>

FARIA, Luis, CASTRO, Luis – RODA Repositório de Objectos Digitais Autênticos: relatório final [em linha]. Lisboa: Direcção Geral de Arquivos e Universidade do Minho, 2007 [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/roda_relatorio.pdf>

FARIA, Luis [et al.] - RODA : a service-oriented repository to preserve authentic digital objects. In International conference on open repositories [Em linha]. [S.l.:s.n.], 2009. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://hdl.handle.net/1822/9408>

FARIA, Luis [et al.] - Automatic preservation watch using information extraction on the Web: a case study on semantic extraction of natural language for digital preservation. In International conference on preservation of digital objects iPRES 2013 [Em linha]. [S.l.:s.n.], 2013. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorium.sdum.uminho.pt/handle/1822/25214>

FARIA, Maria Isabel; PERICÃO, Maria da Graça - Dicionário do livro: da escrita ao livro electrónico. Coimbra: Edições Almedina, 2008. ISBN 978-972-40-3499-7

FERREIRA, Carla - Preservação da informação digital : uma perspectiva orientada para as bibliotecas [Em linha]. Coimbra : [s.n], 2011. [Consult. 11 Nov. 2013]. Tese de Mestrado em Informação, Comunicação e Novos Media apresentada à Faculdade de Letras da Universidade de Coimbra. Disponível na Internet: <URL:http://hdl.handle.net/10316/15001>

FERREIRA, Miguel – RODA: descrição do sistema. V. 0.5. [S.l.]: Direcção-Geral de Arquivos, 2009

FERREIRA, Miguel - Introdução à preservação digital : conceitos, estratégias e actuais consensos [Em linha]. Guimarães: Escola de Engenharia da Universidade do Minho, 2006. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL:http://hdl.handle.net/1822/5820>. ISBN 972-8692-30-7

FERREIRA, Miguel – Preservação de longa duração de informação digital no contexto de um arquivo histórico. [Em linha]. Guimarães : [s.n.], 2009. Tese de doutoramento em Tecnologias e Sistemas de Informação (Sociedade da Informação) apresentada à Escola de Engenharia da Universidade do Minho. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL:http://repositorium.sdum.uminho.pt/handle/1822/9563>.

FERREIRA, Miguel - Certificação de repositórios digitais. In Seminário (r)evolução da informação pública : preservar, certificar e acessibilizar [Em linha]. Lisboa; DGARQ, 2011. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL:http://repositorium.sdum.uminho.pt/handle/1822/19412>

FERREIRA, Miguel; BAPTISTA, Ana Alice; RAMALHO, José Carlos - A Foundation for automatic digital preservation. Ariadne [Em linha]. Nº 48 (2006). [Consult. 24 Nov. 2013]. Disponível na Internet: <URL:http://www.ariadne.ac.uk/issue48/ferreira-et-al>. ISSN 1361-3200

FERREIRA, Miguel, BAPTISTA, Ana Alice, RAMALHO, José Carlos - CRIB : a service oriented architecture for digital preservation outsourcing. In Actas XATA: XML: aplicações e tecnologias associadas, Portalegre, 2006. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL:http://repositorium.sdum.uminho.pt/handle/1822/4457>. ISBN 972-99166-2-4

FERREIRA, Miguel, SARAIVA, Ricardo; RODRIGUES, Eloy - Estado da arte em preservação digital: Relatório sobre o estado da arte em preservação digital desenvolvido no âmbito do projeto Repositório Científico de Acesso Aberto de Portugal (RCAAP) [Em linha]. [S.l.]: RCAAP: Universidade do Minho, 2012. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://repositorium.sdum.uminho.pt/handle/1822/17049>

FERREIRA, Miguel [et al.] – SCAPE Report on compliance validation. [S.l.:s.n.], 2014.

FOX, Edward - The digital libraries initiative: update and discussion. Bulletin of the America Society of Information Science [Em linha]. Vol. 26, Nº 1, (1999). [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.asis.org/Bulletin/Oct-99/fox.html>. ISSN 1550-8366

G8 SCIENCE MINISTERS STATEMENT: news story. In GOV.UK [Em linha] 2013. [Consult. 16 jun. 2013]. Disponível na Internet: <URL:https://www.gov.uk/government/news/g8-science-ministers-statement>

GAMBETTA, Diego - Can we trust trust? In GAMBETTA, Diego, ed. lit. - Trust: making and breaking cooperative relations. [Em linha] Oxford: Basil Blackwell, 1988. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf>. ISBN 0-631-15506-6

GLADNEY, Henry - Perspectives on trustworthy information. Digital document quarterly. [Em linha]. Vol. 1, nº 1 (2002). [Consult. 24 Nov. 2013]. Disponível na Internet: <URL: http://www.hgladney.com/ddq_1_1.htm>. ISSN 1547-8610

GLADNEY, Henry – Preserving digital information [Em linha]. New York : Springer. 2007. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://link.springer.com/book/10.1007%2F978-3-540-37887-7>. ISBN 978-3-540-37887-7

GLADNEY, Henry - Trustworthy 100-year digital objects: evidence after every witness is dead. Journal ACM transactions on information systems [Em linha]. Vol. 22, nº 3 (2004), p. 406–436. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL:http://dl.acm.org/citation.cfm?doid=1010614.1010617>. ISSN 1046-8188

GIARETTA, David; HARMSEN, Henk; KEITEL, Christian – Memorandum of understanding to create a european framework for audit and certification of digital repositories [Em linha]. [S.l.]: DAS: CCSDS: DIN. 2010. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL: http://www.trusteddigitalrepository.eu/Site/Memorandum%20of%20Understanding.html>

GIDDENS, Anthony - As conseqüências da modernidade. São Paulo: UNESP, 1991. ISBN 85-7139-022-3

GRANGER, Stewart - Digital preservation and deep infrastructure. D-Lib magazine. Vol. 8, nº2 (2002). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL:http://www.dlib.org/dlib/february02/granger/02granger.html>. ISSN 1082-9873

GUENTHER, Rebecca [et al.] - PREMIS data dictionary for preservation metadata [Em linha]. V. 2.0. [S.l.]: PREMIS Editorial Commitee: LOC, 2008. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.loc.gov/standards/premis/v2/premis-2-0.pdf >

GUENTHER, Rebecca [et al.] - PREMIS data dictionary for preservation metadata [Em linha]. V. 2.2. [S.l.]: PREMIS Editorial Commitee: LOC, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.loc.gov/standards/premis/v2/premis-2-2.pdf >

GUENTHER, Rebecca [et al.] - PREMIS data dictionary for preservation metadata [Em linha]. V. 2.1. [S.l.]: PREMIS Editorial Commitee: LOC, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.loc.gov/standards/premis/v2/premis-2-1.pdf >

HALL, Richard; TOLBERT, Pamela - Organizations: structure, processes, and outcomes. 10th ed. Upper Saddle River, N.J.: Pearson, 2009. ISBN 978-0132448406

HARMSEN, Henk [et al.] - Explanatory notes on the NESTOR seal for trustworthy digital archives [Em linha]. Frankfurt am Main, Alemanha: Network of Expertise for Long-Term STORage and Long-Term Availability of Digital Resources in Germany, 2013. [Consult. 11 Nov.

2013]. Disponível na Internet: <URL: http://files.d-nb.de/nestor/materialien/nestor_mat_17_eng.pdf>

HARVARD UNIVERSITY. Harvard Library - Global Digital Format Registry [Em linha]. Cambridge, MA, EUA: Harvard Library, [2013?]. [Consult. 24 Nov. 2013]. Disponível na Internet: < URL:http://library.harvard.edu/preservation/digital-preservation_gdfr.html>

HEDSTROM, Margaret - Digital preservation: a time bomb for digital libraries. Computers and the humanities. [Em linha]. Vol. 31, nº 3 (1997), p. 189-202. [Consult. 6 Mar. 2014] Disponível na Internet: <URL: http://www.uky.edu/~kiernan/DL/hedstrom.html>. ISSN 1572-8412

HEDSTROM, Margaret - Digital preservation: problems and prospects. Digital Library Network (DLnet) [Em linha]. Nº 20 (2001). [Consult. 6 Mar. 2014] Disponível na Internet: <URL: http://www.dl.slis.tsukuba.ac.jp/DLjournal/No_20/1-hedstrom/1-hedstrom.html>.

HEERY, Rachel; ANDERSON, Sheila - Digital repositories review [Em linha]. [S.l.]: Joint Information Systems Committee, 2005. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL: http://www.jisc.ac.uk/uploaded_documents/digital-repositories-review-2005.pdf>.

HENDLEY, Tony – Comparison of methods and costs of digital preservation: British Library research and inovation report 106 [Em linha]. [S.l.]: British Library Research and Innovation Centre, 1998. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL:http://www.ukoln.ac.uk/services/elib/papers/tavistock/hendley/hendley.html>. ISBN 0-7123-9713-2

HENRIQUES, Cecília - Preservação digital: uma perspectiva arquivística. In BORBINHA, José L. [et al.] - Manifesto para a preservação digital. [Em linha]. [Lisboa: APBAD, 2002]. [Consult. 24 Nov. 2013]. Disponível na Internet: <URL: http://www.apbad.pt/CadernosBAD/Caderno22002/Borbinha.pdf >

HENRIQUES, Cecília [et al.] - Recomendações para a gestão de documentos de arquivo electrónicos: SIADE 2. modelo de requisitos para a gestão de arquivos electrónicos [Em linha]. Lisboa: Instituto dos Arquivos Nacionais/Torre do Tombo: Instituto de Informática, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/siade_caderno2.pdf>.

HENRIQUES, Cecília – RODA: política de preservação digital. V. 1.0. [S.l.]: Direcção-Geral de Arquivos, 2009

HESLOP, Helen; DAVIS, Simon; WILSON, Andrew - An approach to the preservation of digital records [Em linha]. Camberra: National Archives of Australia, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.naa.gov.au/Images/An-approach-Green-Paper_tcm16-47161.pdf>.

HOFMAN, Hans - Can bits and bytes be authentic? Preserving the authenticity of digital objects. In IFLA annual Conference, 2002 -- IFLA conference proceedings [Em linha]. Glasgow: IFLA, [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://eprints.erpanet.org/39/01/hofman_glasgow02.pdf>.

HOCKX-YU, Helen – Digital preservation in the context of institutional repositories [Em linha]. Program: electronic library and information systems [Em linha]. Vol. 40, nº3 (2006). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://eprints.rclis.org/8189/>. ISSN 0033-0337

HOFSTEDE, Geert – Culturas e organizações. [S.l.]: Edições Sílabo, 2003. ISBN 0-07-707474-2

HOU, Chien-Yi; WOJCIK, Caryn; MARCIANO, Richard - Trusted digital repository design: a policy-driven approach. In Archiving conference: final program and proceedings: 2001 [Em linha]. [S.l.]:Society for Imaging Science and Technology. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://salt.unc.edu/DCAPE/docs/Conferences/archiving_2011.pdf>

HURLEY, Bernard [et al.] - The Making of America II testbed project: A digital library service model [Em linha]. Washington, D.C.: Council on Library and Information Resources, 1999. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/reports/pub87/pub87.pdf>. ISBN 1-887334-72-6

INFOPÉDIA. Dicionários Porto Editora [Em linha] [2013?]. Porto Editora. [Consult. 16 jun. 2013]. Disponível na Internet: <URL: http://www.infopedia.pt/>

INNOCENTI, Perla [et al.] - Towards a holistic approach to policy interoperability in digital libraries and digital repositories. The international journal of digital curation [Em linha]. Vol. 6, nº 1 (2011), p. 111-124. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.ijdc.net/index.php/ijdc/article/view/167>. 124 ISSN 1746-8256

INNOCENTI, Perla [et al.] - SHAMAN requirements analysis report (public version) and specification of the SHAMAN assessment framework and protocol [Em linha]. [S.l.]: SHAMAN Project, 2009. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL:http://shaman-ip.eu/sites/default/files/SHAMAN_D1.2_Requirements%20analysis%20report_0.pdf>

INTERNATIONAL COUNCIL ON ARCHIVES. Committee on Electronic Records - Guide for managing electronic records from an archival perspective [Em linha]. Paris: ICA, 1997 [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.ica.org/download.php?id=1631>. ISBN 0-9682361-0-3

INTERNATIONAL COUNCIL ON ARCHIVES. Committee on Electronic Records - Documentos de arquivo electrónicos: manual para arquivistas [Em linha]. Paris; Lisboa: International Council on Archives: Instituto dos Arquivos Nacionais/Torre do Tombo, 2005. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2013/10/ica_estudo16.pdf>.

INTERPARES Project. Glossary Task Force - The InterPARES glossary [Em linha]. Vancouver: Interpares, 2001 [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.interpares.org/ip1/ip1_documents.cfm?cat=gtf>.

INTERPARES Project - InterPARES 2 terminology database [Em linha]. Vancouver: InterPARES, [2006?]. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.interpares.org/ip2/ip2_terminology_db.cfm>.

INTERPARES Project - InterPARES 3 terminology database [Em linha]. Vancouver: InterPARES, [2012?]. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.interpares.org/ip3/ip3_terminology_db.cfm>.

IOANNIDIS, Yannis - Digital libraries at a crossroads. International journal on digital libraries [Em linha]. Vol. 5, nº 4 (2005), p. 255-265. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://link.springer.com/article/10.1007%2Fs00799-004-0098-4>. ISSN 1432-1300

ISO 15489-1: 2001, Information and documentation -- Records management: Part 1: General. Geneva. ISO

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

ISO/PRF 16919, Space data and information transfer systems - Requirements for bodies providing audit and certification of candidate trustworthy digital repositories. Geneva. ISO

ISO 19005-1:2005, Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1). Geneva. ISO

ISO 20652:2006, Space data and information transfer systems - Producer-archive interface: Methodology abstract standard. Geneva. ISO

ISO 27001:2013, Information technology - Security techniques - Information security management systems – Requirements. Geneva. ISO

HENRIQUES, Marta [et al.] - Bidirectional conversion between XML documents and relational data bases. In International conference on CSCW in design [Em linha]. [S.l.:s.n.], 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorium.sdum.uminho.pt/handle/1822/601>

JISC - Repositories Support Project [Em linha]. [S.l.] : JISC, [2006-2013?]. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.rsp.ac.uk/>.

KEITEL, Christian - DIN standard 31644 and NESTOR certification. In Cultural heritage on line international conference 2012 [Em linha]. Florence: Fondazione Rinascimento Digitale, 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://93.63.166.138:8080/dspace/handle/2012/99 >

KINGSLEY, Danny - Those who don't look don't find: disciplinary considerations in repository advocacy [em linha]. [S.l.:s.n.] [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://hdl.handle.net/1885/46229>.

KRAXNER, Michael [et al.] - The SCAPE planning and watch suite : supporting the preservation lifecycle in repositories. In International conference on preservation of digital objects iPRES 2013 [Em linha]. [S.l.:s.n.], 2013. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorium.sdum.uminho.pt/handle/1822/25215>

KULMUKHAMETOV, Artur; PETROV, Petar - C3PO Clever, Crafty Content Profiling of Objects [Em linha]. [S.l.]: Vienna University of Technology [2012?], rev. 25 Fev. 2014. [Consult. 11 Mar. 2014]. Disponível na Internet: <URL: http://ifs.tuwien.ac.at/imp/c3po>

KUNY, Terry - A digital dark ages? Challenges in the preservation of electronic information. In IFLA Council and General Conference, 63 , 1997 - IFLA conference proceedings [Em linha]. [S.l.]: IFLA, [1997?]. [Consult. 6 Mar. 2014]. Disponível na Internet: <URL: http://archive.ifla.org/IV/ifla63/63kuny1.pdf>.

LASZLO, Krisztina; MCMILLAN, Timothy, YUHASZ, Jennifer - The InterPARES 3 project: implementing digital records preservation in a contemporary art gallery and ethnographic museum. In Annual conference of the International Documentation Committee of the International Council of Museums [Em linha]. Atenas: CIDOC, 2008. [Consult. 6 Mar. 2014]. Disponível na Internet: <URL: http://www.interpares.org/display_file.cfm?doc=ip3_canada_dissemination_cp_laszlo_et-al_cidoc_2008.pdf>

LAVOIE, Brain - The Open Archival Information System reference model: introductory guide [Em linha]. Dublin, Ohio: Digital Preservation Coalition: Online Computer Library Center, 2004. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.dpconline.org/index.php?option=com_docman&task=doc_download&gid=347>

LAVOIE, Brain [et al.] - Preservation metadata and the OAIS information model: a metadata framework to support the preservation of digital objects [Em linha]. Dublin, Ohio: OCLC/RLG Working Group on preservation metadata, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.oclc.org/content/dam/research/activities/pmwg/pm_framework.pdf?urlm=161391 >

LAVOIE, Brain; GARTNER, Richard - Preservation metadata [Em linha]. v.1. [S.l.]: Digital Preservation Coalition: Oxford University Library Services: Online Computer Library Center, 2005. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.dpconline.org/docs/reports/dpctw05-01.pdf>

LAWRENCE, Gregory W. [et al.] - Risk management of digital information: a file format investigation [Em linha]. Washington, DC.: Council on Library and Information Resources, 2000. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/reports/pub93/pub93.pdf>. ISBN 1-887334-78-5

LEE, Kyong-Ho, [et al.] - The state of the art and practice in digital preservation. Journal of research of the National Institute of Standards and Technology [Em linha]. Vol. 107, nº 1 (2002), p. 93-106. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: https://ia600705.us.archive.org/23/items/jresv107n1p93/jresv107n1p93_A1b.pdf>. ISSN 2165-7254

LUHMANN, Niklas – Introduction to systems theory. Cambridge: Polity Press, 2013. ISBN 978-0-7456-4572-8

LUHMANN, Niklas - Familiarity, confidence, trust: problems and alternatives. In: GAMBETTA, Diego, ed. lit. - Trust: making and breaking cooperative relations. [Em linha] Oxford: Basil Blackwell, 1988. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf>. ISBN 0-631-15506-6

LUPOVICI, Catherine; MASANÈS, Julien - Metadata for the long term preservation of electronic publications [Em linha]. The Hague: NEDLIB Consortium, 2000. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.kb.nl/sites/default/files/docs/NEDLIBmetadata.pdf>. ISBN 90-6259-146-9

LUSENET, Yola de - Digital heritage for the future. Cadernos BAD. Lisboa. ISSN 0007-9421. Nº 2 (2002) p.15-27.

LYNCH, Clifford - Institutional repositories: essential infrastructure for scholarship in the digital age. ARL: a bimonthly report [Em linha]. Nº 226 (Fev. 2003), p. 1-7. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.arl.org/component/content/article/6/1229>. ISSN 1050-6098

LYNCH, Clifford - Authenticity and integrity in the digital environment: an exploratory analysis of the central role of trust. In Authenticity in a digital environment [Em linha]. Washington, DC.: Council on Library and Information Resources, 2000. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/pub92/pub92.pdf/view>. ISBN 1-887334-77-7

MÁRDERO ARELLANO, Miguel - Critérios para a preservação digital da informação científica [Em linha]. Brasília: [s.n.], 2008. Tese submetida ao programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito parcial para obtenção do grau de Doutor em Ciência da Informação. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorio.unb.br/handle/10482/1518>

MARTINS, Ernesto - O repositório: imagem de marca e objeto de aprendizagem em meio digital. In III Conferência do IPCB sobre o livre acesso ao conhecimento científico – O desafio da publicação em meio científico: como, onde, porquê? – Livro de resumos [Em linha]. Castelo Branco: Instituto Politécnico de Castelo Branco, 2013. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorio.ipcb.pt/handle/10400.11/1766>. ISBN 978-989-8196-28-6

MARTINS, Francisco – Preservação digital: novos desafios na justiça. Revista do Ministério Público [Em linha]. Nº 131 (2012) p. 171-189. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://rmp.smmp.pt/wp-content/uploads/2012/10/8.RMP_N131_FRANCISCO-MARTINS.pdf>

MARYNIAK, Cathy [et al.] - Definitions of digital preservation [Em linha]. Chicago: ALA, 2007. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.ala.org/ala/mgrps/divs/alcts/resources/preserv/defdigpres0408.pdf>.

MCGOVERN, Nancy - A digital decade: where have we been and where are we going in digital preservation? RLG DigiNews [Em linha]. Vol. 11, nº 1 (2007). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://deepblue.lib.umich.edu/handle/2027.42/60441>. ISSN 1093-5371

MCGOVERN, Nancy - Principles and good practice for preserving data: interuniversity Consortium for Political and Social Research working paper [Em linha]. 2009. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.ihsn.org/home/sites/default/files/resources/IHSN-WP003.pdf>.

MCHUGH, Andrew [et al.] – Digital repository audit method based on risk assessment: DRAMBORA [Em linha]. [S.l.]: DCC: DPE, 2007. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.repositoryaudit.eu/download>. ISBN 978-1-906242-00-8

MCHUGH, Andrew [et al.] - Bringing self-assessment home: repository profiling and key lines of enquiry within DRAMBORA. The international journal of digital curation. Vol. 3, nº 2 (2008) p. 130-142. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://dx.doi.org/10.2218/ijdc.v3i2.64>. ISSN 1746-8256

MERRIAN-WEBSTER DICTIONARY. In Merriam Webster web site [Em linha]. 2013. [Consult. 16 jun. 2013]. Disponível na Internet: <URL: http://www.merriam-webster.com/>

METS - Metadata Encoding and Transmission Standard [Em linha]. [S.l.]: LOC, 2007, actual. 2010?. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.loc.gov/standards/mets/mets-home.html>

METS – METS schema [Em linha]. V1.10 [S.l.]: LOC, 2013. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.loc.gov/standards/mets/mets.xsd>

MIRANDA, Geraldo – Organização e métodos. 5ª ed. São Paulo: Atlas, 1981

MITCHAM, Jenny; HARMAN, Catherine - ADS and the Data Seal of Approval: case study for the DCC. In DCC online. [Em linha]. [S.l.]: DCC, 2011. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.dcc.ac.uk/resources/case-studies/ads-dsa>

NILSSON, Hans [et al.] - Final report of the EESSI expert team [Em linha], [S.l.]: European Electronic Signature Standardization Initiative, 1999. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://cryptome.org/eessi.htm>

NP 4041: 2005, Informação e Documentação - Terminologia arquivística. Conceitos básicos. IPQ

NP 4438-1:2005, Informação e Documentação - Gestão de documentos de arquivo: parte 1: Princípios Directores. IPQ

OWEN, John Mackenzie – Preserving the digital heritage: roles and responsibilities for heritage repositories [Em linha]. In Preserving the digital heritage : principles and policies. The Hague: UNESCO: European Commission on Preservation and Access, 2007. [Consult. 03 Mar. 2014]. Disponível em WWW: <URL: www.ica.org/download.php?id=613>. ISBN 978-90-6984-523-4

PAÍSES BAIXOS. Nationaal Archief - Digital preservation testbed white paper: migration: context and current status [Em linha]. The Hague: ICTU, 2001. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.nationaalarchief.nl/sites/default/files/docs/kennisbank/migration_0.pdf>

PETROV, Petar; BECKER, Christoph - Large-scale content profiling for preservation analysis. In International Conference on Preservation Of Digital Objects iPRES 2012 [Em linha]. [S.l.:s.n.] 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://ifs.tuwien.ac.at/~petrov/publications/c3po-poster-ipres12.pdf>

PINTO, Maria Manuela Gomes de Azevedo – Do «efémero» ao «sistema de informação» : a preservação na era digital. Páginas a&b [Em linha]. Nº 15 (2005), p.53-178. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://hdl.handle.net/10216/13432>. ISSN 0873-5670.

PINTO, Maria Manuela Gomes de Azevedo - Gestão da informação e preservação digital: uma perspectiva portuguesa de uma mudança de paradigma. In Nuevas perspectivas para la difusión y organización del conocimiento: actas del IX Congreso Isko-España [Em linha]. [S.l.:s.n.], 2009. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://dialnet.unirioja.es/servlet/articulo?codigo=2923189>. ISBN 978-84-8363-397-7

PINTO, Maria Manuela Gomes de Azevedo - PRESERVMAP: um roteiro da preservação na era digital. Porto: Edições Afrontamento; CETAC.MEDIA, 2009. ISBN 978-972-36-1070-3

PORTUGAL. Biblioteca Nacional – BND: Biblioteca Nacional Digital [Em linha]. Lisboa: Biblioteca Nacional, 2002, [actual. 2014?]. [Consult. 25 Mar. 2014]. Disponível na Internet: <URL: http://bnd.bn.pt>

PREMIS – 2013 PREMIS Implementation Fair (PIF) minutes [Em linha]. Lisboa: PREMIS: LOC, 2013. [Consult. 6 Mar. 2014]. Disponível na Internet: <URL: http://www.loc.gov/standards/premis/premis-implementation-fair-minutes-2013.docx>

PRIETO, Adolfo - From conceptual to perceptual reality: trust in digital repositories. Library Review [Em linha]. Vol.58, nº 8 (2009), p. 593-606. [Consult. 25 Mar. 2014]. Disponível na Internet: <URL: http://www.emeraldinsight.com/journals.htm?articleid=1810441>. ISSN 0024-2535

RAMALHO, José Carlos - Repositórios digitais. In Pesquisa de informação e inteligência artificial: 3ª Tertúlia em Inteligência Artificial (TeIA) [Em linha]. Porto: [s.n.], 2007. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://repositorium.sdum.uminho.pt/handle/1822/7382>

RAMALHO, José Carlos - RODA : repositório de objectos digitais autênticos. In (R)evolução da informação pública : preservar, certificar e acessibilizar. Lisboa: Direção-Geral de Arquivos, Torre do Tombo, 2011. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://hdl.handle.net/1822/17849>

RAMALHO, José Carlos [et al.] - RODA and CRiB a service-oriented digital repository. In International conference on preservation of digital objects iPRES 2008. [S.l.:s.n.], 2008. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://hdl.handle.net/1822/8226>

RAUBER, Andreas; ASCHENBRENNER, Andreas - Part of our culture is born digital: on efforts to preserve it for future generations. TRANS - Internet-Zeitschrift für Kulturwissenschaften [Em linha]. Nº 10, (2001). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.ifs.tuwien.ac.at/~aola/publications/trans10>. ISSN 1560-182X

RAYMOND, Eric - Bit rot. In The Jargon File [Em linha] Version 4.4.7. Actual. 29 Dez. 2003. [Consult. 6 Jan. 2014]. Disponível na Internet: <URL:http://www.catb.org/jargon/html/B/bit-rot.html>.

RECKER, Astrid - The preservation of digital objects in german repositories: three case studies. Cologne: NESTOR, 2010. Tese de Mestrado em Biblioteca e Ciências da Informação da Faculdade de Ciências da Informação e Comunicação da Escola Superior Técnica de Colónia [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.langzeitarchivierung.de/Subsites/nestor/SharedDocs/Downloads/edition/03_recker.pdf>

REINO UNIDO. Public Record Office - Management, appraisal and preservation of electronic records: principles [Em linha]. 2nd. ed. Kew: Public Record Office, 1999. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://collections.europarchive.org/tna/20080108103210/http:/www.nationalarchives.gov.uk/documents/principles.pdf>.

REINO UNIDO. Public Record Office - Requirements for electronic records management systems: 1: functional requirements [Em linha]. Kew: Public Record Office, 2002. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.nationalarchives.gov.uk/documents/requirementsfinal.pdf>

REINO UNIDO. National Archives – PRONOM: the technical registry [Em linha]. Kew: The National Archives. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.nationalarchives.gov.uk/PRONOM/Default.aspx>

RDF - Resource Description Framework [Em linha]. [S.l.]: World Wide Web Consortium, 2004, [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.w3.org/RDF/>

RODA Community [Em linha]. [S.l.]: KEEP Solutions, 2012. [Consult. 24 Nov. 2013]. Disponível em WWW: <URL: http://www.roda-community.org/>

ROSS, Seamus; HUGH, Andrew - The role of evidence in establishing trusting repositories. D-Lib magazine. Vol. 12, nº7/8 (2006). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL:http://www.dlib.org/dlib/july06/ross/07ross.html>. ISSN 1082-9873

ROTHENBERG, Jeff - Avoiding technological quicksand: finding a viable technical foundation for digital preservation: a report to the Council on Library and Information Resources [Em linha] Washington, D.C.: Commission on Preservation and Access: Council on Library and Information

Resources, 1999. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/rothenberg/reports/rothenberg/pub77.pdf>. ISBN 1-887334-63-7

ROTHENBERG, Jeff - Ensuring the longevity of digital information [Em linha]. Washington D.C.: Commission on Library and Information Resources, 1999. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/archives/ensuring.pdf>

ROTHENBERG, Jeff - Preserving authentic digital information. In Authenticity in a digital environment [Em linha]. Washington, D.C.: Council on Library and Information Resources, 2000. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/pub92/pub92.pdf/view>. ISBN 1-887334-77-7

ROUSSEAU, Denise [et al.] - Not so different after all: across-discipline view of trust. Academy of management review [Em linha]. Vol.23, nº 3 (1998), p. 393–404. [Consult. 26 Fev 2014]. Disponível na Internet: <URL:http://portal.psychology.uoguelph.ca/faculty/gill/7140/WEEK_3_Jan.25/Rousseau,%20Sitkin,%20Burt,%20%26%20Camerer_AMR1998.pdf>.ISSN 1930-3807

RUSSEL, Kelly; SERGEANT, Derek - The CEDARS project: implementing a model for distributed digital archives. RLG DigiNews [Em linha], vol. 3, nº 3 (1999). [Consult. 26 Fev. 2014]. Disponível na Internet: <URL:http://webdoc.gwdg.de/edoc/aw/rlgdn/preserv/diginews/diginews3-3.html>. ISSN 1093-5371

RUSSELL, Kelly - Digital preservation and the CEDARS project experience. New review of academic librarianship. [Em linha]. Vol. 6, nº 1 (2000), p. 139-154. [Consult. 26 Fev. 2014]. Disponível na Internet: <URL:http://www.tandfonline.com/doi/pdf/10.1080/13614530009516805>. ISSN 1740-7834

SALO, Dorothea - Inkeeper at the roach motel. Library trends [Em linha]. Vol.57, nº 2 (2008). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://digital.library.wisc.edu/1793/22088>. ISSN 1559-0682

SALTER, Jim - Bitrot and atomic COWs: inside “next-gen” filesystems. In Ars technical [Em linha], 2014. [Consult. 30 Jan. 2014] Disponível na Internet: <URL: http://arstechnica.com/information-technology/2014/01/bitrot-and-atomic-cows-inside-next-gen-filesystems/>.

SARAMAGO, Maria de Lurdes – Preservação digital de longo prazo: estado da arte e boas práticas em repositórios digitais. Lisboa: [s.n], 2003. Tese de mestrado em Estudos de Informação e Bibliotecas Digitais apresentada ao Instituto Superior de Ciências do Trabalho e da Empresa.

SHANNON, Claude – A mathematical theory of communication. The Bell system technical journal [Em linha]. Vol. 27, nº 3 (1948), p. 379–423; Vol. 27, nº 4 (1948), p. 623–656. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www3.alcatel-lucent.com/bstj/vol27-

1948/articles/bstj27-3-379.pdf> e <URL: http://www3.alcatel-lucent.com/bstj/vol27-1948/articles/bstj27-4-623.pdf>

SHANNON, Claude; WEAVER, Warren – The mathematical theory of communication. 1st. ed. Urbana, Il.: University of Illinois Press, 1949.

SCHMIDT, Rainer - An architectural overview of the SCAPE preservation platform In International conference on preservation of digital objects iPRES 2012 [Em linha]. 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://ipres-conference.org/ipres12/sites/ipres.ischool.utoronto.ca/files/iPres%202012%20Conference%20Proceedings%20Final.pdf>. ISBN 978-0-9917997-0-1

SCHUMANN, Natascha - Tried and trusted: experiences with certification processes at the GESIS data archive. IASSIST quarterly [Em linha]. Vol. 36, nº 3/4, (Fall - Winter 2012). P. 23-27. [Consult. 6 Mar. 2014]. Disponível na Internet: <URL: http://iassistdata.org/downloads/iqvol36_34_schumann_0.pdf>

SIERMAN, Barbara; JONES, Catherine; ELSTRØM, Gry – SCAPE Catalogue of preservation policy elements [Em linha]. [S.l.:s.n.], 2014. [Consult. 16 Set. 2014]. Disponível na Internet: <URL: http://www.scape-project.eu/wp-content/uploads/2014/02/SCAPE_D13.2_KB_V1.0.pdf>

SIMMEL, Georg – The philosophy of money [Em linha]. 3rd. ed. New York: Routledge, 2004. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.eddiejackson.net/web_documents/Philosophy%20of%20Money.pdf>. ISBN 0-203-48113-5

SUDERMAN, Jim - Principle-based concepts for the long-term preservation of digital records. In Proceedings of the 1st international digital preservation interoperability framework symposium. [Em linha]. New York: ACM, 2010. [Consult. 6 Mar. 2014]. Disponível na Internet: <URL: http://dl.acm.org/citation.cfm?doid=2039263.2039270>. ISBN 978-1-4503-0110-7

SWADE, Doron - Preserving software in an object-centred culture. In HIGGS, Edward, ed. lit. - History and electronic artefacts, Oxford: Clarendon Press, 1998. ISBN 978-0-19-823633-7, p. 195-206

THIBODEAU, Kenneth - Building the archives of the future: advances in preserving electronic records at the NARA. D-Lib magazine. Vol. 7, nº 2 (2001). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.dlib.org/dlib/february01/thibodeau/02thibodeau.html>. ISSN 1082-9873

THIBODEAU, Kenneth - Overview of technological approaches to digital preservation and challenges in coming years. In The state of digital preservation: an international perspective [Em linha]. Washington, D. C.: Council on Library and Information Resources, 2002. [Consult. 26 Fev. 2014]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/reports/pub107/pub107.pdf>. ISBN 1-887334-92-0

THOMAZ, Katia - Critical factors for digital records preservation. Journal of information, information technology, and organizations [Em linha]. Vol. 1 (2006), p. 21-41 [Consult. 26 Fev.

2014]. Disponível na Internet: <URL: http://jiito.org/articles/JIITOv1p021-041Thomaz12.pdf>. ISSN 1557-1327

THOMAZ, Katia - A draft TRAC-DRAMBORA mapping RLG/NARA TRAC with NESTOR CCTDR, DCC/DPE DRAMBORA, ISO27001 and OECD guidelines [Em linha]. [S.l.:s.n.:2008?]. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://wiki.digitalrepositoryauditandcertification.org/pub/Main/DocAnalyses/ComparisonChart.doc>

THOMAZ, Katia; SOARES, Antonio José - A preservação digital e o modelo de referência Open Archival Information System. DataGramaZero: revista de ciência da informação [Em linha]. Rio de Janeiro. Vol. 5, nº 1 (2004). [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://dgz.org.br/fev04/Art_01.htm>. ISSN 1517-3801

TOCCI, Ronald; WIDMER, Neal; MOSS, Gregory - Digital systems: principles and applications. 10ª ed. [S.l.]: Prentice Hall, 2007. ISBN 0-13-173969-7

UNESCO - Charter on the preservation of the digital heritage. In Records of the General Conference 32nd session: vol. 1, Resolutions [Em linha]. Paris, UNESCO, 2003. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://unesdoc.unesco.org/images/0013/001331/133171e.pdf#page=80>

UNIÃO EUROPEIA. Comissão - Guidelines on best practices for using electronic information [Em linha]. Luxemburg: DLM Forum; Office for Official Publications of the European Communities, 1997. [Consult. 26 Fev. 2014]. Disponível na Internet: <URL: http://ec.europa.eu/archives/ISPO/dlm/documents/guidelines.html>. ISBN 92-828-2285-0

UNIÃO EUROPEIA. Comissão - Guidelines on data management in Horizon 2020 [Em linha]. v.1.0 Luxemburgo: DLM Forum: Office for Official Publications of the European Communities, 2013. [Consult. 26 Fev. 2014]. Disponível na Internet: <URL: http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf>.

UNIÃO EUROPEIA. Comissão - Guidelines on open access to scientific publications and research data in Horizon 2020 [Em linha]. v.1.0 Luxemburg: DLM Forum: Office for Official Publications of the European Communities, 2013. [Consult. 26 Fev. 2014]. Disponível na Internet: <URL: http://ec.europa.eu/research/par Fev. icipants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf>

UNIÃO EUROPEIA. Comissão – MoReq specification: Model Requirements for the Management of Electronic Records [Em linha]. Brussels: Office for Official Publications of the European Communities, 2001. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL:http://ec.europa.eu/archival-policy/moreq/doc/moreq_en.pdf>. ISBN 92-894-1290-9

UNIÃO EUROPEIA. Comissão – Online survey on scientific information in the digital age [Em linha]. Luxemburg: Office for Official Publications of the European Communities, 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://ec.europa.eu/research/science-

society/document_library/pdf_06/survey-on-scientific-information-digital-age_en.pdf>. ISBN 978-92-79-23170-4

UNIVERSITY OF CALIFORNIA. Curation Center - Unified Digital Format Registry [Em linha] [S.l.]: The Regents of the University of California, 2012. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.udfr.org/>

VERHEUL, Ingeborg - Networking for digital preservation: current practice in 15 national libraries - IFLA Publications 119 [Em linha]. Munich: Saur: IFLA, 2006. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL:http://www.ifla.org/files/assets/hq/publications/ifla-publications-series-119.pdf>. ISBN 3-598-21847-8.

VIÑAS, Vicente; VIÑAS, Rute - Traditional restoration techniques: a RAMP study. Paris: UNESCO, 1988.

WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information [Em linha]. Washington D.C.; Mountain View, Ca.: Commission on Preservation and Access: Research Libraries Group, 1996. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.clir.org/pubs/reports/reports/pub63watersgarrett.pdf>. ISBN 1-88733450-5

WAUGH, Andrew [et al.] - Preserving Digital Information Forever. In Proceedings of the DL 2000 5th. ACM conference on digital libraries [Em linha]. New York: ACM, 2000. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://dl.acm.org/citation.cfm?id=336659>. ISBN 1-58113-231-X

WEBB, Colin [et al.] - Guidelines for the preservation of digital heritage [Em linha]. [S.l.]: UNESCO, 2003. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://unesdoc.unesco.org/images/0013/001300/130071e.pdf>.

WHEATLEY, Paul - Institutional repositories in the context of digital preservation [Em linha]. [S.l.]: Digital Preservation Coalition, 2004. [Consult. 11 Nov. 2013]. Disponível na Internet: <URL: http://www.dpconline.org/docs/DPCTWf4word.pdf>

Wikipedia contributors – Bit rot. In Wikipedia, the free encyclopedia [Em linha]. actual. 8 Out. 2013. [Consult. 6 Jan. 2014]. Disponível na Internet: <URL: http://en.wikipedia.org/wiki/Bit_rot/>

WITTEN, Ian; BAINBRIDGE, David; NICHOLS, David - How to build a digital library [Em linha]. 2nd.Ed. [S.l.]: Morgan Kaufmann Publishers: Elsevier, 2010. [Consult. 11 Nov. 2013]. Disponível parcialmente na WWW: <URL: http://books.google.pt/books?id=HiJNbEy5f70C&lpg=PP1&dq=how%20to%20build%20a%20digital%20library%20witten&pg=PP1#v=onepage&q&f=false>. ISBN 978-0-12-374857-7

YAKEL, Elizabeth [et al.] - Trust in digital repositories. International journal of digital curation [Em linha]. Vol. 8, nº 1, (2013), p. 143-156. [Consult. 6 Abril. 2014]. Disponível na Internet: <URL: http://www.ijdc.net/index.php/ijdc/article/view/8.1.143>. ISSN 1746-8256

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

ANEXOS

Anexo 1 - Tabela comparativa do TRAC

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure	3 ORGANIZATIONAL INFRASTRUCTURE		
AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure> A1. Governance & organizational viability	3.1 GOVERNANCE AND ORGANIZATIONAL VIABILITY		
A1.1 Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information.	3.1.1 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.	1.2 The digital repository assumes responsibility for long-term preservation of the information represented by the digital objects.	1.2 The digital repository assumes responsibility for long-term preservation of the information represented by the digital objects
A1.2 Repository has an appropriate, formal 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 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.	4.5 Continuation of the preservation tasks is ensured even beyond the existence of the digital repository.	4.6 Continuation of the preservation tasks is ensured even beyond the existence of the digital repository
AUDIT & CERTIFICATION CRITERIA > A. Organizational Infrastructure > A2. Organizational structure & staffing	3.2 ORGANIZATIONAL STRUCTURE AND STAFFING		
A2.1 Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties.	3.2.1 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.	4.3 Appropriate organisational structures exist for the digital repository. 5.1 All processes and responsibilities have been defined.	4.3 Appropriate organisational structures exist for the digital repository. 5.1 All processes and responsibilities have been defined.
A2.2 Repository has the appropriate number of staff to support all functions and services.	3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.	4.2 Sufficient numbers of appropriately qualified staff are available	4.2 Sufficient numbers of appropriately qualified staff are available

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
A2.3 Repository has an active professional development program in place that provides staff with skills and expertise development opportunities.	3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.		
AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure> A3. Procedural accountability & policy framework	3.3 PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK		
A3.1 Repository has defined its designated community(ies) and associated knowledge base(s) and has publicly accessible definitions and policies in place to dictate how its preservation service requirements will be met.	Partly the 3.3.1 The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.	1.3 The digital repository has defined its designated community(ies).	1.3 The digital repository has defined its designated community(ies).
A3.2 Repository has procedures and policies in place, and mechanisms for their review, update, and development as the repository grows and as technology and community practice evolve.	Partly 3.3.2 The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.		
A3.3 Repository maintains written policies that specify the nature of any legal permissions required to preserve digital content over time, and repository can demonstrate that these permissions have been acquired when needed.	[Partly] 3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects. [????]		
A3.4 Repository is committed to formal, periodic review and assessment to ensure responsiveness to technological developments and evolving requirements.	3.3.2.1 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.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
A3.5 Repository has policies and procedures to ensure that feedback from producers and users is sought and addressed over time.			

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
A3.6 Repository has a documented history of the changes to its operations, procedures, software, and hardware that, where appropriate, is linked to relevant preservation strategies and describes potential effects on preserving digital content.	3.3.3 The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.		
A3.7 Repository commits to transparency and accountability in all actions supporting the operation and management of the repository, especially those that affect the preservation of digital content over time.	3.3.4 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.		
A3.8 Repository commits to defining, collecting, tracking, and providing, on demand, its information integrity measurements.	3.3.5 The repository shall define, collect, track, and appropriately provide its information integrity measurements.		
A3.9 Repository commits to a regular schedule of self-assessment and certification and, if certified, commits to notifying certifying bodies of operational changes that will change or nullify its certification status.	3.3.6 The repository shall commit to a regular schedule of self-assessment and external certification.		
AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure> A4. Financial sustainability	3.4 FINANCIAL SUSTAINABILITY		
A4.1 Repository has short- and long-term business planning processes in place to sustain the repository over time.	3.4.1 The repository shall have short- and long-term business planning processes in place to sustain the repository over time.	4.1 Adequate financing of the digital repository is secured.	4.1 Adequate financing of the digital repository is secured
A4.2 Repository has in place processes to review and adjust business plans at least annually.			
A4.3 Repository's financial practices and procedures are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.	3.4.2 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.		

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
A4.4 Repository has ongoing commitment to analyze and report on risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).	3.4.3 The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).		
A4.5 Repository commits to monitoring for and bridging gaps in funding.	3.1.2.2 The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements. [Em parte]		
AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure> A5. Contracts, licenses, & liabilities			
A5.1 If repository manages, preserves, and/or provides access to digital materials on behalf of another organization, it has and maintains appropriate contracts or deposit agreements.	3.5.1 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.	3.1 Legal contracts exist between producers and the digital repository.	3.1 Legal contracts exist between producers and the digital repository
A5.2 Repository contracts or deposit agreements must specify and transfer all necessary preservation rights, and those rights transferred must be documented.	3.5.1.1 The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred shall be documented.		
A5.3 Repository has specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	3.5.1.2 The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	3.2 In carrying out its archiving tasks, the digital repository acts on the basis of legal rulings.	3.2 In carrying out its archiving tasks, the digital repository acts on the basis of legal arrangements
A5.4 Repository tracks and manages intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	3.5.2 The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	12.6 The DR acquires adequate metadata to record the corresponding usage rights and conditions. ???	12.6 The DR acquires adequate metadata to record the corresponding usage rights and conditions. ???

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
A5.5 If repository ingests digital content with unclear ownership/rights, policies are in place to address liability and challenges to those rights.	3.5.1.4 The repository shall have policies in place to address liability and challenges to ownership/rights.		
AUDIT & CERTIFICATION CRITERIA> B. Digital Object Management	4 DIGITAL OBJECT MANAGEMENT		
AUDIT & CERTIFICATION CRITERIA> B. Digital Object Management> B1. Ingest: acquisition of content	4.1 INGEST: ACQUISITION OF CONTENT	1.1 The digital repository has developed criteria for the selection of its digital objects.	1.1 The digital repository has developed criteria for the selection of its digital objects
B1.1 Repository identifies properties it will preserve for digital objects.	4.1.1 The repository shall identify the Content Information and the Information Properties that the repository will preserve.	9.2 The digital repository identifies which characteristics of the digital objects are significant for information preservation.	9.2 The digital repository identifies which characteristics of the digital objects are significant for information preservation.
B1.2 Repository clearly specifies the information that needs to be associated with digital material at the time of its deposit (i.e., SIP).	4.1.2 The repository shall clearly specify the information that needs to be associated with specific Content Information at the time of its deposit.	9.1 The digital repository specifies its transfer objects (Submission Information Packages, SIPs).	9.1 The digital repository specifies its transfer objects (Submission Information Packages, SIPs).
B1.3 Repository has mechanisms to authenticate the source of all materials.	4.1.4 The repository shall have mechanisms to appropriately verify the identity of the Producer of all materials.	7.1 Ingest: the digital repository ensures the authenticity of the digital objects.	7.1 Ingest: the digital repository ensures the authenticity of the digital objects.
B1.4 Repository's ingest process verifies each submitted object (i.e., SIP) for completeness and correctness as specified in B1.2.	4.1.5 The repository shall have an ingest process which verifies each SIP for completeness and correctness.	6.1 Ingest: the digital repository ensures the integrity of the digital objects.	6.1 Ingest: the digital repository ensures the integrity of the digital objects
B1.5 Repository obtains sufficient physical control over the digital objects to preserve them.	4.1.6 The repository shall obtain sufficient control over the Digital Objects to preserve them.	9.3 The digital repository has technical control of the digital objects in order to carry out long-term preservation measures.	9.3 The digital repository has technical control of the digital objects in order to carry out long-term preservation measures.

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B1.6 Repository provides producer/depositor with appropriate responses at predefined points during the ingest processes.	4.1.7 The repository shall provide the producer/depositor with appropriate responses at agreed points during the ingest processes.		
B1.7 Repository can demonstrate when preservation responsibility is formally accepted for the contents of the submitted data objects (i.e., SIPs).	3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.		
B1.8 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Ingest: content acquisition).	4.1.8 The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.		
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B2. Ingest: creation of the archivable package	4.2 INGEST: CREATION OF THE AIP		
B2.1 Repository has an identifiable, written definition for each AIP or class of information preserved by the repository.	4.2.1.1 The repository shall be able to identify which definition applies to which AIP.	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).
B2.2 Repository has a definition of each AIP (or class) that is adequate to fit long-term preservation needs.	4.2.1.2 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.	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).
B2.3 Repository has a description of how AIPs are constructed from SIPs.	4.2.2 The repository shall have a description of how AIPs are constructed from SIPs.	10.2 The digital repository takes care of transforming the transfer objects (SIPs) into archival objects (AIPs).	10.2 The digital repository takes care of transforming the transfer objects (SIPs) into archival objects (AIPs).

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B2.4 Repository can demonstrate that all submitted objects (i.e., SIPs) are either accepted as whole or part of an eventual archival object (i.e., AIP), or otherwise disposed of in a recorded fashion.	4.2.3 The repository shall document the final disposition of all SIPs. 4.2.3.1 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.		
B2.5 Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).	4.2.4 The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs.	12.1 The digital repository uniquely and permanently identifies its objects and their relationships.	12.1 The digital repository uniquely and persistently identifies its objects and their relationships.
B2.6 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).			
B2.7 Repository demonstrates that it has access to necessary tools and resources to establish authoritative semantic or technical context of the digital objects it contains (i.e., access to appropriate international Representation Information and format registries).	4.2.5 The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.		

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B2.8 Repository records/registers Representation Information (including formats) ingested.	4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects. 4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community. [????] 4.2.5.3 The repository shall have access to the requisite Representation Information. [????] 4.2.5.4 The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects. [????]	12.3 The digital repository acquires adequate metadata for structural description of the digital objects. 12.5 The digital repository acquires adequate metadata for technical description of the digital objects.	12.3 The digital repository acquires adequate metadata for structural description of the digital objects. 12.5 The digital repository acquires adequate metadata for technical description of the digital objects.
B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.	4.2.6 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.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.	4.2.7 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. 4.2.7.1 Repository shall have a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation. 4.2.7.2 The repository shall execute the testing process for each class of Content Information of the AIPs. 4.2.7.3 The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.	2.2 The digital repository ensures that the designated community can interpret the digital objects.	2.2 The digital repository ensures that the designated community can interpret the digital objects.
B2.11 Repository verifies each AIP for completeness and correctness at the point it is generated.	4.2.8 The repository shall verify each AIP for completeness and correctness at the point it is created.		
B2.12 Repository provides an independent mechanism for audit of the integrity of the repository collection/content.	4.2.9 The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.	6.1 Ingest: the digital repository ensures the integrity of the digital objects.	6.1 Ingest: the digital repository ensures the integrity of the digital objects.
B2.13 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (AIP creation).	4.2.10 The repository shall have contemporaneous records of actions and administration processes that are relevant to AIP creation.		
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B3. Preservation planning	4.3 PRESERVATION PLANNING		
B3.1 Repository has documented preservation strategies.	4.3.1 The repository shall have documented preservation strategies relevant to its holdings	4.4 The digital repository engages in long-term planning. 8 The digital repository has a strategic plan for its technical preservation	4.4 The digital repository engages in long-term planning. 8 The digital repository has a strategic plan for its technical preservation

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B3.2 Repository has mechanisms in place for monitoring and notification when Representation Information (including formats) approaches obsolescence or is no longer viable.	4.3.2 The repository shall have mechanisms in place for monitoring its preservation environment. 4.3.2.1 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.		
B3.3 Repository has mechanisms to change its preservation plans as a result of its monitoring activities.	4.3.3 The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
B3.4 Repository can provide evidence of the effectiveness of its preservation planning.	4.3.4 The repository shall provide evidence of the effectiveness of its preservation activities.		
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B4. Archival storage & preservation/maintenance of AIPs	4.4 AIP PRESERVATION		
B4.1 Repository employs documented preservation strategies.			
B4.2 Repository implements/responds to strategies for archival object (i.e., AIP) storage and migration.	4.4.1 The repository shall have specifications for how the AIPs are stored down to the bit level.	10.4 The digital repository implements strategies for the long-term preservation of the AIPs.	10.4 The digital repository implements strategies for the long-term preservation of the AIPs.
B4.3 Repository preserves the Content Information of archival objects (i.e., AIPs).	4.4.1.1 The repository shall preserve the Content Information of AIPs.		

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B4.4 Repository actively monitors integrity of archival objects (i.e., AIPs).	4.4.1.2 The repository shall actively monitor the integrity of AIPs.	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects. 7.2 Archival Storage: the digital repository ensures the authenticity of the digital 10.3 The digital repository guarantees the storage and readability of the AIPs.	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects. 7.2 Archival Storage: the digital repository ensures the authenticity of the digital 10.3 The digital repository guarantees the storage and readability of the AIPs.
B4.5 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Archival Storage).	4.4.2 The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.		
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B5. Information management	4.5 INFORMATION MANAGEMENT		
B5.1 Repository articulates minimum metadata requirements to enable the designated community(ies) to discover and identify material of interest.	4.5.1 The repository shall specify minimum information requirements to enable the Designated Community to discover and identify material of interest.		
B5.2 Repository captures or creates minimum descriptive metadata and ensures that it is associated with the archived object (i.e., AIP).	4.5.2 The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.	12.2 The digital repository acquires adequate metadata for formal and content- based description and identification of the digital objects.	12.2 The digital repository acquires adequate metadata for formal and content- based description and identification of the digital objects
B5.3 Repository can demonstrate that referential integrity is created between all archived objects (i.e., AIPs) and associated descriptive information.	4.5.3 The repository shall maintain bi-directional linkage between each AIP and its descriptive information.	12.7 The assignment of metadata to the digital objects is guaranteed at all times.	12.7 The package structure is preserved at all at all times
B5.4 Repository can demonstrate that referential integrity is maintained between all archived objects (i.e., AIPs) and associated descriptive information.	4.5.3.1 The repository shall maintain the associations between its AIPs and their descriptive information over time.	12.7 The assignment of metadata to the digital objects is guaranteed at all times.	12.7 The package structure is preserved at all at all times

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B6. Access management	4.6 ACCESS MANAGEMENT	2.1 The digital repository ensures its designated community can access the digital objects. 11.1 The digital repository defines its usage objects (Dissemination Information Packages, DIPs) 11.2 The digital repository ensures transformation of AIPs into DIPs.	2.1 The digital repository ensures its designated community can access the digital objects. 11.1 The digital repository defines its usage objects (Dissemination Information Packages, DIPs) 11.2 The digital repository ensures transformation of AIPs into DIPs.
B6.1 Repository documents and communicates to its designated community(ies) what access and delivery options are available.	4.6.1 The repository shall comply with Access Policies. [???]		
B6.2 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.			
B6.3 Repository ensures that agreements applicable to access conditions are adhered to.		3.3 With regard to use, the digital repository acts on the basis of legal requirements.	3.3 With regard to use, the digital repository acts on the basis of legal arrangements.
B6.4 Repository has documented and implemented access policies (authorization rules, authentication requirements) consistent with deposit agreements for stored objects.			
B6.5 Repository access management system fully implements access policy.	4.6.1 The repository shall comply with Access Policies.	6.3 Access: the digital repository ensures the integrity of the digital objects.	6.3 Access: the digital repository ensures the integrity of the digital objects.
B6.6 Repository logs all access management failures, and staff review inappropriate “access denial” incidents.	4.6.1.1 The repository shall log and review all access management failures and anomalies.		

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
B6.7 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is completed in relation to the request.	4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users. [????]		
B6.8 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is correct in relation to the request.	4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users. [????]		
B6.9 Repository demonstrates that all access requests result in a response of acceptance or rejection.	4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users. [????]		
B6.10 Repository enables the dissemination of authentic copies of the original or objects traceable to originals.	4.6.2 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.	7.3 Access: the digital repository ensures the authenticity of the digital objects.	7.3 Access: the digital repository ensures the authenticity of the digital objects.
AUDIT & CERTIFICATION CRITERIA > C. Technologies, Technical Infrastructure, & Security	5 INFRASTRUCTURE AND SECURITY RISK MANAGEMENT		
AUDIT & CERTIFICATION CRITERIA > C. Technologies, Technical Infrastructure, & Security > C1. System infrastructure	5.1 TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	5.2 The digital repository documents all its elements based on a defined process. 13.1 The IT infrastructure implements the object management demands.	5.2 The digital repository documents all its elements based on a defined process. 13.1 The IT infrastructure implements the object management demands.
C1.1 Repository functions on well-supported operating systems and other core infrastructural software.	5.1.1 The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure.[????]		
C1.2 Repository ensures that it has adequate hardware and software support for backup functionality sufficient for the repository's services and for the data held, e.g., metadata associated with access controls, repository main content.	5.1.1.2 The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.		

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
C1.3 Repository manages the number and location of copies of all digital objects.	5.1.2 The repository shall manage the number and location of copies of all digital objects.		
C1.4 Repository has mechanisms in place to ensure any/multiple copies of digital objects are synchronized.	5.1.2.1 The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized.		
C1.5 Repository has effective mechanisms to detect bit corruption or loss.	5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects.	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects.
C1.6 Repository reports to its administration all incidents of data corruption or loss, and steps taken to repair/replace corrupt or lost data.	5.1.1.3.1 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.		
C1.7 Repository has defined processes for storage media and/or hardware change (e.g., refreshing, migration).	5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).		
C1.8 Repository has 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 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.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
C1.9 Repository has a process for testing the effect of critical changes to the system.	5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
C1.10 Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment.	5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
AUDIT & CERTIFICATION CRITERIA > C. Technologies, Technical Infrastructure, & Security > C2. Appropriate technologies			

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
C2.1 Repository has hardware technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.	5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems. 5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities. 5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware. 5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so. [????]	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.	5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems. 5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities. 5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed. 5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software. 5.1.1.1.8 The repository shall have procedures, commitment, and funding to replace software when evaluation indicates the need to do so.[????]	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
AUDIT & CERTIFICATION CRITERIA > C. Technologies, Technical Infrastructure, & Security > C3. Security	5.2 SECURITY RISK MANAGEMENT		

TRAC	ISO 16363:2012	NESTOR 1	NESTOR 2
C3.1 Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs.	5.2.1 The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.	14 The infrastructure protects the digital repository and its digital objects.	14 The infrastructure protects the digital repository and its digital objects.
C3.2 Repository has implemented controls to adequately address each of the defined security needs.	5.2.2 The repository shall have implemented controls to adequately address each of the defined security risks	13.2 The IT infrastructure implements the security demands of the IT security system.	13.2 The IT infrastructure implements the security requirements of the IT security system
C3.3 Repository staff have delineated roles, responsibilities, and authorizations related to implementing changes within the system.	5.2.3 The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.		
C3.4 Repository has suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan(s).	5.2.4 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).		

Anexo 2: Tabela Comparativa do NESTOR (2ª Edição)

NESTOR 2	ISO 16363:2012	TRAC
A Organisational framework		A. Organizational Infrastructure
1 The DR has defined its goals.		
1.1 The DR has developed criteria for the selection of its digital objects.	4.1 INGEST: ACQUISITION OF CONTENT	B. Digital Object Management> B1. Ingest: acquisition of content
1.2 The DR assumes responsibility for long-term preservation of the information represented by the digital objects.	3.1.1 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.	A1.1 Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information.
1.3 The DR has defined its designated community/communities.	Partly the 3.3.1 The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.	A3.1 Repository has defined its designated community(ies) and associated knowledge base(s) and has publicly accessible definitions and policies in place to dictate how its preservation service requirements will be met.
2 The DR grants its designated community/communities adequate access to the information represented by the digital objects.		
2.1 The DR ensures its designated community/communities can access the digital objects.	4.6 ACCESS MANAGEMENT	B. Digital Object Management > B6. Access management

NESTOR 2	ISO 16363:2012	TRAC
2.2 The DR ensures that the designated community/communities can interpret the digital objects.	4.2.7 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. 4.2.7.1 Repository shall have a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation. 4.2.7.2 The repository shall execute the testing process for each class of Content Information of the AIPs. 4.2.7.3 The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.	B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.
3 Legal and contractual rules are observed.		
3.1 Legal contracts exist between producers and the digital repository.	3.5.1 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.	A5.1 If repository manages, preserves, and/or provides access to digital materials on behalf of another organization, it has and maintains appropriate contracts or deposit agreements.
3.2 In carrying out its archiving tasks, the DR acts on the basis of legal arrangements.	3.5.1.2 The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	A5.3 Repository has specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.
3.3 With regard to use, the DR acts on the basis of legal arrangements.		B6.3 Repository ensures that agreements applicable to access conditions are adhered to.
4 The organisational form is appropriate for the DR.		
4.1 Adequate financing of the digital repository is secured.	3.4.1 The repository shall have short- and long-term business planning processes in place to sustain the repository over time	A4.1 Repository has short- and long-term business planning processes in place to sustain the repository over time.
4.2 Sufficient numbers of appropriately qualified staff are available.	3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.	A2.2 Repository has the appropriate number of staff to support all functions and services.

NESTOR 2	ISO 16363:2012	TRAC
4.3 Appropriate organisational structures exist for the DR.	3.2.1 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.	A2.1 Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties.
4.4 The DR engages in long-term planning.	4.3.1 The repository shall have documented preservation strategies relevant to its holdings	B3.1 Repository has documented preservation strategies.

NESTOR 2	ISO 16363:2012	TRAC
4.5 The DR reacts to substantial changes.	3.3.2.1 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. 4.3.3 The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities. 5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems. 5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware. 5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so. 5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed. 5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software. 5.1.1.1.8 The repository shall have procedures, commitment, and funding to replace software when evaluation indicates the need to do so. 5.1.1.6.1 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. 5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes. 5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.	A3.4 Repository is committed to formal, periodic review and assessment to ensure responsiveness to technological developments and evolving requirements. B3.3 Repository has mechanisms to change its preservation plans as a result of its monitoring activities. C1.8 Repository has a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities. C1.9 Repository has a process for testing the effect of critical changes to the system. C1.10 Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment C2.1 Repository has hardware technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed. C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.

NESTOR 2	ISO 16363:2012	TRAC
4.6 Continuation of the preservation tasks is ensured even beyond the existence of the DR.	3.1.2.1 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	A1.2 Repository has an appropriate, formal 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.
5 The digital repository undertakes appropriate quality management.		
5.1 All processes and responsibilities have been defined.	3.2.1 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.	A2.1 Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties.
5.2 The DR documents all its elements based on a defined process.	5.1 TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	C. Technologies, Technical Infrastructure, & Security > C1. System infrastructure
B Object management		
6 The DR ensures the integrity of the digital objects during all processing stages.		
6.1 Ingest: the DR ensures the integrity of the digital objects.	4.1.5 The repository shall have an ingest process which verifies each SIP for completeness and correctness. 4.2.9 The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.	B1.4 Repository's ingest process verifies each submitted object (i.e., SIP) for completeness and correctness as specified in B1.2. B2.12 Repository provides an independent mechanism for audit of the integrity of the repository collection/content
6.2 Archival Storage: the DR ensures the integrity of the digital objects.	4.4.1.2 The repository shall actively monitor the integrity of AIPs 5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.	B4.4 Repository actively monitors integrity of archival objects (i.e., AIPs). C1.5 Repository has effective mechanisms to detect bit corruption or loss
6.3 Access: the DR ensures the integrity of the digital objects.	4.6.1 The repository shall comply with Access Policies	B6.5 Repository access management system fully implements access policy.
7 The DR ensures the authenticity of the digital objects during all processing stages.		
7.1 Ingest: the DR ensures the authenticity of the digital objects.	4.1.4 The repository shall have mechanisms to appropriately verify the identity of the Producer of all materials.	B1.3 Repository has mechanisms to authenticate the source of all materials.

NESTOR 2	ISO 16363:2012	TRAC
7.2 Archival Storage: the DR ensures the authenticity of the digital objects.	4.4.1.2 The repository shall actively monitor the integrity of AIPs 4.4.2 The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.	B4.4 Repository actively monitors integrity of archival objects (i.e., AIPs).
7.3 Access: the DR ensures the authenticity of the digital objects.	4.6.2 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.	B6.10 Repository enables the dissemination of authentic copies of the original or objects traceable to originals.
8 The DR has a strategic plan for its technical preservation measures.	3.1.2 The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission. 4.3.1 The repository shall have documented preservation strategies relevant to its holdings.	
9 The DR accepts digital objects from the producers based on defined criteria.		
9.1 The DR specifies its submission information packages (SIPs).	4.1.2 The repository shall clearly specify the information that needs to be associated with specific Content Information at the time of its deposit.	B1.2 Repository clearly specifies the information that needs to be associated with digital material at the time of its deposit (i.e., SIP).
9.2 The DR identifies which characteristics of the digital objects are significant for information preservation.	4.1.1 The repository shall identify the Content Information and the Information Properties that the repository will preserve.	B1.1 Repository identifies properties it will preserve for digital objects.
9.3 The DR has technical control of the digital objects in order to carry out long-term preservation measures.	4.1.6 The repository shall obtain sufficient control over the Digital Objects to preserve them.	B1.5 Repository obtains sufficient physical control over the digital objects to preserve them.
10 Archival storage of the digital objects is undertaken to defined specifications.		
10.1 The DR defines its archival information packages (AIPs).	4.2.1.1 The repository shall be able to identify which definition applies to which AIP. 4.2.1.2 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	B2.1 Repository has an identifiable, written definition for each AIP or class of information preserved by the repository. B2.2 Repository has a definition of each AIP (or class) that is adequate to fit long-term preservation needs

NESTOR 2	ISO 16363:2012	TRAC
	within that AIP.	
10.2 The DR takes care of transforming the submission information packages (SIPs) into archival information packages (AIPs).	4.2.2 The repository shall have a description of how AIPs are constructed from SIPs.	B2.3 Repository has a description of how AIPs are constructed from SIPs.
10.3 The DR guarantees the storage and readability of the archival information packages (AIPs).	4.4.1.2 The repository shall actively monitor the integrity of AIPs	B4.4 Repository actively monitors integrity of archival objects (i.e., AIPs).
10.4 The DR implements strategies for the long-term preservation of the archival information packages (AIPs).	3.1.2 The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission. 4.3.1 The repository shall have documented preservation strategies relevant to its holdings.	B4.2 Repository implements/responds to strategies for archival object (i.e., AIP) storage and migration.
11 The DR permits usage of the digital objects based on defined criteria.		
11.1 The DR defines its dissemination information packages (DIPs).	4.6 ACCESS MANAGEMENT	B. Digital Object Management> B6. Access management
11.2 The DR ensures transformation of archival information packages (AIPs) into dissemination information packages (DIPs).	4.6 ACCESS MANAGEMENT	B. Digital Object Management> B6. Access management
12 The data management system is capable of providing the necessary digital repository functions.		
12.1 The DR uniquely and permanently identifies its objects and their relationships.	4.2.4 The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs.	B2.5 Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).
12.2 The DR records adequate metadata for formal and content-based description and identification of the digital objects.	4.5.2 The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.	B5.2 Repository captures or creates minimum descriptive metadata and ensures that it is associated with the archived object (i.e., AIP).

NESTOR 2	ISO 16363:2012	TRAC
12.3 The DR records adequate metadata for structural description of the digital objects.	4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community. ??? 4.2.5.3 The repository shall have access to the requisite Representation Information. ??? 4.2.5.4 The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects. [???]	B2.8 Repository records/registers Representation Information (including formats) ingested.
12.4 The DR records adequate metadata to record all the changes made by the digital repository to the digital objects.	4.2.6 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.	B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.
12.5 The DR acquires adequate metadata for technical description of the digital objects.	4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects.	B2.8 Repository records/registers Representation Information (including formats) ingested.
12.6 The DR acquires adequate metadata to record the corresponding usage rights and conditions.	4.2.6 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.	A5.4 Repository tracks and manages intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.[?????] B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.
12.7 The package structure is preserved at all times.	4.5.3 The repository shall maintain bi-directional linkage between each AIP and its descriptive information. 4.5.3.1 The repository shall maintain the associations between its AIPs and their descriptive information over time.	B5.3 Repository can demonstrate that referential integrity is created between all archived objects (i.e., AIPs) and associated descriptive information. B5.4 Repository can demonstrate that referential integrity is maintained between all archived objects (i.e., AIPs) and associated descriptive information.
C. Infrastructure and Security		
13 The IT infrastructure is adequate.		
13.1 The IT infrastructure implements the object management requirements.	5.1 TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	C. Technologies, Technical Infrastructure, & Security > C1. System infrastructure

NESTOR 2	ISO 16363:2012	TRAC
13.2 The IT infrastructure implements the security requirements of the IT security system.	5.2.2 The repository shall have implemented controls to adequately address each of the defined security risks	C3.2 Repository has implemented controls to adequately address each of the defined security needs.
14 The infrastructure protects the digital repository and its digital objects.	5.2.1 The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant	C3.1 Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs.

Anexo 3: Tabela Comparativa da ISO 16363:2012

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
3 ORGANIZATIONAL INFRASTRUCTURE	AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure		
3.1 GOVERNANCE AND ORGANIZATIONAL VIABILITY	AUDIT & CERTIFICATION CRITERIA> A. Organizational Infrastructure> A1. Governance & organizational viability		
3.1.1 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.	A1.1 Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information	1.2 The digital repository assumes responsibility for long-term preservation of the information represented by the digital objects.	1.2 The digital repository assumes responsibility for long-term preservation of the information represented by the digital objects
3.1.2 The repository shall have a Preservation Strategic Plan that defines the approach the repository will take in the long-term support of its mission.		4.4 The digital repository engages in long-term planning [????] 8 The digital repository has a strategic plan for its technical preservation measures.	4.4 The digital repository engages in long-term planning.[????] 8 The digital repository has a strategic plan for its technical preservation
3.1.2.1 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.	A1.2. Repository has an appropriate, formal 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.	4.5 Continuation of the preservation tasks is ensured even beyond the existence of the digital repository.	4.6 Continuation of the preservation tasks is ensured even beyond the existence of the digital repository
3.1.2.2 The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.	A4.5. Repository commits to monitoring for and bridging gaps in funding. [em parte]	4.5 Continuation of the preservation tasks is ensured even beyond the existence of the digital repository.	4.6 Continuation of the preservation tasks is ensured even beyond the existence of the digital repository

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
3.1.3 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.		1.1 The digital repository has developed criteria for the selection of its digital objects. [???]	1.1 The digital repository has developed criteria for the selection of its digital objects [????]
3.2 ORGANIZATIONAL STRUCTURE AND STAFFING	A2. Organizational structure & staffing		
3.2.1 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.	A2.1. Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties A2.2. Repository has the appropriate number of staff to support all functions and services.	4.3 Appropriate organisational structures exist for the digital repository. 5.1 All processes and responsibilities have been defined. 4.2 Sufficient numbers of appropriately qualified staff are available	4.3 Appropriate organisational structures exist for the digital repository. 5.1 All processes and responsibilities have been defined. 4.2 Sufficient numbers of appropriately qualified staff are available
3.2.1.1 The repository shall have identified and established the duties that it needs to perform.	A2.1. Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties	4.3 Appropriate organisational structures exist for the digital repository. 5.1 All processes and responsibilities have been defined.	4.3 Appropriate organisational structures exist for the digital repository. 5.1 All processes and responsibilities have been defined.
3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.	A2.2. Repository has the appropriate number of staff to support all functions and services.	4.2 Sufficient numbers of appropriately qualified staff are available	4.2 Sufficient numbers of appropriately qualified staff are available
3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.	A2.3. Repository has an active professional development program in place that provides staff with skills and expertise development opportunities.		
3.3 PROCEDURAL ACCOUNTABILITY AND PRESERVATION POLICY FRAMEWORK	A3. Procedural accountability & policy framework		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
3.3.1 The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.	A3.1. Repository has defined its designated community(ies) and associated knowledge base(s) and has publicly accessible definitions and policies in place to dictate how its preservation service requirements will be met.	1.3 The digital repository has defined its designated community(ies).	1.3 The digital repository has defined its designated community(ies).
3.3.2 The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.			
3.3.2.1 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.	A3.2. Repository has procedures and policies in place, and mechanisms for their review, update, and development as the repository grows and as technology and community practice evolve.		
3.3.3 The repository shall have a documented history of the changes to its operations, procedures, software, and hardware.	A3.6. Repository has a documented history of the changes to its operations, procedures, software, and hardware that, where appropriate, is linked to relevant preservation strategies and describes potential effects on preserving digital content.		
3.3.4 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	A3.7. Repository commits to transparency and accountability in all actions supporting the operation and management of the repository, especially those that affect the preservation of digital content over time.		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
3.3.5 The repository shall define, collect, track, and appropriately provide its information integrity measurements.	A3.8 Repository commits to defining, collecting, tracking, and providing, on demand, its information integrity measurements.		
3.3.6 The repository shall commit to a regular schedule of self-assessment and external certification.	A3.9 Repository commits to a regular schedule of self-assessment and certification and, if certified, commits to notifying certifying bodies of operational changes that will change or nullify its certification status.		
3.4 FINANCIAL SUSTAINABILITY	A4. Financial sustainability		
3.4.1 The repository shall have short- and long-term business planning processes in place to sustain the repository over time.	A4.1. Repository has short- and long-term business planning processes in place to sustain the repository over time.	4.1 Adequate financing of the digital repository is secured.	4.1 Adequate financing of the digital repository is secured
3.4.2 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.	A4.3. Repository's financial practices and procedures are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.		
3.4.3 The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).	A4.4. Repository has ongoing commitment to analyze and report on risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).		
3.5 CONTRACTS, LICENSES, AND LIABILITIES	A5. Contracts, Licenses and Liabilities		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
3.5.1 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.	A5.1 If repository manages, preserves, and/or provides access to digital materials on behalf of another organization, it has and maintains appropriate contracts or deposit agreements.	3.1 Legal contracts exist between producers and the digital repository.	3.1 Legal contracts exist between producers and the digital repository
3.5.1.1 The repository shall have contracts or deposit agreements which specify and transfer all necessary preservation rights, and those rights transferred shall be documented.	A5.2 Repository contracts or deposit agreements must specify and transfer all necessary preservation rights, and those rights transferred must be documented.		
3.5.1.2 The repository shall have specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	A5.3 Repository has specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	3.2 In carrying out its archiving tasks, the digital repository acts on the basis of legal rulings.	3.2 In carrying out its archiving tasks, the digital repository acts on the basis of legal arrangements
3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects.	A3.3. Repository maintains written policies that specify the nature of any legal permissions required to preserve digital content over time, and repository can demonstrate that these permissions have been acquired when needed.[????] B1.7. Repository can demonstrate when preservation responsibility is formally accepted for the contents of the submitted data objects (i.e., SIPs).	1.1 The digital repository has developed criteria for the selection of its digital objects.	1.1 The digital repository has developed criteria for the selection of its digital objects.
3.5.1.4 The repository shall have policies in place to address liability and challenges to ownership/rights.	A5.5 If repository ingests digital content with unclear ownership/rights, policies are in place to address liability and challenges to those rights		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
3.5.2 The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	A5.4 Repository tracks and manages intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	12.6 The DR acquires adequate metadata to record the corresponding usage rights and conditions. ????	12.6 The DR acquires adequate metadata to record the corresponding usage rights and conditions. ????
4 DIGITAL OBJECT MANAGEMENT	B. Digital Object Management		
4.1 INGEST: ACQUISITION OF CONTENT	B.1 Ingest: acquisition of content		
4.1.1 The repository shall identify the Content Information and the Information Properties that the repository will preserve.	B1.1. Repository identifies properties it will preserve for digital objects.	9.2 The digital repository identifies which characteristics of the digital objects are significant for information preservation.	9.2 The digital repository identifies which characteristics of the digital objects are significant for information preservation.
4.1.1.1 The repository shall have a procedure(s) for identifying those Information Properties that it will preserve.			
4.1.1.2 The repository shall have a record of the Content Information and the Information Properties that it will preserve.			
4.1.2 The repository shall clearly specify the information that needs to be associated with specific Content Information at the time of its deposit.	B1.2. Repository clearly specifies the information that needs to be associated with digital material at the time of its deposit (i.e., SIP).	9.1 The digital repository specifies its transfer objects (Submission Information Packages, SIPs).	9.1 The digital repository specifies its transfer objects (Submission Information Packages, SIPs).
4.1.3 The repository shall have adequate specifications enabling recognition and parsing of the SIPs.			
4.1.4 The repository shall have mechanisms to appropriately verify the identity of the Producer of all materials.	B1.3. Repository has mechanisms to authenticate the source of all materials.	7.1 Ingest: the digital repository ensures the authenticity of the digital objects.	7.1 Ingest: the digital repository ensures the authenticity of the digital objects.

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.1.5 The repository shall have an ingest process which verifies each SIP for completeness and correctness.	B1.4. Repository's ingest process verifies each submitted object (i.e., SIP) for completeness and correctness as specified in B1.2.	6.1 Ingest: the digital repository ensures the integrity of the digital objects.	6.1 Ingest: the digital repository ensures the integrity of the digital objects
4.1.6 The repository shall obtain sufficient control over the Digital Objects to preserve them.	B1.5. Repository obtains sufficient physical control over the digital objects to preserve them (Ingest: content acquisition).	9.3 The digital repository has technical control of the digital objects in order to carry out long-term preservation measures.	9.3 The digital repository has technical control of the digital objects in order to carry out long-term preservation measures.
4.1.7 The repository shall provide the producer/depositor with appropriate responses at agreed points during the ingest processes.	B1.6. Repository provides producer/depositor with appropriate responses at predefined points during the ingest processes.		
4.1.8 The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.	B1.8. Repository has contemporaneous records of actions and administration processes that are relevant to preservation.		
4.2 INGEST: CREATION OF THE AIP	B.2 Ingest: creation of the archivable package		
4.2.1 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 longterm preservation needs.			
4.2.1.1 The repository shall be able to identify which definition applies to which AIP.	B2.1. Repository has an identifiable, written definition for each AIP or class of information preserved by the repository.	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).
4.2.1.2 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.	B2.2. Repository has a definition of each AIP (or class) that is adequate to fit long-term preservation needs.	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).	10.1 The digital repository defines its archival objects (Archival Information Packages, AIPs).

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.2.2 The repository shall have a description of how AIPs are constructed from SIPs.	B2.3. Repository has a description of how AIPs are constructed from SIPs	10.2 The digital repository takes care of transforming the transfer objects (SIPs) into archival objects (AIPs).	10.2 The digital repository takes care of transforming the transfer objects (SIPs) into archival objects (AIPs).
4.2.3 The repository shall document the final disposition of all SIPs.			
4.2.3.1 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.	B2.4. Repository can demonstrate that all submitted objects (i.e., SIPs) are either accepted as whole or part of an eventual archival object (i.e., AIP), or otherwise disposed of in a recorded fashion. [em parte]		
4.2.4 The repository shall have and use a convention that generates persistent, unique identifiers for all AIPs.	B2.5. Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).	12.1 The digital repository uniquely and permanently identifies its objects and their relationships.	12.1 The digital repository uniquely and persistently identifies its objects and their relationships.
4.2.4.1 The repository shall uniquely identify each AIP within the repository.	B2.5. Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).	12.1 The digital repository uniquely and permanently identifies its objects and their relationships.	12.1 The digital repository uniquely and persistently identifies its objects and their relationships.
4.2.4.1.1 The repository shall have unique identifiers.	B2.5. Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).	12.1 The digital repository uniquely and permanently identifies its objects and their relationships.	12.1 The digital repository uniquely and persistently identifies its objects and their relationships.
4.2.4.1.2 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.	B2.5. Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).	12.1 The digital repository uniquely and permanently identifies its objects and their relationships.	12.1 The digital repository uniquely and persistently identifies its objects and their relationships.
4.2.4.1.3 Documentation shall describe any processes used for changes to such identifiers.			

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.2.4.1.4 The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.			
4.2.4.1.5 The system of identifiers shall be adequate to fit the repository's current and foreseeable future requirements such as numbers of objects.			
4.2.4.2 The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location.			
4.2.5 The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.	B2.7. Repository demonstrates that it has access to necessary tools and resources to establish authoritative semantic or technical context of the digital objects it contains (i.e., access to appropriate international Representation Information and format registries).		
4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects.	B2.8 Repository records/registers Representation Information (including formats) ingested. [???]	12.3 The digital repository acquires adequate metadata for structural description of the digital objects. 12.5 The digital repository acquires adequate metadata for technical description of the digital objects.	12.3 The digital repository acquires adequate metadata for structural description of the digital objects. 12.5 The digital repository acquires adequate metadata for technical description of the digital objects.

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.	B2.8 Repository records/registers Representation Information (including formats) ingested. [???]		
4.2.5.3 The repository shall have access to the requisite Representation Information.			
4.2.5.4 The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects.			
4.2.6 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.	B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.
4.2.6.1 The repository shall have documented processes for acquiring PDI.	B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.2.6.2 The repository shall execute its documented processes for acquiring PDI.	B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.
4.2.6.3 The repository shall ensure that the PDI is persistently associated with the relevant Content Information.	B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.	12.4 The digital repository acquires adequate metadata to record the changes made by the digital repository to the digital objects. 12.6 The digital repository acquires adequate metadata to record the corresponding usage rights and conditions.
4.2.7 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.	B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.	2.2 The digital repository ensures that the designated community can interpret the digital objects.	2.2 The digital repository ensures that the designated community can interpret the digital objects.
4.2.7.1 Repository shall have a documented process for testing understandability for their Designated Communities of the Content Information of the AIPs at their creation.	B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.	2.2 The digital repository ensures that the designated community can interpret the digital objects.	2.2 The digital repository ensures that the designated community can interpret the digital objects.
4.2.7.2 The repository shall execute the testing process for each class of Content Information of the AIPs.	B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.	2.2 The digital repository ensures that the designated community can interpret the digital objects.	2.2 The digital repository ensures that the designated community can interpret the digital objects.

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.2.7.3 The repository shall bring the Content Information of the AIP up to the required level of understandability if it fails the understandability testing.	B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.	2.2 The digital repository ensures that the designated community can interpret the digital objects.	2.2 The digital repository ensures that the designated community can interpret the digital objects.
4.2.8 The repository shall verify each AIP for completeness and correctness at the point it is created.	B2.11 Repository verifies each AIP for completeness and correctness at the point it is generated		
4.2.9 The repository shall provide an independent mechanism for verifying the integrity of the repository collection/content.	B2.12 Repository provides an independent mechanism for audit of the integrity of the repository collection/content.	6.1 Ingest: the digital repository ensures the integrity of the digital objects.	6.1 Ingest: the digital repository ensures the integrity of the digital objects.
4.2.10 The repository shall have contemporaneous records of actions and administration processes that are relevant to AIP creation.	B2.13 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (AIP creation).		
4.3 PRESERVATION PLANNING	B.3 Preservation Planning		
4.3.1 The repository shall have documented preservation strategies relevant to its holdings.	B3.1. Repository has documented preservation strategies	4.4 The digital repository engages in long-term planning. 8 The digital repository has a strategic plan for its technical preservation	4.4 The digital repository engages in long-term planning. 8 The digital repository has a strategic plan for its technical preservation
4.3.2 The repository shall have mechanisms in place for monitoring its preservation environment.	B3.2. Repository has mechanisms in place for monitoring and notification when Representation Information (including formats) approaches obsolescence or is no longer viable. B3.3 Repository has mechanisms to change its preservation plans as a result of its monitoring activities.		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.3.2.1 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.	B3.2. Repository has mechanisms in place for monitoring and notification when Representation Information (including formats) approaches obsolescence or is no longer viable.		
4.3.3 The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.	B3.3 Repository has mechanisms to change its preservation plans as a result of its monitoring activities.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
4.3.3.1 The repository shall have mechanisms for creating, identifying or gathering any extra Representation Information required.			
4.3.4 The repository shall provide evidence of the effectiveness of its preservation activities	B3.4. Repository can provide evidence of the effectiveness of its preservation planning		
4.4 AIP PRESERVATION	B.4 Archival storage & preservation/ maintenance of AIPs		
4.4.1 The repository shall have specifications for how the AIPs are stored down to the bit level.	B4.2. Repository implements/responds to strategies for archival object (i.e., AIP) storage and migration [????]	10.4 The digital repository implements strategies for the long-term preservation of the AIPs.	10.4 The digital repository implements strategies for the long-term preservation of the AIPs.
4.4.1.1 The repository shall preserve the Content Information of AIPs.	B4.3 Repository preserves the Content Information of archival objects (i.e., AIPs).		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.4.1.2 The repository shall actively monitor the integrity of AIPs.	B4.4 Repository actively monitors integrity of archival objects (i.e., AIPs).	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects. 7.2 Archival Storage: the digital repository ensures the authenticity of the digital 10.3 The digital repository guarantees the storage and readability of the AIPs.	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects. 7.2 Archival Storage: the digital repository ensures the authenticity of the digital 10.3 The digital repository guarantees the storage and readability of the AIPs.
4.4.2 The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.	B4.5 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Archival Storage).		
4.4.2.1 The repository shall have procedures for all actions taken on AIPs.			
4.4.2.2 The repository shall be able to demonstrate that any actions taken on AIPs were compliant with the specification of those actions.			
4.5 INFORMATION MANAGEMENT	B.5 Information Management		
4.5.1 The repository shall specify minimum information requirements to enable the Designated Community to discover and identify material of interest.	B5.1 Repository articulates minimum metadata requirements to enable the designated community to discover and identify material of interest.		
4.5.2 The repository shall capture or create minimum descriptive information and ensure that it is associated with the AIP.	B5.2 Repository captures or creates minimum descriptive metadata and ensures that it is associated with the archived object (i.e., AIP).	12.2 The digital repository acquires adequate metadata for formal and content- based description and identification of the digital objects.	12.2 The digital repository acquires adequate metadata for formal and content- based description and identification of the digital objects

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.5.3 The repository shall maintain bi-directional linkage between each AIP and its descriptive information.	B5.3 Repository can demonstrate that referential integrity is created between all archived objects (i.e., AIPs) and associated descriptive information.	12.7 The assignment of metadata to the digital objects is guaranteed at all times.	12.7 The package structure is preserved at all at all times
4.5.3.1 The repository shall maintain the associations between its AIPs and their descriptive information over time.	B5.4 Repository can demonstrate that referential integrity is maintained between all archived objects (i.e., AIPs) and associated descriptive information.	12.7 The assignment of metadata to the digital objects is guaranteed at all times.	12.7 The package structure is preserved at all at all times
4.6 ACCESS MANAGEMENT	B.6 Access Management	2.1 The digital repository ensures its designated community can access the digital objects. 11.1 The digital repository defines its usage objects (Dissemination Information Packages, DIPs) 11.2 The digital repository ensures transformation of AIPs into DIPs.	2.1 The digital repository ensures its designated community can access the digital objects. 11.1 The digital repository defines its usage objects (Dissemination Information Packages, DIPs) 11.2 The digital repository ensures transformation of AIPs into DIPs.
4.6.1 The repository shall comply with Access Policies.	B6.1 Repository documents and communicates to its designated community(ies) what access and delivery options are available.[???] B6.5 Repository access management system fully implements access policy.	6.3 Access: the digital repository ensures the integrity of the digital objects.	6.3 Access: the digital repository ensures the integrity of the digital objects.
4.6.1.1 The repository shall log and review all access management failures and anomalies.	B6.6 Repository logs all access management failures, and staff review inappropriate “access denial” incidents.		
4.6.2 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.	B6.10 Repository enables the dissemination of authentic copies of the original or objects traceable to originals.	7.3 Access: the digital repository ensures the authenticity of the digital objects.	7.3 Access: the digital repository ensures the authenticity of the digital objects.

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users.	B6.7 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is completed in relation to the request. B6.8 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is correct in relation to the request. B6.9 Repository demonstrates that all access requests result in a response of acceptance or rejection.		
5 INFRASTRUCTURE AND SECURITY RISK MANAGEMENT	C. Technologies, Technical Infrastructure & Security		
5.1 TECHNICAL INFRASTRUCTURE RISK MANAGEMENT	C1. System Infrastructure C.2 Appropriate technologies[???]	5.2 The digital repository documents all its elements based on a defined process. 13.1 The IT infrastructure implements the object management demands.	5.2 The digital repository documents all its elements based on a defined process. 13.1 The IT infrastructure implements the object management demands.
5.1.1 The repository shall identify and manage the risks to its preservation operations and goals associated with system infrastructure.	C1.1 Repository functions on well-supported operating systems and other core infrastructural software.		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems.	C2.1 Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed. C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities.	C2.1 Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.	C2.1 Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.	C2.1 Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.	C2.1 Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.[????]	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities.	C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed.	C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software.	C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.1.8 The repository shall have procedures, commitment, and funding to replace software when evaluation indicates the need to do so.	C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.[????]	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.2 The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.	C1.2 Repository ensures that it has adequate hardware and software support for backup functionality sufficient for the repository's services and for the data held, e.g., metadata associated with access controls, repository main content.		
5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.	C1.5 Repository has effective mechanisms to detect bit corruption or loss	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects.	6.2 Archival Storage: the digital repository ensures the integrity of the digital objects.
5.1.1.3.1 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.	C1.6 Repository reports to its administration all incidents of data corruption or loss, and steps taken to repair/replace corrupt or lost data.		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.	C1.10 Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment		
5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).	C1.7 Repository has defined processes for storage media and/or hardware change (e.g., refreshing, migration).		
5.1.1.6 The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.			
5.1.1.6.1 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.	C1.8 Repository has a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities..	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes.	C1.9 Repository has a process for testing the effect of critical changes to the system.	5.3 The digital repository reacts to substantial changes	4.5 The digital repository reacts to substantial changes
5.1.2 The repository shall manage the number and location of copies of all digital objects.	C1.3 Repository manages the number and location of copies of all digital objects		
5.1.2.1 The repository shall have mechanisms in place to ensure any/multiple copies of digital objects are synchronized.	C1.4 Repository has mechanisms in place toensure any/multiple copies of digital objects are synchronized.		
5.2 SECURITY RISK MANAGEMENT	C.3 Security		

ISO 16363:2012	TRAC	NESTOR 1	NESTOR 2
5.2.1 The repository shall maintain a systematic analysis of security risk factors associated with data, systems, personnel, and physical plant.	C3.1 Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs.	14 The infrastructure protects the digital repository and its digital objects.	14 The infrastructure protects the digital repository and its digital objects.
5.2.2 The repository shall have implemented controls to adequately address each of the defined security risks.	C3.2 Repository has implemented controls to adequately address each of the defined security needs	13.2 The IT infrastructure implements the security demands of the IT security system.	13.2 The IT infrastructure implements the security requirements of the IT security system
5.2.3 The repository staff shall have delineated roles, responsibilities, and authorizations related to implementing changes within the system.	C3.3 Repository staff have delineated roles, responsibilities, and authorizations related to implementing changes within the system		
5.2.4 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).	C3.4 Repository has suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an off- site copy of the recovery plan(s).		