

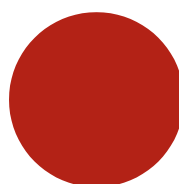
MESTRADO EM CIÊNCIA DA INFORMAÇÃO

Repositório Digital Seguro: um modelo de requisitos para um provedor de serviços de certificação

Ângela Sofia de Sousa Santos

M
2015

UNIDADES ORGÂNICAS ENVOLVIDAS
FACULDADE DE ENGENHARIA
FACULDADE DE LETRAS



Ângela Sofia de Sousa Santos

Repositório Digital Seguro: um modelo de requisitos para um provedor de serviços de certificação

Dissertação realizada no âmbito do Mestrado em Ciência da Informação,
orientada pela Professora Doutora Olívia Pestana e coorientada pela
Dra. Maria Manuela Pinto

Faculdade de Engenharia e Faculdade de Letras
Universidade do Porto

Junho de 2015

Repositório Digital Seguro: um modelo de requisitos para um provedor de serviços de certificação

Ângela Sofia de Sousa Santos

Dissertação realizada no âmbito do Mestrado em Ciência da Informação,
orientada pela Professora Doutora Olívia Pestana e coorientada pela
Dra. Maria Manuela Pinto

Membros do Júri

Professor Doutor António Manuel Lucas Soares
Faculdade de Engenharia - Universidade do Porto

Professor Doutor Carlos Manuel da Conceição Guardado da Silva
Faculdade de Letras - Universidade de Lisboa

Professora Dr.^a Maria Manuela Gomes de Azevedo Pinto
Faculdade de Letras - Universidade do Porto

Agradecimentos

Ao longo destes meses de trabalho, muitos foram os que contribuíram (direta ou indiretamente) para o sucesso do mesmo e por isso merecem o meu agradecimento.

Primeiro quero começar por agradecer às minhas orientadoras pelo apoio dado, em especial à Dr.^a Maria Manuela Pinto que foi incansável na ajuda preciosa que me deu e pela constante palavra de incentivo, no decorrer deste projeto. Obrigada pela sua amizade e paciência demonstrada. Foi muito importante para que tudo corresse de feição.

Quero agradecer à Multicert pela oportunidade em realizar este projeto e por me proporcionar a honra de fazer parte da equipa.

A todos os Colaboradores da Multicert que me acolheram muito bem e fizeram com que me sentisse uma Colaboradora como eles. Agradeço especialmente à Laura Cerqueira, minha tutora na Multicert que esteve sempre disponível para me ajudar no que precisasse e que foi também uma ajuda preciosa neste projeto.

Às minhas “*Brazucas*” e colegas de Mestrado Rúbia e Elisângela cujo apoio foi essencial, e a quem eu considero parte da minha família.

À minha família que sempre me apoiou, incentivou e contribuiu para que eu chegasse até aqui. Devo a eles tudo aquilo que sou.

Por último, e não menos importante, um agradecimento muito especial ao Nuno que já me acompanha na vida há vários anos e que me apoia incondicionalmente em tudo, tendo sempre um carinho e uma palavra de incentivo que me dá sempre força para continuar em frente.

A todos eles, um MUITO OBRIGADA!

Resumo

O impacto da evolução tecnológica ocorrida ao longo do século passado é evidenciado pelas massas de informação, nado-digital ou digitalizada, armazenadas, disponibilizadas e acedidas em meio digital. Para as organizações a informação é, hoje, um ativo de grande valor competitivo e uma fonte estratégica para o negócio. O aumento do fluxo informacional em formato digital e a necessidade de recuperar essa informação conduz à criação de mecanismos de armazenamento e recuperação da informação que respondam à complexidade informacional de uma forma eficiente e eficaz e que garantam o acesso continuado no longo prazo. É, pois, necessário garantir a preservação e segurança dessa informação para que as organizações a potenciem e se foquem nos seus objetivos, missão e estratégia. Este projeto de dissertação no campo da Ciência da Informação (CI), área de estudos da Gestão da Informação (GI), tem como contexto um provedor de serviços de certificação digital, a Multicert, e como principal objetivo contribuir para a criação do seu repositório digital seguro através de um detalhado diagnóstico organizacional e informacional e a consequente elaboração de documentos estruturantes.

Sendo a Multicert um provedor de serviços de certificação eletrónica, tem uma grande preocupação com a segurança da informação e pretende que esta se mantenha autêntica, íntegra, fidedigna, acessível e inteligível no longo prazo. A estruturação de um repositório confiável/seguro constitui um passo decisivo para a concretização deste objetivo, potenciando a informação como memória, ativo operacional e estratégico, evidência da qualidade do serviço e oportunidade de inovação organizacional. Desta forma, partindo do foco no meio digital, aborda-se a problemática da certificação do repositório digital correlacionando a implementação de Sistemas de Gestão da Informação com a preservação da informação numa perspetiva sistémica e integrada e como uma função chave na Gestão da Informação organizacional, isto é, não prescindindo do alinhamento de objetivos, do desenvolvimento de políticas e estratégias transversais e do respeito pelas boas práticas assumindo a preservação e a segurança da informação e, necessariamente, da tecnologia que a suporta, ao longo de todo o seu ciclo de vida e de gestão e no contexto organizacional em que ocorre.

Metodologicamente recorreu-se ao método quadripolar como dispositivo orientador do estudo/atividades especificadas para os quais contribuem os seus quatro polos interatuantes, no contexto de uma visão holística e dinâmica da abordagem do problema/necessidade em foco e da respetiva operacionalização em permanente avaliação e aperfeiçoamento. Ferramentas como a entrevista, a aplicação de inquérito por questionário e a observação participante permitiram conhecer a organização e aferir a sua maturidade na perspetiva da GI e da Tecnologia (ECM), com base em modelos e especificações internacionais (o IM3 Tool e o ECM Maturity model). Ao nível do repositório partiu-se do *European Framework for Audit and Certification of Digital Repositories* e confrontaram-se requisitos para certificação básica (o *DSA Data Seal of Approval* e o WDS) e requisitos de auditoria e certificação, com base na ISO 16363:2012.

Como resultados apresentam-se o *Documento de Especificação de Requisitos* que congrega requisitos a cumprir pelo sistema de gestão documental/conteúdos e requisitos com vista à certificação do Repositório Digital Seguro, bem como Documentos de suporte à elaboração da Política de Preservação Digital, das Estratégias de Preservação Digital e do Plano de Preservação Digital. Abordou-se, ainda, uma via para a desmaterialização da Informação que passa pela utilização do *Luratech* e a adoção do formato PDF/A contribuindo, assim, para a preservação no longo prazo de uma parte considerável da informação armazenada em meio digital pela Multicert.

Palavras-chave: Gestão da Informação; Preservação da Informação; Segurança da Informação; Repositório Digital Seguro; Certificação de repositório; Provedor de Serviços de Certificação

Abstract

The impact of technological developments that occurred over the past century is evidenced by the masses of information, swim-digital or scanned, stored, made available and accessible in digital media. For organizations the information is, today, a valuable competitive asset and a strategic source for business. The increased informational flow in digital format and the need to retrieve this information, leading to the creation of mechanisms of storage and retrieval of information that respond to the informational complexity of an efficient and effective and to ensure continued access in the long term. It is therefore necessary to ensure the preservation and safety of information for organizations to enhance and focus on your goals, mission and strategy. This dissertation project in the field of information science (ICS), the area of information management studies (GI), its context a digital certification service provider, the Multicert, and main objective is to contribute to the creation of your secure digital repository through a detailed organizational and informational diagnostic and the consequent development of structuring documents.

Being the Multicert an electronic certification services provider, has a great concern for the security of information and you want this to remain authentic, reliable, accessible, and understandable in the long run. The structuring of a trusted repository/insurance constitutes a decisive step towards the realization of this goal, boosting the information as memory, operating and strategic asset, evidence of the quality of service and opportunity of organizational innovation. In this way, leaving the focus on digital media, deals with the problems of digital repository certification by correlating the implementation of information management Systems with the preservation of information in a systemic and integrated perspective and as a key function in the management of organizational Information, regardless of the alignment of objectives, the development of transversal policies and strategies and on compliance with the good practice assuming the preservation and security of information and necessarily, the technology that supports it, throughout their life cycle and management and organizational context in which it occurs.

Methodologically four-pole method was used as study Advisor/specified activities for which contribute their four interatuantes poles, in the context of a holistic and dynamic approach of the problem/need in focus and its operationalization in permanent evaluation and improvement. Tools such as interview, survey and the participant observation allowed to know the Organization and assess your maturity from the perspective of the GI and technology (ECM), based on international specifications and templates (the IM3 *Tool* and ECM Maturity model). The repository level broke the *European Framework for Audit and Certification of Digital Repositories* and clashed for basic certification requirements (the *DSA Date Seal of Approval* and WDS) and audit and certification requirements, on the basis of ISO 16363.

As results are the requirements specification document that brings together requirements for document management system/content and requirements with a view to secure Digital Repository certification, as well as supporting documents in the drafting of the Digital Preservation policy, strategies for Digital preservation and Digital preservation plan. Approached, a route to dematerialization of information that passes through the use of the Luratech and PDF/A format adoption, thus contributing to the long-term preservation of a considerable part of the information stored in digital media by Multicert.

Keywords: Information Management; Digital Repository; Information Security; Preservation of Information; Trustworthy Digital Repository; Digital Certification; Certification Services Provider

Lista de figuras

Figura 1 Modelo conceptual OAIS (CCSDS, 2012)	27
Figura 2 Organograma da Multicert.....	57
Figura 3 O modelo de planeamento PLANETS segundo o OAIS (Becker, et.al, 2009)	80
Figura 4 Workflow do planeamento da Preservação (Becker, 2009).....	82

Abreviaturas e Símbolos

APA	Aliança para o Acesso Permanente
APARSEN	Alliance Permanent Access to the Records of Science in Europe Network
API	Application Programming Interface
CCSDS	Consultative Committee for Space Data Systems
CD's	Compact Disks
CI	Ciência da Informação
CRL	Center of Research Libraries
DCC	Digital Curation Center
DPE	Digital Preservation Europe
DSA	Data Seal of Approval
DVD	Digital Versatile Disc
ECEE	Entidade de Certificação Eletrónica do Estado
ECM	Enterprise Content Management
ERP	Enterprise Resource Planning
FEUP	Faculdade de Engenharia da Universidade do Porto
GDE	Gestor de Documentos Eletrónicos
GI	Gestão da Informação
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
OAIS	Open Archival Information System
OCLC	Online Computer Library Center
OCR	Optical Character Recognition
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RLG	Research Libraries Group
SAAI	Sistema Aberto de Arquivo de Informação
SCEE	Sistema de Certificação Eletrónica do Estado
SGD	Sistema de Gestão Documental
SGDA	Sistema de Gestão de Documentos de Arquivo
SGIAP	Sistema de Gestão de Informação Ativa e Permanente
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistema de Informação
SIAP	Sistema de Informação Ativa e Permanente
SIM	Sistema de Informação da Multicert
STI	Sistema Tecnológico de Informação

TI	Tecnologias da Informação
TIC	Tecnologias da Informação e Comunicação
TRAC	Trustworthy Repository Audit Certification
TSL	Trust Service Status List
UE	União Europeia
UK	United Kingdom
XML	Extensible Markup Language
WDS	World Data System

Sumário

Agradecimentos	iii
Resumo	iv
Abstract	v
Lista de figuras	vi
Lista de Tabelas	vii
Abreviaturas e Símbolos.....	viii
Introdução	1
1. Enquadramento e motivação.....	1
2. Problema e objetivos	3
3. Abordagem teórica e metodológica.....	4
4. Estrutura da dissertação	8
1. Gestão da Informação: Segurança e Preservação em meio digital	10
1.1 A Gestão da informação nas organizações	10
1.2 A Segurança da informação	13
1.3 Da Conservação à Preservação como variável da Gestão da Informação	15
1.4 Uma Política de Preservação da Informação Integrada	19
1.5 Instrumentos normativos e orientadores	21
2. Repositórios Digitais: confiança, segurança e preservação	25
2.1 Repositório digital: conceito e modelo	25
2.2 Confiança e certificação em repositórios digitais	27
2.3 O repositório seguro: modelos, especificações e ferramentas para a certificação	29
2.4 Casos de referência em certificação	35
3. O caso em estudo: MULTICERT S.A	38
3.1 A Certificação Digital	38
3.1.1 Contexto legal e regulamentar	43
3.1.2 Provedores, produtos e serviços.....	43
3.2 A MULTICERT S.A.....	50
3.2.1 Produtos e serviços	52
3.2.2 Estrutura organizacional	56
3.2.3 O software Alfresco	58
4. A GI na MULTICERT - Capítulo Confidencial	66
4.1 Políticas e modelo de GI.....	66
4.2. Estrutura de Suporte Informacional	69
4.3 Infraestrutura tecnológica	70
4.4 Estrutura de processos: principais e de suporte	71
4.5 Avaliação da maturidade da GI e da Tecnologia ECM	75
4.5.1 O modelo IM3 tool: aplicação e resultados	76
4.5.2 O modelo ECM Maturity: aplicação e resultados.....	80
5. Bases para a implementação do Repositório Digital Seguro	83
5.1 A conformidade nos serviços de Gestão Documental via Alfresco	83
5.1.1 O Modelo de Requisitos Modulares para a Gestão de Documentos: Moreq 2010	84
5.1.2. Especificação e conformidade aos requisitos MoReq2010	85
5.2. A conformidade no serviço de Repositório	86
5.2.1 A ISO 16363:2012	87
5.2.2 Especificação e conformidade aos requisitos ISO 16363	87
5.3 Bases para o planeamento da preservação em meio digital	93

5.3.1 Planos de preservação.....	93
5.3.2 O Projeto PLANETS e o Modelo de Planeamento PLANETS/OAIS.....	94
5.3.3 Ferramentas para o planeamento da preservação	104
5.4 Uma estratégia na desmaterialização da informação: normalização e formato de preservação. - Subcapítulo CONFIDENCIAL	107
Conclusões e perspetivas futuras	113
Referências Bibliográficas.....	117
Anexos Públicos	129
Anexo 1 - Árvore de Objetivos	130
Anexo 2 - Legislação usada pela Multicert	131
Anexo 3 - Principais parceiros da Multicert	135
Anexo 4: Questionário IM3 tool	138
Anexo 5 - Poster da dissertação apresentado nas XIII Jornadas de Ciência da Informação em Maio de 2015	152
Anexos Confidenciais	153
Anexo 6 - Quadro de avaliação da Maturidade do ECM	154
Anexo 7 - Documentos de Suporte à Especificação.....	155
Anexo 8 - Guia para o Plano de Preservação da Informação.....	155
Anexo 9 - Guia para a Política de Preservação da Informação	169
Anexo 10 - Guia para Estratégia de Preservação da Informação	178
Anexo 11 - Documento de Especificação de Requisitos.....	179

Introdução

1. Enquadramento e motivação

Vivemos numa sociedade denominada de Sociedade da Informação, Sociedade do Conhecimento ou, ainda, Sociedade em Rede caracterizada pelo grande impacto que as Tecnologias de Informação e Comunicação (TIC) têm na vida das pessoas e mais particularmente nas Instituições e demais Organizações.

O crescimento exponencial da produção e fluxo informacional em meio digital, a possibilidade de se armazenarem eletronicamente grandes volumes de informação, quer tivesse sido criada nesse meio ou digitalizada, e a necessidade de disseminar e garantir a preservação e o acesso continuado no longo prazo à mesma, fez com que fossem pensadas e criadas infraestruturas de armazenamento e recuperação da informação como os Repositórios Digitais.

Um Repositório Digital é um termo com uma aceção específica no meio digital, devendo ser sustentável e fiável, como também ser bem enquadrado e bem gerido.

Constitui-se como uma plataforma em meio digital na qual é possível aceder à informação em tempo real e sempre que se necessite.

Os repositórios são apresentados de diferentes formas e perspetivas, com uma grande variedade de contextos, comunidades, objetivos e práticas ligadas à sua criação e funcionamento. Podem ser colaborativos e apresentar um baixo controlo dos conteúdos e de acesso aos documentos, como podem ter um alto nível de controlo (Masson, 2008). Contudo, não basta criar um Repositório Digital e aí colocar toda a informação produzida e recebida pela Organização no decorrer das suas atividades. É necessário garantir a preservação e segurança dessa informação para que possa suportar as Organizações na concretização dos seus objetivos, missão e estratégia. Um repositório deve ter como características fundamentais a reutilização, a acessibilidade, a durabilidade, a flexibilidade, a versatilidade, a interoperabilidade e a inteligibilidade (Sousa, 2013).

Nas Organizações a informação é, atualmente, encarada como um dos ativos de maior valia, isto é, uma fonte de vantagem estratégica, exigindo a sua proteção que sejam providenciados os meios necessários para minimizar o risco de esta poder ser “violada” nos seus atributos fundamentais, isto é, em termos de confidencialidade, autenticidade, integridade, não-repúdio e disponibilidade.

É com base na informação, interna e externa, que se tomam as decisões mais importantes e que levam a que a organização se torne competitiva e estratégica e se distinga no meio empresarial. Acresce que o problema da fragilidade e da obsolescência tecnológica faz com que a preservação da informação seja indissociável da segurança da mesma e que, ao perspetivar a criação de um repositório seguro/confiável, tenham, também, que ser pensadas, desenvolvidas e implementadas políticas, metodologias, ferramentas e técnicas que garantam a preservação dos objetos digitais no longo prazo, conscientes da existência de ciclos de obsolescência de *hardware* e *software* cada vez mais curtos (3 a 5 anos).

Para garantir a autenticidade, a responsabilidade, o não-repúdio e a confiabilidade na informação (a par da acessibilidade e inteligibilidade) é necessário implementar, entre outras, uma *Política de Preservação* que esteja alinhada com a Política de Gestão da Informação (GI) na Organização e em concordância com o plano estratégico de preservação (ISO16363:2012)¹. A política de Preservação fica desde logo plasmada numa declaração por escrito na qual é assumido o compromisso e descritos os procedimentos que devem ser tomados pelo repositório para promover a preservação da informação.

No entanto a operacionalização que está em foco nos diversos instrumentos normativos carece de uma base teórica e metodológica que oriente a abordagem de cada caso e, na perspetiva da Ciência da Informação, Pinto e Silva (2005) afirmam que as Organizações precisam de “uma abordagem que congregue, desde a fase de conceção da plataforma tecnológica (*hardware* e *software*), até à produção, circulação, avaliação, armazenamento, disponibilização e preservação da informação, toda a Organização e os seus processos de negócio”. É neste pressuposto que se procurou contribuir para o desenvolvimento de um SIAP (Sistema de Informação Ativa e Permanente) na Multicert adotando o modelo teórico de base sistémica e informacional com o mesmo nome e que visa orientar a análise e a operacionalização da GI no contexto organizacional, envolvendo a Organização e os seus colaboradores no processo de GI com vista a torná-lo mais eficiente e eficaz.

Para que o SIAP seja desenvolvido e preservado, por forma a garantir o acesso continuado no longo prazo e a segurança da informação que o integra, é necessário conhecer, compreender e representar o contexto organizacional para depois conhecer, compreender, organizar, representar e gerir o próprio SI (Pinto, 2009).

¹ Cf. Sousa, 2013 e Oliveira, 2014.

2. Problema e objetivos

A Multicert, Serviços de Certificação Eletrónica, S.A. iniciou a sua atividade em 2002, posicionando-se no mercado como fornecedor de soluções completas de segurança e/ou certificação digital para todo o tipo de transações eletrónicas que exigem segurança (*e-commerce, e-banking, e-government, email, etc.*). Atualmente, a Multicert desenvolve a sua atividade nas seguintes áreas: Identidade; Desmaterialização; Serviços Profissionais e Investigação/Desenvolvimento. Na área da Identidade destacam-se os documentos de identificação como o Cartão de Cidadão Português e o Cartão Nacional de Identificação de Cabo Verde, bem como o Passaporte Eletrónico Português e Cabo-Verdiano. Ainda a personalização de Cartões e Cédulas profissionais que permitem aos seus associados a possibilidade de autenticação e assinatura digital na sua qualidade profissional.

Considerando os serviços, produtos e mercado a que se direciona, a Multicert está particularmente sensível à temática da segurança da informação e, crescentemente, à vertente específica relacionada com a criação dos Repositórios Seguros/ Confiáveis.

O seu repositório deve acima de tudo ser seguro, não se limitando apenas aos aspetos tecnológicos mas também às instalações físicas e às ações pessoais.

Este projeto tem, assim, como principal objetivo contribuir para a estruturação e certificação do repositório digital da Multicert desenvolvendo o respetivo *Documento de Especificação de Requisitos*, enquadrado por um esboço de proposta de *Estratégia e Políticas de Preservação da Informação da Multicert*, com vista à posterior elaboração do seu *Plano de Preservação da Informação*.

Deste projeto podem-se destacar como principais objetivos²:

- Compreender o mercado e o papel do provedor de serviços de certificação eletrónica, identificando e analisando os problemas e as suas necessidades numa perspetiva de acesso continuado no longo prazo;
- Mapear e referenciar modelos, normas, regulamentação e casos de boas práticas;
- Desenvolver o Documento de Especificação de Requisitos com vista à criação do Repositório Digital Certificável da Multicert, que terá como principal documento orientador a norma ISO 16363:2012;

² Árvore de Objetivos em anexo 1

- Apoiar a elaboração do Documento relativo à Estratégia e Políticas de Preservação da Informação da Multicert;
- Conceber um modelo de implementação na ótica do provedor de serviços e produtos de certificação eletrónica.

Procurar-se-á articular a vertente da segurança da informação com a preservação da informação dado serem ambas essenciais para garantir o acesso continuado e a preservação no longo prazo dos atributos supra referenciados.

Será, também, abordada a problemática da Preservação da Informação numa perspetiva sistémica e integrada (SIAP) e como variável da Gestão da Informação Organizacional, alinhando para isso os objetivos, o desenvolvimento de estratégias e políticas organizacionais, respeitando as boas práticas da preservação e segurança da informação, independentemente do suporte/meio usado para o seu registo e ao longo de todo o seu ciclo de vida e de gestão, no contexto organizacional em que ocorre.

3. Abordagem teórica e metodológica

A presente dissertação insere-se no campo científico da Ciência da Informação, área de estudos da Gestão da Informação e assume a Preservação da Informação como variável da GI, no contexto da estruturação e certificação do Repositório Digital da Multicert.

Este estudo tem como referente o paradigma pós-custodial e como ferramenta interpretativa a Teoria Sistémica socorrendo-se do Método Quadripolar, proposto por P. de Bruyne et al. em 1974, como instrumento metodológico a aplicar no âmbito das Ciências Sociais e, neste caso, em Ciência da Informação.

O Método Quadripolar enquadra e guia a investigação e o trabalho a desenvolver nesta dissertação sendo constituído por quatro pólos interatuantes com vista a desenvolver uma visão holística e dinâmica da abordagem do problema/necessidade em foco e de projetos de operacionalização em permanente avaliação e aperfeiçoamento. Este método é constituído por quatro polos a saber: Pólo Epistemológico, Pólo Teórico, Pólo Técnico e Pólo Morfológico.

O **Pólo Epistemológico** diz respeito ao debate e à construção do objeto científico, definindo-se aqui os limites da problemática de investigação em termos da identificação e delimitação do problema ou necessidade e dos paradigmas que orientarão todo o processo. Este projeto de dissertação em CI desenvolveu-se, assim, a luz do novo paradigma pós-custodial científico-informacional.

No **Polo Teórico** manifesta-se a racionalidade que o sujeito reconhece no objeto de estudo, na formulação de conceitos, teorias, e leis.

Tomando como referência, o referido paradigma e os conceitos que o mesmo implica, parte-se da formulação da seguinte questão orientadora:

- Como pode um fornecedor de produtos e serviços de certificação eletrónica contribuir para a segurança e a preservação da informação numa perspetiva de acesso continuado no longo prazo?

O **Polo Técnico** compreende a fase onde acontece o contacto com a realidade através de experimentação, observação ou análise/avaliação, com a finalidade de resolver o problema. Sendo este projeto de carácter prático, o principal enfoque neste polo será inevitavelmente qualitativo, acrescentando contributos da investigação dada a forma interativa como se desenvolve e permite a produção de saberes ao longo de todo o processo desenvolvido e grupos de trabalho que nele participam. Esta opção visa contribuir tanto para os interesses das pessoas numa situação problemática imediata, como para promover os objetivos das ciências sociais (O'Brien, 1998). Enquanto o investigador resolve o problema que tem em mãos está, também, a contribuir para o conhecimento científico, divulgando os resultados do seu trabalho. Como refere O'Brien (1998), realizar este duplo objetivo requer a colaboração ativa do investigador com o promotor/cliente, salientando-se, assim, a importância da co aprendizagem como aspeto fundamental do processo de investigação. O processo de investigação pode ser descrito como um modelo simples que se desenvolve de forma cíclica sendo composto por quatro fases - planejar, agir, observar e refletir (Kemmis, S. *apud* O'Brien, 1998) - que num projeto de dissertação correspondem a ciclos de ajustamentos do projeto à Organização e problema em foco.

Na fase de planeamento, foi desenvolvida a revisão da literatura, que partiu de uma pesquisa bibliográfica sobre vários recursos e fontes de informação, nomeadamente artigos, dissertações e instrumentos orientadores e normativos sobre o tema do projeto, e da análise das ferramentas disponíveis para a certificação de repositórios.

Na parte da ação procedeu-se ao levantamento e análise das necessidades da empresa, realizaram-se entrevistas aos Colaboradores da Multicert, observou-se e participou-se ativamente nos diversos grupos de trabalho, recolhendo indicações que conduziram à revisão do plano e a uma melhor objetivação do problema, passando-se, depois, para ciclos de validação dos instrumentos que se iam desenvolvendo.

O processo de análise e especificação dos requisitos recorreu à Engenharia de Requisitos, assumida como a ciência e disciplina que se preocupa com a análise (das necessidades) e documentação dos requisitos, fornecendo mecanismos apropriados para facilitar as atividades de análise, documentação e verificação (Lopes, 2004). Em termos operacionais trata-se do processo sistemático de desenvolvimento de requisitos de sistemas, sendo composto por diversas atividades que recorrem na sua execução à utilização de um conjunto de técnicas e modelos que tornam sistemática e repetitiva a execução dessas mesmas tarefas (Pinheiro, 2003).

Este processo envolve a identificação dos objetivos do sistema e a descrição das propriedades associadas a restrições ou condicionantes no seu desenvolvimento. O resultado consiste num documento de requisitos onde é descrito o comportamento esperado do sistema em questão (Pinheiro, 2003).

As duas atividades principais são a análise do problema e a especificação de requisitos. Estas duas atividades são interdependentes e devem ser realizadas conjuntamente. A análise e especificação de requisitos envolvem as atividades de determinar os objetos de um sistema e as restrições associadas a ele, assim como, estabelecem o relacionamento entre esses objetivos e restrições e a especificação precisa do sistema, nomeadamente, descrições acerca das propriedades do sistema e descrições associadas a restrições ou condicionantes no seu desenvolvimento. (Pinheiro, 2003). Os principais objetivos da Engenharia de Requisitos consistem em:

- Estabelecer uma visão comum entre o cliente e a equipa de projeto em relação aos requisitos que serão atendidos;
- Registrar e acompanhar requisitos ao longo de todo o processo de desenvolvimento;
- Manter planos, artefactos e atividades de *software* consistentes com os requisitos alocados (Gaspar, J. 2012).

Estes requisitos podem ter três funções:

- Ferramenta de contratualização: uma especificação que define o contexto técnico e um contrato de desenvolvimento com valor legal e que serve para proteger todas as partes envolvidas;
- Ferramenta de gestão de configurações: a definição e a relação entre os requisitos que constituem as funcionalidades e o contexto do sistema. Controlando os requisitos controla-se a definição da configuração;
- Ferramenta de engenharia: os requisitos podem ser usados como plataforma de comunicação entre todos os atores para descrever e compreender as necessidades operacionais, apoiar decisões de cariz técnico, definir a

arquitetura e/ou para verificar a conclusão de módulos ou do próprio projeto.
(Gaspar, J. 2012)

Este projeto congrega quer a definição da configuração, quer a compreensão e descrição de necessidades e a construção de uma plataforma de informação e comunicação para suportar a estruturação e certificação de um repositório.

As principais operações a desenvolver neste polo serão:

- Recolha de bibliografia em fontes diversificadas (bases dados, repositórios);
- Revisão de literatura com base nos métodos de recolha de dados (pesquisa documental, validação de fontes, análise de conteúdo, seleção e síntese com a elaboração de fichas de leitura);
- Identificação e análise de casos similares ao projeto a realizar;
- Análise do contexto organizacional da Multicert;
- Observação direta e participante do funcionamento da Multicert;
- Realização de entrevistas exploratórias (aos Colaboradores);
- Levantamento, análise e especificação de requisitos.

No **polo morfológico** reflete-se a eficácia destas operações. Aqui assume-se por inteiro a análise dos dados recolhidos e parte-se para a abordagem da problemática em estudo e para a exposição de todo o processo que permitiu a sua construção, nomeadamente na função de comunicação. Trata-se da organização e da apresentação dos dados, devidamente criticados no polo teórico e harmonizado no polo epistemológico, o que ilustra o peso interativo da investigação quadripolar.

Neste polo são analisados os dados da avaliação à maturidade da GI e da maturidade do *Enterprise Content Management*, o Sistema de Gestão de Documentos, neste caso o Alfresco.

Desta forma pretende-se apresentar os resultados através de:

- *Documento de Especificação de Requisitos* com vista à conformidade e eventual certificação do Repositório. O documento de requisitos aparece estruturado em três grandes secções: Infraestrutura Organizacional; Gestão de Objetos Digitais; Infraestrutura e Gestão de Riscos de Segurança. Este documento está também dividido em requisitos funcionais e não funcionais. Os requisitos funcionais descrevem os serviços que o sistema deve fornecer, especificando como este deve reagir por exemplo a solicitações dos utilizadores (Pinheiro, 2003). Dizem respeito à definição das funções que um sistema ou um componente de um sistema deve fazer. Descrevem as funções

a serem realizadas nas entradas de um sistema ou em um dos seus componentes, a fim de que se produzam saídas (Lopes, 2004).

Os requisitos não funcionais descrevem as restrições sobre os serviços e funções do sistema, como restrições temporais, requisitos de segurança, etc. (Pinheiro, 2003) dizem também respeito a aspetos de desempenho, interfaces com o utilizador, confiabilidade, segurança, portabilidade, padrões, e outras propriedades que o sistema deve possuir, bem como aspetos sociais e políticos. Alguns desses requisitos são provavelmente traduzidos em funções (operacionalizados), ao longo do processo de desenvolvimento de *software* (Lopes, 2004).

- Elaboração de uma proposta de modelo de implementação na ótica do provedor de serviços e produtos de certificação eletrónica.

4. Estrutura da dissertação

O presente documento compreende uma introdução, cinco capítulos, conclusões e perspectivas futuras.

Na Introdução é definido o enquadramento e motivação que levaram ao desenvolvimento desta dissertação. É definido, ainda, o problema, objetivos e resultados esperados no final do projeto, assim como a abordagem teórica e metodológica adotada e, por fim, apresenta-se a estrutura da dissertação.

No primeiro capítulo o tema central é a Gestão da Informação com o foco na segurança e preservação da informação em meio digital. Decidiu-se começar por descrever o conceito da Gestão da Informação, nas suas vertentes de Segurança e Preservação em meio digital, por ser um dos temas centrais que levará depois ao Repositório Digital. Assim neste capítulo aborda-se a questão da GI nas organizações; parte-se do conceito de Conservação do documento para chegar a uma visão holística e sistémica que situa a Preservação como uma variável da GI; faz-se uma abordagem integrada da Preservação e Segurança da Informação e analisam-se os instrumentos normativos e orientadores identificados.

No segundo capítulo entra-se no campo dos Repositórios Digitais e aborda-se a confiança, segurança e preservação. Apresentam-se os modelos, as especificações e as ferramentas usadas para a certificação como: o *European Framework for Audit and Certification of Digital Repositories*; o *Data Seal of Approval* e o WDS, como requisitos para uma certificação básica; e o TRAC e a ISO 16363, como modelos de requisitos de auditoria e certificação, sendo que este trabalho de certificação se vai focar essencialmente nos requisitos definidos na norma ISO 16363. Refere-se,

também, a ferramenta *Drambora*, para auditar a gestão do risco em repositórios. Neste capítulo são, ainda, apresentados casos de referência em certificação como o *Hathitrust*, o *Chronopolis*, o *Clockss* e o *Pórtico*. Cada um destes casos representa um conjunto de boas práticas na certificação de repositórios digitais.

No terceiro capítulo entra-se no campo da certificação digital para contextualizar o objeto de estudo desta dissertação que versa a certificação de um repositório digital numa organização cujo negócio se desenvolve em torno de produtos e serviços de “certificação digital”, mas não de repositórios.

Neste capítulo apresenta-se também a Organização Multicert à qual se faz uma análise ao nível da estrutura organizacional, produtos e serviços disponibilizados pela mesma. A ferramenta Alfresco aparece também referenciada neste capítulo, apresentando-se como uma ferramenta que serve de Repositório Digital na Multicert.

O quarto capítulo faz referência à Gestão da Informação na Multicert. Aqui são apresentados as políticas e modelos de Gestão de Informação, a estrutura de suporte informacional e infraestrutura tecnológica que sustenta todos os processos da Multicert. Foi feita uma avaliação à GI na organização e do ECM que suporta a sua atividade, com o intuito de perceber como a GI está enraizada na organização e como os colaboradores lidam com ela. Estas análises revelaram-se fundamentais para a fase que se segue. Este capítulo encontra-se apenas em acesso privado, mas no sumário estão indicados os pontos que foram desenvolvidos.

No quinto e último capítulo, sistematizam-se as bases para a implementação do Repositório Digital Seguro. Apresenta-se uma análise à conformidade nos serviços de Gestão Documental do Alfresco fazendo uma comparação com os requisitos do *Moreq* 2010 e da norma ISO 16363: 2012. O capítulo conta ainda com a exposição das bases para o planeamento da preservação em meio digital através da *framework Planets* e de ferramentas de planeamento da preservação da informação como o *Plato*, o *Scape* e o projeto *APARSEN* e ainda uma proposta para a desmaterialização da informação produzida e recebida. A parte referente à desmaterialização também se encontra somente em acesso privado.

Por fim são apresentadas as Conclusões e perspetivas futuras que podem ser retiradas deste projeto e os principais contributos e perceções a ter em conta para o trabalho futuro com vista à implementação de novas características e elementos no Repositório Digital Confiável/Seguro.

1. Gestão da Informação: Segurança e Preservação em meio digital

1.1 A Gestão da informação nas organizações

A informação é algo muito precioso e tornou-se num recurso estratégico para qualquer organização. É com ela que se tornam as decisões mais importantes e que levam a que a organização se torne competitiva e estratégica e se distinga no meio empresarial.

Como definir “informação”?

Segundo o Dicionário de Língua Portuguesa *online*, informação é:

“Derivação fem. sing. de informar, ato ou efeito de informar ou informar-se; comunicação; indagação, devassa; conjunto de conhecimentos sobre alguém ou alguma coisa; conhecimentos obtidos por alguém; facto ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens; elemento de conhecimento suscetível de ser transmitido e conservado graças a um suporte e um código”³.

Ao nível organizacional, a informação apresenta-se como algo que tem valor para a organização e lhe permite tomar decisões.

No *HARROD’S Librarian’s Glossary of Terms used in Librarianship* (1989) o termo informação vem definido como “um conjunto de dados registados de uma forma compreensível em papel ou outro meio, e capaz de comunicação” (Silva, et.al, 1999).

Segundo Silva et al. a “[...] informação parecerá, pois, uma espécie de ‘substância’, suscetível de ser movimentada, transferida, manipulada e ‘consumida’, muitas vezes com vista à satisfação de uma necessidade psicológica. Essa substância deverá ter existência material e, conseqüentemente, terá de ser depositada sobre algo manuseável, ou seja um suporte físico. É sinónimo de dados do conhecimento registado (registo da atividade humana) e por isso tem sido designada por informação documental... é este tipo de informação que, sendo materializado através das

mensagens contidas nos documentos, que constitui o objeto de interesse dos cientistas da informação ... " (Silva, et.al, 1999).

Na perspectiva da Ciência da Informação (CI) informação é definida como “o conjunto estruturado de representações mentais e emocionais codificadas (signos e símbolos) e modeladas pela interação social, passíveis de serem registadas num qualquer suporte material (papel, filme, banda magnética, disco compacto, etc) e, portanto, comunicadas de forma assíncrona e multidireccionada” (Silva e Ribeiro, 2002). A informação depende do processo que a produzem, e tem de ser vista em ligação com os meios operativos e na interação sistémica inerente ao processo informacional.

O objeto de estudo da CI é, assim, a informação, a sua constituição, organização, recuperação e comunicação. Silva e Ribeiro (2002) apresentam a CI como o campo científico que investiga as propriedades e comportamento da informação, as forças que regem o fluxo da informação e os meios de processamento da informação para um máximo de acessibilidade e uso. O processo inclui a origem, disseminação, coleta, organização, armazenamento, recuperação, interpretação e uso da informação. O campo deriva ou relaciona-se com a matemática, a lógica, a linguística, a psicologia, a tecnologia computacional, as operações de pesquisa, as artes gráficas, as comunicações, a biblioteconomia, a gestão e alguns outros campos.

Tendo como objeto a informação foi adotado para a CI, Ciência Social, o dispositivo metodológico quadripolar e a Teoria Sistémica como ferramenta interpretativa.

Associado ao conceito de informação encontram-se, assim, associados o conceito de Sistema de Informação (SI) e o de Sistema Tecnológico de Informação (STI).

De acordo com Silva (2006) o SI é “constituído pelos diferentes tipos de informação registada ou não externamente ao sujeito (...), não importa qual o suporte (material e tecnológico), de acordo com uma estrutura (entidade produtora/recetora) prolongada pela ação na linha do tempo”, distinguindo-se da plataforma tecnológica de suporte (Silva, 2006).

Pinto apresenta o STI como a “(...) plataforma tecnológica - meio físico/lógico de suporte à produção, transmissão, armazenamento e acesso à informação que constitui o SI propriamente dito” acrescentando que independentemente de se tratar de um SI digital, híbrido ou analógico será este, que identifica a missão/necessidades da

³ DICCIONARIO PRIBERAM DA LINGUA PORTUGUESA (2013). Priberam dicionário. *Informação*. Consultado em Dezembro 8, 2014, em <http://www.priberam.pt/DLPO/>

organização que o produz, acumula e usa e que norteia a função de gestão e os profissionais da informação por ela responsáveis (Pinto, 2010).

A informação se não for tratada nem gerida não serve de muito às organizações, é necessário avaliá-la, organizá-la e representá-la adequadamente para que se consiga decodificar adequadamente, é aí que surge o conceito de Gestão da Informação (GI).

Choo afirma que o objetivo principal da GI é aproveitar recursos de informação e capacidades de informação de modo a que a organização aprenda e se adapte ao seu meio ambiente em mudança. A criação, a aquisição, o armazenamento, a análise e a utilização da informação fornecem, portanto, a treliça intelectual que suporta o crescimento e o desenvolvimento da organização inteligente. No contexto organizacional, a informação tem contexto, tem um significado semântico, é enviada e recebida por uma pessoa, é transmitida através de um suporte, é uma entrada para a criação do conhecimento e é uma forma de representar conhecimentos (Choo, 2003). Para alguns autores a GI pode ser considerada como um conjunto de processos que apoiam e estão em simetria com as atividades de aprendizagem na organização.

Na opinião de Choo (2003) a GI enquadra-se tradicionalmente nas áreas dos Sistemas de Informação, Economia e Gestão Empresarial, correspondendo à gestão do conhecimento explícito permitindo a gestão dos objetivos, dos processos e demais recursos de uma organização. Por outro lado, a gestão do conhecimento é mais difícil de gerir, pois é o conjunto de atividades que controlam e desenvolvem todo o tipo de conhecimento numa organização.

As tecnologias da informação e comunicação (TIC) estão desde cedo associadas à GI. As TIC foram auxiliando as organizações na gestão quotidiana da informação e permitindo a integração da informação que resulta da atividade interna e externa, bem como na criação de memória organizacional, nomeadamente em repositórios onde é armazenada e disponibilizada para uso e promoção da aprendizagem organizacional.

Numa perspetiva CI, e de acordo com Silva, o conceito de GI encontra-se diretamente ligado ao ciclo de vida da informação, compreendendo uma “vasta problemática ligada à produção da informação (do meio ambiente à estrutura produtora, a operacionalização e utilidade da memória orgânica, os atores, os objetivos, as estratégias e os ajustamentos à mudança) em contexto orgânico institucional e informal” (Silva, 2009).

Ao enquadrar a preservação da informação como uma variável da GI (Pinto, 2009) e presente em todo o ciclo de vida da informação Pinto define a GI como a “gestão

integrada de todo o ciclo de vida da informação, incluindo a identificação, compreensão, representação lógica e redesenho dos processos organizacionais e configurações físicas e/ou meios tecnológicos que modelam a sua produção, fluxo, uso, disseminação e preservação, no contexto da ação humana e social” (Pinto, 2014).

Pinto e Silva (2005) afirmam que as organizações precisam de “uma abordagem que congregue, desde a fase de concepção da plataforma tecnológica (*hardware* e *software*), até à produção, circulação, avaliação, armazenamento, disponibilização e preservação da informação, toda a Organização e os seus processos de negócio”. É neste pressuposto que se desenvolve o SI-AP (Sistema de Informação - Ativa e Permanente), um modelo teórico de base sistémica que visa orientar uma organização e os seus colaboradores no processo de GI com vista a torná-la eficaz e uma “organização inteligente”.

Para que o SI-AP seja desenvolvido e preservado, por forma a garantir o acesso continuado no longo prazo e a segurança da informação que o integra, é necessário conhecer, compreender e representar o contexto organizacional para depois conhecer, compreender, organizar, representar e gerir o próprio SI (Pinto, 2009).

1.2 A Segurança da informação

A segurança da informação é essencial na Era da Informação em que vivemos e na qual há um rápido crescimento e proliferação da informação em meio digital. Por isso, torna-se essencial elaborar um conjunto de políticas de suporte essenciais para a observação dos três princípios básicos da segurança da informação: a confidencialidade, a integridade e a disponibilidade (Sousa, 2013). Citando Sousa estas políticas “colocam-se a outros níveis e, para serem efetivamente asseguradas, têm que ser equacionadas proporcionalmente à importância da informação, como ativo crucial em qualquer organização, e refletir o seu papel, presença e requisitos ou atributos que lhe são exigidos no seio e fora da Organização que a produz, recebe e acumula” (Sousa, 2013). Pensando na preservação a longo prazo aspetos como a autenticidade, a acessibilidade e a inteligibilidade são aspetos adicionais a ter em conta.

As boas práticas em segurança e preservação permitiram desenvolver normas como a ISO/IEC 27001:2005, a ISO 14721:2012 e a ISO 16363:2012 que são auxiliares fundamentais quando se pretende implementar um Repositório Digital para que seja

assegurada o armazenamento, salvaguarda, acesso e uso da informação digital (Sousa, 2013).

Neste sentido a Política de Segurança constitui-se como um documento de excelência que define as regras de segurança, apontando como um conjunto de procedimentos, princípios, normas e diretrizes que explicitam os requisitos do negócio de uma organização, protegendo por isso a informação da mesma. Esta deve alinhar-se com a Gestão de Risco de maneira a garantir o controlo e avaliação, tendo que ser revista periodicamente para adequar a eventuais alterações na organização (Sousa, 2013).

As Políticas de Segurança da Informação permitem a análise, identificação e tratamento das ameaças e risco obtendo por isso um maior controlo e prevenção sobre as mesmas. Assim uma Política de Segurança da Informação deve:

- ser aprovada pela Direção, publicada e comunicada a todos os funcionários e partes externas relevantes;
- indicar o compromisso da gestão e a abordagem da organização relativamente à gestão da segurança da informação;
- indicar uma definição de segurança da informação, os seus objetivos globais e âmbito, bem como a importância da segurança como um mecanismo facilitador da partilha de informação;
- conter uma declaração das intenções da gestão, apoiando os objetivos e princípios de segurança da informação em consonância com a estratégia de negócio e objetivos;
- conter uma *framework* que estabeleça os objetivos de controlo e controlos, incluindo a estrutura de avaliação e de gestão do risco;
- conter uma definição das responsabilidades gerais e específicas para a gestão da segurança da informação, incluindo o registo dos incidentes de segurança da informação;
- conter uma breve explicação das políticas, princípios, normas e requisitos de conformidade que se revelem de particular importância para a organização;
- ser analisada criticamente a intervalos planeados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia. (Sousa, 2013).

Ao pensar estrategicamente a Segurança e as Políticas a desenvolver deverá, também, ser pensada a Preservação da informação para, assim, responder a todos os atributos de informação que são essenciais para as organizações na Era da Informação e que são inseparáveis da GI e das suas políticas e estratégias.

1.3 Da Conservação à Preservação como variável da Gestão da Informação

A Conservação é uma área que vem despertando o interesse de vários autores desde o século XIX, mas, desde sempre, indivíduos e organizações procuraram proteger a informação que produziam. Com o fenómeno do “boom” de produção informacional e o aparecimento e rápida proliferação das TIC foi associada à ideia da Conservação o de Preservação a desenvolver pelos serviços de informação.

No dicionário brasileiro de terminologia arquivística o termo “conservação” aparece definido como “*Promoção da preservação e da restauração dos documentos*” e o termo “preservação” aparece como “*Prevenção da deterioração e danos em documentos, por meio de adequado controle ambiental e/ou tratamento físico e/ou químico*”⁴.

No HARROD’S *Librarian’s Glossary and Reference Book* (1987) o termo **Preservação** surge diretamente ligado aos arquivos e com duas aceções, sendo referido na primeira aceção, que a preservação constitui a função primordial dos arquivos, e, na segunda aceção, que engloba as medidas, quer individuais, quer coletivas, desenvolvidas para tratar, restaurar, proteger e manter os arquivos. Por sua vez, o termo **Conservação**, é definido como o renascer das preocupações com a constituição e manutenção das coleções das bibliotecas no longo prazo, uma preocupação desde sempre presente nas bibliotecas nacionais mas agora a alargar-se às bibliotecas públicas e aos investigadores, “[...] significando conservação a aplicação de procedimentos simples de tratamento e reforço de livros, capas, lombadas e o desenvolvimento de ações para a utilização de materiais fisicamente mais robustos na produção de livros [...]” (Pinto, 2009).

Também no *Dicionário de Terminologia Arquivística*, publicado nos anos 90, o termo **preservação** é definido como um “*conjunto de medidas de gestão tendentes a neutralizar potenciais fatores de degradação de documentos*”. Conservação é aqui definida como “*função do arquivo que consiste em assegurar a custódia e preservação dos arquivos*” (Alves, et.al 1993 *apud* Pinto, 2009).

Do ponto de vista do Novo Dicionário do Livro (1999) O termo **preservação** aparece definido em duas aceções nomeadamente como “*função de providenciar cuidados adequados à proteção e manutenção do acervo bibliográfico e documental de qualquer espécie, com vista a manter a sua forma original*” e em segundo como

⁴ ARQUIVO NACIONAL DO BRASIL (2005). Dicionário brasileiro de terminologia arquivística. Publicações técnicas: Rio de Janeiro. 232p. ISBN: 85-7009-075-7. Consultado em Dezembro 8, 2014 em <http://www.arquivonacional.gov.br/Media/Dicion%20Term%20Arquiv.pdf>

“Medidas coletivas e individuais tomadas no que respeita à reparação, restauro, proteção e manutenção do património bibliográfico”. Relativamente ao conceito de **conservação**, neste mesmo documento são apresentadas sete aceções nomeadamente *“ 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”, “Ações iniciais para conter o processo de degradação de um documento; centram-se em operações de proteção ao documento, como limpeza e manutenção de condições ideais de armazenamento que contribuam para garantir a sua integridade”, o termo é definido como “Proteção”; “Campo do conhecimento respeitante à coordenação, restauro, química do papel e outro material tecnológico, assim como outros conhecimentos relativos à preservação dos fundos arquivísticos”, “Preservação”; “Processo inicial de restauro” e por fim, “ Nome dado ao conjunto de processos que visam a estabilização mecânica e química dos materiais constituintes do documento gráfico” (Pinto, 2009)*

Numa perspetiva de Ciência da Informação, o conceito de Preservação assume uma única aceção que implica dois planos interrelacionados: *“a componente estratégica e de gestão”, e a conservação como “a componente operacional e a aplicação dos procedimentos, medidas e técnicas e o desenvolvimento de ações de proteção da informação” (Silva, apud Pinto, 2009)*

Quando se trata de **preservação** entra-se no campo da estratégica da Organização e gestão e ainda do ambiente externo que a rodeia. Esta é uma condição intrínseca na gestão de uma Organização [...] *devendo ser pensada no longo prazo e em termos de políticas, planos e programas, recursos e estrutura orgânica/funcional que os suporte tendo, consequentemente, implicações quer na fixação da Missão da Organização, quer nos objetivos (estratégicos e operacionais), quer nas metas fixadas, quer, ainda, nas ações/atividades e projetos planeados para os efetivar.* Ainda no que concerne à Gestão da Informação pode-se dizer que *“ A preservação projeta-se ao nível da gestão da Organização, da gestão do serviço de informação e da gestão do sistema de informação organizacional.” (Pinto, 2009)*

No que diz respeito à **Conservação**, esta adota contornos de cariz mais preventivo, onde são aplicadas medidas e técnicas que irão desenvolver, *“ações que garantirão a proteção da informação/documento, neutralizando potenciais fatores de degradação do meio material/tecnológico, tarefa preferencialmente a cargo de profissionais da informação com preparação específica” (Pinto, 2009).*

Como referido a Preservação tornou-se num dos grandes desafios do século XXI.

Com o aumento significativo da produção da informação criada em formato digital, tornou-se fundamental garantir que esta fosse preservada e que estivesse disponível por longos períodos de tempo.

Mas preservar o quê? Esta não é uma preocupação apenas de centros de documentação ou bibliotecas ou arquivos, preocupa todos aqueles que lidam com informação e que exerçam as suas decisões em função da informação produzida e recebida e que são cada vez mais relacionadas com a Preservação da informação digital.

A primeira prioridade e de acordo com Hofman (2001) é, salvar o que já existe tão bem quanto possível e, entretanto, tentar encontrar soluções mais permanentes. A este respeito é necessário para lidar com dois problemas ao mesmo tempo como os registos digitais já criados que precisam ser preservados, e a criação de um “ambiente” que cuida desses registos desde o início. A preservação da informação digital aplica-se à informação criada digitalmente e à convertida dos formatos convencionais.

Na área da preservação da informação digital e especialmente na preservação a longo prazo já existem muitas iniciativas e bastante promissoras.

Para a UNESCO (2003), a preservação digital *“Consists of the processes aimed at ensuring the continued accessibility of digital materials. To do this involves finding ways to re-present what was originally presented to users by a combination of software and hardware tools acting on data. To achieve this requires digital objects to be understood and managed at four levels: as physical phenomena; as logical encodings; as conceptual objects that have meaning to humans; and as sets of essential elements that must be preserved in order to offer future users the essence of the object”*.

Para Ferreira “A preservação digital consiste na capacidade de garantir que a informação digital permanece acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação” (Ferreira, 2006). “A preservação digital é, ao mesmo tempo, um tema novo, vasto e complexo. É um tema novo porque ele apenas se autonomizou e desenvolveu de forma visível há pouco mais de dez anos. É um tema vasto e complexo porque o conjunto de questões e problemas, quer de natureza conceptual e teórica, quer de natureza prática e tecnológica, é imenso. [...] O volume crescente, a heterogeneidade e as características da informação digital [...] tais como a facilidade de manipulação,

interligação e reutilização vão traduzir-se certamente no alargamento do campo da preservação digital” (Ferreira, 2006).

A proteção e preservação são competências desenvolvidas no sentido de manter a integridade da informação e a sua acessibilidade evitando uso inadequados por má interpretação ou/e representação da informação por parte dos sistemas computacionais (Thomaz e Soares, 2004).

Para alcançar qualquer solução a longo prazo requer compreensão acerca do que está acontecer no mundo. A fim de ser capaz de se adaptar às novas exigências e para agir (ou em alguns casos reagir) esta compreensão é crucial. Ela exige imaginação e pensar "fora do quadrado". Pensando em linhas tradicionais, não será suficiente, por causa do caráter inovador das Tecnologias da Informação (Hofman, 2001).

Pinto (2010) traça o roteiro da Preservação na Era da Informação representando no PRESERVMAP o desenvolvimento da atuação quer em suportes tradicionais, quer no novo “meio digital”. Cria, assim, um mapa que identifica duas rotas que se desenvolvem de forma paralela - a linha azul (tradicional) e a linha vermelha (preservação digital) - mas cujo *terminus* conflui para uma única e nova rota - a linha verde - (preservação perspectivada sistemicamente), refletindo o aparecimento das preocupações com a Preservação da informação em meio digital a par da tradicional área da Preservação e Conservação (P&C) e a proposta de confluência que considera indispensável.

Para Pinto (2007a) o objetivo da preservação em meio digital é garantir o acesso continuado à informação ao longo dos processos e atividades desenvolvidos em todo o seu ciclo de vida. No meio digital esse acesso é determinado não já em termos de “permanente” mas em termos do “tanto tempo quanto o necessário” dado que envolve também o “curto prazo”, e já não só o “longo prazo”, considerada a instabilidade do novo meio e a rapidez da obsolescência tecnológica.

Entre outros aspetos, a Preservação envolve a criação com intuito preventivo de um plano com descrição dos locais dos recursos e a aplicação dos métodos de preservação e tecnologias indispensáveis para que a informação digital seja acessível e usada por longos períodos de tempo tendo em conta os impactos das mudanças tecnológicas, ou seja, caso o ambiente original em que foi criado se torne obsoleto.

Neste sentido, e segundo Pinto, deve-se olhar para a Preservação como variável da GI. Pinto (2013) afirma que se entra no campo estratégico como algo que deve ser pensado a longo prazo e em termos de políticas, planos e programas, recursos e estrutura orgânica/funcional e tecnológica que os suporte, tendo,

consequentemente, implicações quer na fixação da Missão da Organização (qualquer que seja), quer nos objetivos (estratégicos e operacionais), quer nas metas fixadas, quer ainda, nas ações/atividades e projetos planeados para os efetivar. Há que haver um alinhamento organizacional da estratégia para a Gestão da Informação com a estratégia da Organização. A preservação é algo que deve começar desde logo na conceção e implementação da plataforma tecnológica na qual será produzida, organizada, armazenada e difundida a informação, nomeadamente no *software* utilizado, nos formatos adotados, na recolha, na fase e momento próprio, da meta-informação administrativa, técnica, estrutural, descritiva ou de preservação que permita a sua futura referência e o desencadear das diferentes estratégias de preservação que agirão sobre as diferentes dimensões, seja a bidimensionalidade do documento analógico, seja a pluridimensionalidade do “objeto” digital (Pinto, 2013).

A preservação da informação em meio digital assenta numa pluridimensionalidade que integra de acordo com Thibodeau (2002) quatro dimensões: a **dimensão física**, a **dimensão lógica**, a **dimensão conceptual/intelectual** e a **dimensão essencial** (Pinto, 2009).

A **dimensão física** apresenta-se no conjunto de registos gravados em diversos suportes como discos, disquetes, CD's ou DVD's; a **dimensão lógica** depende da dimensão física do objeto apresentando-se no conjunto de informação que está organizado em estruturas de diferentes formatos como .pdf, .doc, que envolve a utilização do hardware e software para decodificar a informação; na **dimensão conceptual** os sinais digitais transformam-se em sinais analógicos na qual o código adquire significado ao ser humano; por último a **dimensão essencial** garante que os diferentes contextos de produção informacional são perceptíveis, salvaguardando a meta-informação técnica, administrativa, descritiva e/ou estrutural, garantindo a capacidade de a “unidade informacional ser auto demonstrável, mantendo ligados a si, os elementos contextualizadores da sua produção e ciclo de vida, sob o ponto de vista contextual/ambiental - interno e externo, informacional, orgânico, funcional e tecnológico” (Pinto, 2009).

1.4 Uma Política de Preservação da Informação Integrada

Implementar uma *Política de Preservação* que esteja alinhada com a GI na Organização é essencial para garantir a autenticidade, a responsabilidade, o não-repúdio e a confiabilidade na informação (e par da acessibilidade e inteligibilidade).

Segundo a norma ISO 16363:2012, a política de preservação define-se como uma declaração por escrito que foi autorizada pela administração do repositório, na qual são descritos os procedimentos que devem ser tomados pelo repositório para promover a preservação dos objetos digitais. Esta política de preservação deverá portanto estar em concordância com o plano estratégico de preservação.

De acordo com Ferreira (2009) uma política de preservação envolve, geralmente, todas as facetas de um arquivo/repositório, implicando a criação de políticas de avaliação e seleção de materiais, a identificação de esquemas de meta-informação apropriados (e.g. meta informação descritiva, técnica, de disseminação, estrutural e de preservação), a definição de estratégias de preservação adequadas a cada classe de objetos digitais, a criação de planos de sucessão para a eventualidade da Organização detentora da informação interromper a sua atividade, a utilização de modelos sustentáveis de financiamento, entre outros.

O mesmo autor afirma, ainda, que uma política de preservação deve descrever com clareza todas as estratégias que foram adotadas para a preservação dos materiais em todos os níveis de abstração, sendo eles, o físico, lógico e concetual, e ainda o social, económico e o organizacional (Ferreira, 2009).

Vários investigadores em diversas partes do mundo desenvolvem modelos para promover a preservação a longo prazo da informação em meio digital. Beagrie e Greenstein indicam precauções básicas para reduzir o perigo da perda:

- armazenar em ambiente estável e controlável;
- implementar ciclos de atualização (*refreshment*) para cópia em novos suportes;
- fazer cópias de preservação (assumindo licenças e permissões de copyrights);
- implementar procedimentos apropriados de manuseamento;
- transferir para um suporte de armazenamento normalizado (Beargrie e Greenstein, 1998 *apud* Miguel Arellano)

Em 1999, Feeney apontou três estratégias para a preservação da informação digital nomeadamente:

- Preservar o *software* original (e possível *hardware*) que foi utilizado para criar e aceder à informação. Esta é conhecida como a estratégia de preservação da tecnologia que envolve também preservar tanto o sistema operacional original como o *hardware* que é necessário para executá-lo.
- Programar sistemas de computadores poderosos para que no futuro possam emular os mais antigos que possam estar obsoletos.

- Certificar-se que a informação é recodificada em novos formatos antes do formato original se tornar obsoleto. Uma estratégia de migração da informação digital. (*Digital Preservation Coalition*, 2008).

Os National Archives (UK) afirmam que para a implementação de uma estratégia de preservação de informação digital deve haver um mecanismo formal de aceitação de registos (*records*) incluindo uma norma aceite para formatos de ficheiro e níveis de descrição para os registos; também um processo seguro para a transferência de registos para armazenamento, garantindo uma gestão adequada (incluindo verificações de integridade). Torna-se necessário mapear processos para capturar a meta-informação descritiva numa base de dados pesquisável ligada aos registos, permitindo que permaneçam localizáveis; um mecanismo formal para fornecer aos utilizadores o conteúdo dos registos preservados no formato mais apropriado para o mesmo; e ainda implementar um rigoroso sistema de monitorização das atividades de preservação que possa produzir dados de auditoria utilizáveis.

No que respeita à *Política de Preservação Digital* esta deve prover a preservação e o acesso continuado à informação a longo prazo e para isso, de acordo com os National Archives (UK):

- atribuir a responsabilidade e apropriação da política a um elemento sénior dentro da Organização (ou seja, um diretor ou chefe de serviço);
- direcionar quais os procedimentos a seguir e fazer referência a qualquer orientação interna/outras políticas a serem seguidas;
- alinhar a política de preservação digital com outras políticas relevantes, incluindo a gestão de informação a preservar, a proteção de dados, a segurança da informação, etc.;
- apoiar a estratégia de preservação da informação digital. (The National Archives)

1.5 Instrumentos normativos e orientadores

Na preservação de informação criada digitalmente ou transformada em formato digital é recomendável seguir um conjunto de normas e orientações que como o próprio nome indica apoiam as práticas da preservação e permitem a normalização o que não substitui que o processo de GI que lhes está subjacente tenha que estar teórica e metodologicamente sustentado e gere o conhecimento necessário para

avançar para a operacionalização com o suporte normativo. Entre os instrumentos orientadores e normativos existentes destacam-se:

MoReq - *Modelo de Requisitos para a Gestão de Arquivos Eletrónicos*, é uma especificação de requisitos para um sistema de gestão de documentos de arquivo (SGDA) que foi desenvolvida pelo DLM Fórum⁵ com o apoio e suporte da Comissão Europeia. Foi publicado primeiramente em 2001 e tem dado provas de ser um recurso útil na prática da preservação digital, sendo uma norma utilizada em todo o mundo. Foi feita uma revisão em 2008 para avaliação e atualização dos requisitos na qual deu origem ao MoReq2, que teve como principais modificações a inclusão de um esquema de dados XML baseado no MoReq, uma *framework* de teste e a adição de um capítulo zero com o objetivo de fornecer orientação para os requisitos legais e normativos a nível nacional. A versão atual é o MoReq2010 agora direcionado a serviços (Vieira e Borbinha, 2011; Gavina, 2014).

ISO 15489 (1,2) - *Information and documentation - Records Management* - Esta Norma fornece orientações sobre a gestão de registos de organizações públicas ou privadas, para clientes internos e externos. Aplica-se à gestão de registos, em todos os formatos e suportes, criados ou recebidos por qualquer Organização pública ou privada na condução das suas atividades, ou qualquer indivíduo com o dever de criar e manter registos; fornece orientação sobre como determinar as responsabilidades das organizações de registos e políticas, procedimentos, sistemas e processos de registos, assim como orientação sobre gestão de registos em apoio a uma estrutura de processo de qualidade em conformidade com as normas ISO 9001 e ISO 14001; e ainda orientação sobre a conceção e implementação de um sistema de registos, mas não inclui a gestão de documentos de arquivo dentro de instituições arquivísticas.

ISO/TS 23081 (1,2,3) - *Information and documentation - Records management processes Metadata for records*, que complementa a ISO 15489 ao nível da meta-informação - abrange os princípios que sustentam e governam a meta informação da gestão de registos. Estes princípios aplicam-se ao longo do tempo para registos e sua meta-informação; para todos os processos que lhes dizem respeito; qualquer sistema em que residem; e para qualquer Organização que é responsável pela sua gestão.

⁵ O DLM Fórum foi fundado pela Comissão Europeia e pela primeira vez em 1996. Trata-se de uma vibrante comunidade de arquivos públicos e partes interessadas de todo governo, setores comerciais, académicos e voluntários que são ativos na governança de informações, incluindo arquivos, registos,

ISO 14721:2003 - *Space data and information transfer systems. Open archival information system (OAIS). Reference model*- Esta Norma especifica um modelo conceptual de referência para a criação de arquivos digitais. O seu objetivo é estabelecer um sistema de arquivo de informação, tanto digitalizada como física, com uma estrutura organizacional composta por pessoas que aceitam a responsabilidade de preservar a informação e disponibilizá-la para uma designada comunidade. Este modelo de referência aborda uma gama completa de funções para arquivo e preservação da informação, incluindo ingestão, armazenamento, gestão de dados, preservação, acesso e disseminação. Aborda igualmente a migração de informação digital para novos suportes e formatos, os modelos de dados usados para representar a informação, o papel do *software* na preservação da informação, bem como a troca de informação digital entre os arquivos.

ISO/TR 15801:2004 - *Electronic Imaging - Information stored electronically - Recommendations for trustworthiness and reliability* - Esta norma descreve a metodologia de implementação e operação de sistemas tecnológicos de suporte à GI e que armazenam a informação em formato eletrónico, onde a fiabilidade, autenticidade e integridade, são fatores de extrema importância. O ciclo de vida dos documentos armazenados eletronicamente deve ser abordado desde a sua criação e/ou captura, até à sua destruição.

ISO/TR 18492:2005 - *Long-term preservation of electronic document-based information* - fornece orientações práticas metodológicas para a preservação a longo prazo e recuperação de informação autêntica quando o período de retenção excede a expectativa de vida da tecnologia (hardware e software) utilizada para criar e manter essa informação.

Estas orientações reconhecem também que garantir a preservação a longo prazo e recuperação da informação deve envolver especialistas de TI e profissionais da informação.

ISO 16363:2012 - *Space data and information transfer systems - Audit and certification of trustworthy digital repositories* - Define um Guia de práticas recomendadas para desenvolver um processo de certificação e de auditoria para

avaliar a confiabilidade de um repositório digital, no âmbito da preservação em meio digital.

ISO/IEC 27001:2005 - Information technology. Security techniques. Information security management systems. Requirements. - Aborda os requisitos para a estruturação de um SGSI, e daqui obter a certificação em segurança da informação. Defende que o SGSI deve ser uma decisão estratégica para a Organização, providenciando um modelo para seu estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria. Naturalmente que, para o planeamento de um sistema deste género, há diversas condicionantes que têm que ser tidas em conta, nomeadamente: as necessidades e objetivos, os requisitos de segurança, os processos, assim como o tamanho e estrutura da Organização.

2. Repositórios Digitais: confiança, segurança e preservação

2.1 Repositório digital: conceito e modelo

A propósito quer da GI, quer da segurança da informação, quer da sua preservação em contexto de utilização das TIC, surge o repositório como componente imprescindível e auxiliadora no processo da própria preservação.

Nesta dissertação a segurança e a preservação da informação incidem no repositório digital, mas, como se pode verificar, este projeto não poderia ser olhado sem abordar a Organização Multicert, as suas políticas, estratégias, processos, atores e, sobretudo, o sistema de informação organizacional a proteger e preservar.

Os repositórios são apresentados de diferentes formas e perspetivas, com uma grande variedade de contextos, comunidades, objetivos e práticas ligadas à sua criação e funcionamento, podem ser colaborativos e apresentar um baixo controlo dos conteúdos e de acesso aos documentos, como podem ter um alto nível de controlo (Masson, 2008).

Para alguns autores constituem uma “ferramenta de TI” que permite o armazenamento da informação produzida no decorrer das funções de qualquer Organização e, de acordo com o Infokit⁶, um repositório digital é um “meio” de gestão, armazenamento e fornecimento de acesso a conteúdo digital.

Um repositório é um local onde se guarda informação e serve para armazenar, preservar e difundir a informação que contém. Desta forma, é um termo com uma aceção específica no meio digital, devendo ser sustentável e fiável, como também deve ser bem enquadrado e bem gerido.

Segundo Masson os repositórios digitais têm como objetivo “preservar as publicações criadas em meio digital, ou as que são digitalizadas, referentes a artigos em periódicos, ou na *web*, os próprios periódicos, as atas de congresso e outros eventos, trabalhos de pesquisas, teses e dissertações para que constituam uma memória institucional e que possam estar disponível e acessível a quem precisar

⁶ JISC INFONET (2014). Infokits. *Repositórios*. Consultado em Abril 21. 2015 em <http://www.jiscinfonet.ac.uk/infokits/repositories>

consultá-la, ou, no caso dos repositórios digitais temáticos, a memória do conhecimento em uma área especializada do conhecimento” (Masson, 2008).

Na opinião de Arettio (2005) os “objetos de aprendizagem” são fundamentais para complementar os repositórios, de forma em que os objetos de aprendizagem como por exemplo um gráfico, um esquema ou mesmo um mapa são essenciais.

No entanto, os repositórios não se destinam apenas à produção científica ou ao armazenamento de informação de carácter pedagógico, podendo qualquer Organização ter necessidade de criar o seu repositório de informação organizacional produzida em meio digital.

Um repositório digital deve, assim, ter como características fundamentais a reutilização, a acessibilidade, a durabilidade, a flexibilidade, a versatilidade, a interoperabilidade e a inteligibilidade, mas também garantir a confidencialidade, a autenticidade, a integridade e o não-repúdio da informação nele contido.

Inseparável da estruturação de um repositório é o modelo conceptual que orienta essa construção.

O Modelo de referência OAIS é o modelo mais utilizado a nível mundial e foi publicado em 2002 pelo *Consultative Committee for Space Data Systems* (CCSDS) e adotado como norma em 2003 (ISO 14721:2003), tendo como propósito fundamental a preservação e acesso à informação a longo prazo.

Este modelo é um esquema conceptual com regras e linhas orientadoras para sensibilizar as pessoas de modo a ampliar a consciência e compreensão de conceitos, definir terminologias para descrever e comparar modelos de dados e arquiteturas de arquivo, promovendo o consenso sobre os elementos e os processos relacionados com a preservação e acesso à informação digital (CCSDS, 2012).

Este modelo conceptual, ou esquema básico, é considerado uma ferramenta para a melhoria da comunicação e produtividade entre os diversos níveis e as diferentes comunidades. É conhecido como um Sistema Aberto de Arquivo de Informação (SAAI) e resultou da discussão aberta entre diversas comunidades e apoio de duas importantes instituições com grande influência internacional e ampla experiência no desenvolvimento de normas (Backer, et.al 2009).

O OAIS considera os arquivos como organizações de pessoas e sistemas que aceitaram a responsabilidade de preservar a informação e torná-la disponível e melhorar a comunicação e produtividade entre diferentes comunidades (CCSDS, 2012). No modelo atuam três entidades: o produtor, o consumidor, e o administrador.

Contém, ainda, um modelo de informação para inserção da meta-informação de preservação (figura 1).

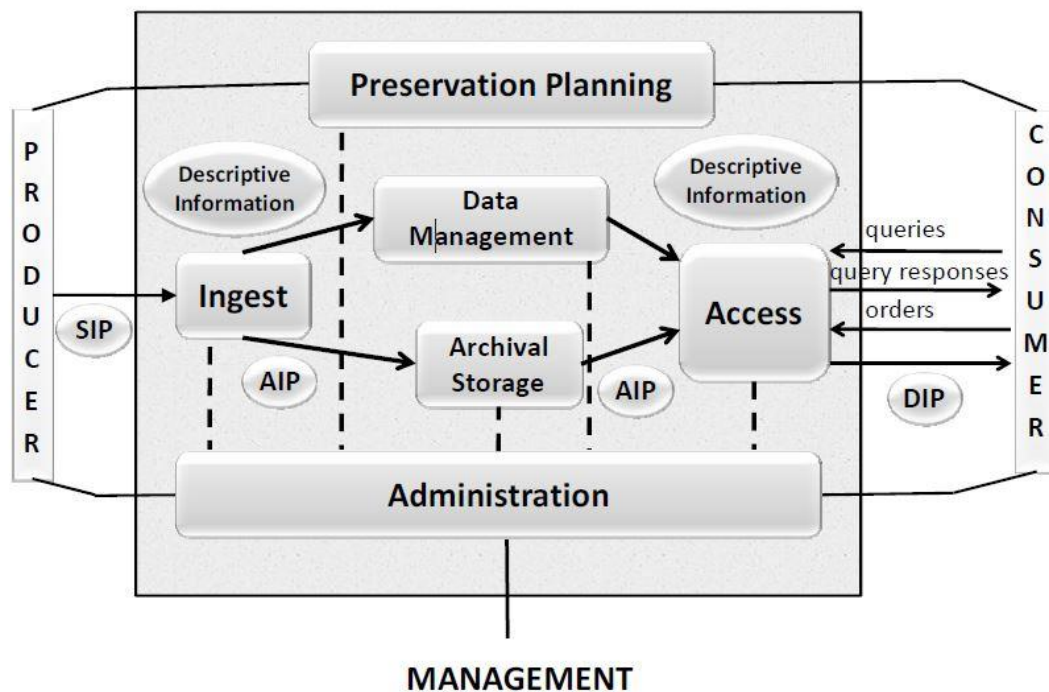


Figura 1 Modelo conceitual OAIS (CCSDS, 2012)

O modelo de referência OAIS ao detalhar os tipos de informação necessária para a preservação dos objetos digitais (Informação Descritiva de Preservação), constitui, de certo modo, o ponto de partida para a reflexão sobre a meta-informação, genericamente descrita como sendo informação sobre informação, uma definição que radica na própria etimologia da palavra, em que o prefixo “meta” indica que algo se aplica a si mesmo. Incide particularmente na meta-informação que é necessária para assegurar a preservação e acesso da informação digital a longo prazo, logo na importância da meta-informação de preservação.

2.2 Confiança e certificação em repositórios digitais

Seja qual for a plataforma de suporte ou as estratégias de preservação adotadas, um repositório deve corresponder às expectativas criadas pelos seus utilizadores. Afirmar que se é capaz de garantir o acesso continuado à informação digital não é suficiente para estabelecer um clima de confiança junto dos vários intervenientes que interagem com o repositório, i.e. produtores, consumidores, operadores do

sistema, gestores, entidades de fomento, ou outros. Para que um repositório seja verdadeiramente confiável, é fundamental que existam formas de medir e demonstrar essa confiabilidade (RLG et al., 2007).

“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. In this report the working group has articulated a framework of attributes and responsibilities for trusted, reliable, sustainable digital repositories capable of handling the range of materials held by large and small research institutions.” (RLG/OCLC, 2002)

Um repositório digital confiável é um repositório digital que é capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário. Para cumprir essa missão, segundo o relatório *“Trusted Digital Repositories: attributes and responsibilities”* (RLG/OCLC, 2002), os repositórios digitais confiáveis devem:

- aceitar, em nome de seus depositantes, a responsabilidade pela manutenção dos materiais digitais;
- dispor de uma estrutura organizacional que apoie não somente a viabilidade de longo prazo dos próprios repositórios, mas também dos materiais digitais sob sua responsabilidade;
- demonstrar sustentabilidade económica e transparência administrativa;
- projetar os seus sistemas de acordo com convenções e padrões habitualmente aceites, no sentido de assegurar, de forma contínua, a gestão, o acesso e a segurança dos materiais depositados;
- estabelecer metodologias para avaliação dos sistemas que considerem as expectativas de confiabilidade esperadas pela comunidade;
- considerar, para desempenhar as suas responsabilidades de longo prazo, os depositários e os utilizadores de forma aberta e explícita;
- dispor de políticas, práticas e desempenho que possam ser auditáveis e mensuráveis; e observar os seguintes fatores relativos às responsabilidades organizacionais e de curadoria dos repositórios: objetivo dos materiais depositados, gestão do ciclo de vida e preservação, atuação junto a uma ampla gama de parceiros, questões legais relacionadas com a propriedade dos materiais armazenados e implicações financeiras.

O repositório deve acima de tudo ser seguro, não se limitando apenas aos aspetos tecnológicos mas também às instalações físicas e às ações pessoais. Estes devem

incluir de uma análise sistemática da informação, sistemas, pessoas e instalações físicas; adotar procedimentos de controlo para tratar adequadamente as necessidades de segurança; delinear papéis, responsabilidades e autorizações relativas à implementação de mudanças no sistema; e por fim criar um plano de prevenção de desastres e de reparação, que inclua, ao menos, um *backup*, *offsite*, de tudo o que é mantido no repositório (documentos, meta-informação, trilhas de auditoria etc.), inclusive do próprio plano de reparação (Conarq⁷).

2.3 O repositório seguro: modelos, especificações e ferramentas para a certificação

A preservação é uma condição *sine qua non* para garantir a qualidade, partilha e uso da informação no longo prazo em repositórios digitais sustentáveis. A informação criada precisa ser gerida, preservada e arquivada de modo a que a resposta às necessidades e memória organizacional e os elevados investimentos na sua produção, preparação e apresentação não sejam perdidos.

A certificação é fundamental para garantir a confiabilidade dos repositórios digitais e, portanto, para sustentar as oportunidades para o acesso e uso da informação no longo prazo e serviços correspondentes.

Nos últimos anos, têm sido desenvolvidas em todo o mundo uma série de normas para a certificação e procedimentos de acreditação, nomeadamente: o *Data Seal of Approval* (DSA), a Rede de Especialização no Armazenamento e Acessibilidade dos Recursos Digitais no longo prazo na Alemanha (NESTOR); o TRAC e a norma ISO:16363, e a certificação WDS, do Conselho Internacional de Ciência do Sistema Mundial de Dados (ICSU-WDS).

Neste contexto, e no que respeita a uma visão global do trabalho a desenvolver, e dado constituir uma proposta recente no âmbito internacional, será considerado no projeto de dissertação o *European Framework for Audit and Certification of Digital Repositories*.

A criação do *European framework* em 2010, direcionado à auditoria e certificação de Repositórios Digitais, resulta da congregação de esforços de três entidades que trabalham no âmbito da certificação de repositórios⁸:

⁷ CONARQ (2014). Conselho Nacional de Arquivos. *Diretrizes para a Implementação de Repositórios Digitais Confiáveis de Documentos Arquivísticos*. Consultado em Mar 15. 2015 em <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>

⁸ No domínio da investigação a partilha de dados está longe de ser uma prática comum. Embora proporcione uma série de vantagens (transparência, capacidade de se replicar e verificar, reutilização

- o CCSDS (Consultative Committee for Space Data Systems)/ISO Repository Audit and Certification Working Group (RAC);
- o Data Seal of Approval Board;
- e o DIN Working Group “Trusted Archives - Certification”;

Estas entidades pretendem “(...) *put in place mechanisms to ensure that the groups can collaborate in setting up an integrated framework for auditing and certifying digital repositories*”.

Esta *Framework* é composta por uma sequência de três níveis de certificação, correspondendo ao aumento da confiabilidade obtida:

1. a certificação básica (*basic certification*) que é concedida aos repositórios que obtêm certificação Data Seal of Approval (DAS);
2. a certificação alargada (*extended Certification*) que é concedida aos repositórios com a certificação básica e que realizam adicionalmente uma autoavaliação estruturada, com revisão externa e disponível publicamente, baseadas na ISO 16363, ou na DIN 31644;
3. a certificação formal (*formal certification*) que é concedida aos repositórios que obtêm, além da certificação básica, uma auditoria externa total e certificação conforme à ISO 16363 ou 31644 DIN.

A concessão desses certificados permitirá aos repositórios mostrar um dos três símbolos nas suas páginas web e outros documentos, além de quaisquer outras marcas de certificação da DSA, ISO ou DIN.

O DSA e o WDS oferecem uma certificação básica para repositórios digitais confiáveis. A sua especificação de requisitos e os seus procedimentos de avaliação baseiam-se nos mesmos princípios de abertura e transparência, no sentido de um justo equilíbrio entre a simplicidade e robustez do trabalho e esforço envolvidos.

O *Data Seal of Approval*⁹, criado em 2009, constitui-se como um selo de aprovação de dados para repositórios digitais que garante que a informação arquivada possa ser encontrada, compreendida e utilizada no futuro.

As Diretrizes de qualidade formuladas na *Data Seal of Approval* são de interesse para os produtores e instituições que criam e trabalham com “dados” digitais, para as organizações que armazenam informação, e para os consumidores de informação, nomeadamente dados científicos. Os objetivos do Selo de Aprovação de Dados são:

de dados, maior retorno sobre o investimento), os investigadores ainda argumentam que não podem confiar em dados produzidos em outro lugar por outra pessoa o que veio reforçar a necessidade de estudar formas que contribuam para a criação de confiança num sistema de repositórios digitais.

⁹ DATA ARCHIVING AND NETWORKED SERVICES . Data Seal of Approval. Consultado em Mar 20. 2015 em <http://www.datasealofapproval.org/en/>

proteger os dados, garantir uma alta qualidade e orientar o manuseamento de dados confiáveis no futuro sem a necessidade da implementação de novas normas, regulamentos ou custos elevados.

Os objetivos do *Data Seal of Approval* é dar aos produtores a garantia de que a sua informação/dados e materiais associados serão armazenados de forma fiável e podem ser reutilizados, proporcionando aos organismos de financiamento confiança de que os dados continuarão disponíveis para reutilização e os seus investimentos não serão perdidos. Dá também suporte aos repositórios de dados para um arquivo e distribuição eficiente da informação/dados.

Trata-se, portanto, de um conjunto de boas-práticas que se pretendem que sejam seguidas sobretudo por organizações responsáveis pela preservação de dados científicos.

É composto por 16 requisitos baseados em 5 critérios: que os dados podem ser encontrados na internet; que estão acessíveis; que estão num formato usável; que são confiáveis; e que são identificados num modo único e persistente.

Dos 16 requisitos, 3 dizem respeito aos produtores e ao processo de ingestão, 10 à qualidade do repositório e 3 ao acesso à informação por parte dos consumidores. O cumprimento de cada requisito é avaliado numa escala de 0-4.

Por sua vez, o ICSU - WDS¹⁰ foi criado pelo Conselho Internacional para a Ciência (ICSU) em outubro de 2008. Os objetivos do sistema de dados WDS são: preservar a qualidade de dados científicos e outra informação; facilitar o acesso aberto; e promover a adoção de normas.

O novo sistema baseia-se no potencial oferecido pelas interligações entre os componentes avançados de gestão de dados para promover aplicações disciplinares e multidisciplinares para o benefício da comunidade científica internacional e outras partes interessadas.

Até ao momento, as duas normas têm evoluído e operado de forma independente.

O foco principal da DSA tem sido em repositórios digitais nas Ciências Humanas e Sociais. Por razões históricas, o foco do ICSU-WDS tem sido em Ciências da Terra e do espaço. Ambas as iniciativas, no entanto, têm missões totalmente multidisciplinares.

Embora as duas organizações tenham diferenças consideráveis, a parceria promoverá ganhos de eficiência, simplificação de opções de avaliação, estimulando mais certificações, e aumentando o impacto na comunidade e como um possível

¹⁰ INTERNATIONAL COUNCIL OF SCIENCE. World Data System (WDS). Consultado em Mar 20, 2015 em: <http://www.icsu.org/what-we-do/interdisciplinary-bodies/wds/?icsudocid=about>

primeiro passo para o desenvolvimento de um quadro comum para a certificação e um serviço de repositórios de dados confiáveis.

No que concerne aos modelos de requisitos de auditoria e certificação é de referenciar o TRAC publicado em 2007 pela *Research Library Group* (RLG) e pelo *National Archives and Records Administration* (NARA). Este contém um conjunto de requisitos que vão desde a gestão organizacional às infraestruturas de suporte que visam assegurar a confiança em torno de um repositório e que estarão na base da ISO 16363.

O TRAC tem como objetivo fornecer uma ferramenta que permita auditar, avaliar, e certificar os repositórios digitais, identificando para isso a documentação necessária para realizar uma auditoria e estabelecendo metodologias apropriadas para determinar a robustez e a sustentabilidade do repositório digital.

Nele é definido o conceito de “confiança” no contexto de um repositório digital: *“is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future. In this report the working group has articulated a framework of attributes and responsibilities for trusted, reliable, sustainable digital repositories capable of handling the range of materials held by large and small research institutions”*.(RLG/OCLC, 2002). Este modelo potencia a confiança junto dos utilizadores do repositório pois estabelece um ambiente de transparência nos processos que são implementados e auxilia na realização de auditorias internas e externas ao repositório.

A preservação digital é, também, definida no documento como *“the managed activities necessary for ensuring both the long-term maintenance of a bytestream and continued accessibility of its contents.”* (RLG/OCLC, 2002). Um repositório digital confiável deverá conseguir detetar os riscos e ameaças ao sistema.

Este documento apresenta-se sob a forma de uma *checklist* que contém os requisitos que um repositório digital deve possuir para que se possa tornar confiável e seguro. Esta *checklist* serve, numa primeira instância, como ferramenta de autodiagnóstico e, posteriormente, de autoavaliação. Este instrumento permite identificar potenciais omissões e pontos de falha nos sistemas e organizações responsáveis pela preservação da informação digital. (RLG et al., 2007)

Por sua vez, a Organização responsável pelo repositório deverá ser capaz de identificar potenciais riscos e prevenir ameaças, transmitindo confiança a quem utiliza os repositórios pois oferece uma imagem de maior transparência dos processos implementados no repositório e de tudo aquilo que lhe é inerente. (RLG et al., 2007)

Como o resultado de anos de trabalho desenvolvido em torno da *checklist* do TRAC acaba por surgir a norma ISO 16363:2012 - *Space data and information transfer systems - Audit and certification of trustworthy digital repositories*, que apresenta como objetivo essencial fornecer uma lista de requisitos a partir da qual se possam realizar auditorias aos repositórios no sentido do controlo de ameaças e riscos à sua segurança com base em 109 critérios.

Como fica patente neste objetivo são equacionados na *checklist* quer requisitos de preservação, quer requisitos de segurança, constituindo a mesma a principal referência a usar no presente projeto de dissertação por forma a desenvolver e completar a abordagem efetuada na perspetiva das tecnologias com as normas da série ISO 27000, a que se deverão acrescer as orientações ao nível da Gestão do Risco, nomeadamente, os inerentes ao meio digital.

Para auditar repositórios de maneira a torná-los íntegros, seguros e confiáveis, a própria norma referencia como áreas que devem ser auditadas e avaliadas as seguintes:

1. Infraestrutura organizacional (25 critérios);
2. Gestão de objetos digitais (60 critérios);
3. Infraestrutura e Gestão de Riscos de Segurança (24 critérios).

A abordagem a realizar deverá contemplar toda a estrutura subjacente ao repositório através da definição de políticas e procedimentos que reflitam a gestão das unidades informacionais digitais, o armazenamento e preservação, a segurança e gestão de acessos, e a infraestrutura tecnológica.

A estrutura documental de suporte deve contemplar os critérios estabelecidos na ISO 16363:2012, de forma a proporcionar evidências de que se encontra em conformidade com a mesma (Sousa, 2013).

Sousa procedeu à tradução dos requisitos incorporados na norma (Sousa, 2013, 2014), referenciando o conjunto de documentos que se revelam essenciais, nomeadamente:

- Declaração de Missão, Visão e Objetivos e a definição da comunidade-alvo;
- Política e a Estratégia de Preservação - que definem a abordagem do repositório relativamente à preservação a longo prazo das unidades informacionais digitais;
- Planos de Contingência;
- Políticas de Segurança;
- Política de Gestão do Risco;
- Políticas de acesso à informação em meio digital;

- Definição das Estratégias de armazenamento e de migração/conversão das unidades informacionais digitais;
- Identificação de esquemas de meta-informação adotados;
- Fichas/Manual de procedimentos de manutenção de *software* e *hardware*;
- Análises de custo-benefício, entre outros (Sousa, 2013).

O estudo de Sousa foi completado com a análise efetuada por Oliveira com base em casos de boas práticas de implementação, propondo uma estrutura de políticas que abarca de forma integrada a perspetiva pela preservação e a perspetiva pela segurança. Ambos constituíram referências para o projeto desenvolvido na Multicert (Sousa e Oliveira, 2014; Oliveira, 2014; Sousa, 2013).

Relacionado com o processo de desenvolvimento do TRAC é de referenciar uma ferramenta aplicável à auditoria e gestão do risco em repositórios, o *Drambora*.

Desenvolvido pelo *Digital Curation Centre* (DCC)¹¹ e pelo *Digital Preservation Europe* (DPE)¹², o *Drambora*¹³ tem por base uma versão preliminar do TRAC e nasceu da experiência acumulada em várias auditorias ao longo do ano de 2006 e 2007.

Trata-se de um documento e uma ferramenta interativa que sistematiza um processo de autoavaliação focando-se mais em aspetos ligados à gestão estratégica e à Organização e menos em aspetos técnicos relacionados com o repositório e a respetiva plataforma tecnológica.

O *Drambora* permite aos administradores de repositórios digitais:

- Elaborar um perfil organizacional, descrevendo e documentando a sua política de depósito, objetivos, responsabilidades, atividades e material armazenado;
- Identificar e avaliar os riscos que poderão impedir a prossecução da sua missão e que ameaçam a salvaguarda da sua informação;
- Gerir eficazmente os riscos, mitigando a sua probabilidade de ocorrência;
- Estabelecer planos de contingência eficazes para minimizar os efeitos provocados por riscos que não puderam ser evitados.

Apresenta uma abordagem mais focada na identificação e gestão de risco e na prevenção de ameaças que é realizada em 6 etapas:

¹¹ O Centro Curadoria Digital (DCC) é um centro líder mundial de experiência em curadoria de informação digital com foco na criação de capacidade e habilidades para a gestão de dados de pesquisa na maior comunidade de pesquisa da educação do Reino Unido.

¹² O DigitalPreservationEurope (DPE) promove a colaboração e sinergias entre muitas iniciativas nacionais existentes em toda a Investigação do Espaço Europeu. Este aborda a necessidade de melhorar a coordenação, cooperação e consistência das atividades em curso para garantir a preservação eficaz de materiais digitais.

¹³ DRAMBORA. Digital Repository Audit Method Based on Risk Assessment. Consultado em Mar 20, 2015 em <http://www.repositoryaudit.eu/>

1. Identificação do contexto organizacional;
2. Documentação da política e procedimentos de gestão;
3. Identificação de atividades, recursos e os respetivos responsáveis;
4. Identificação de riscos;
5. Análise e avaliação dos riscos;
6. Gestão de riscos. (*Digital Curation Centre e Digital Preservation Europe, 2007*)

O processo permite aos administradores de repositórios identificar e categorizar as áreas onde existe maior probabilidade de falha e prevenir a sua ocorrência (*Digital Curation Centre e Digital Preservation Europe, 2007*).

2.4 Casos de referência em certificação

Na literatura encontram-se vários casos de repositórios que passaram por um processo de auditoria com o objetivo de serem certificados, nomeadamente o Pórtico, o *Hathitrust*, o *Chronopolis* e o *Clockss*.

O processo de auditoria ao Pórtico¹⁴ foi realizado entre abril e outubro de 2009, usando a *checklist* do TRAC. Trata-se de uma Organização sem fins lucrativos que fornece um serviço de preservação de informação digital, através de um arquivo permanente de informação maioritariamente científica e técnica (livros, revistas eletrónicas e outros tipos de conteúdo académico).

O objetivo da auditoria foi o de obter a confirmação de que o Pórtico oferece um adequado nível de segurança, afirmando-se a probabilidade de continuar a fornecer serviços adequados, sem falhas ou defeitos materiais como descrito na divulgação pública do Pórtico.

No relatório constata-se que a metodologia adotada pretendeu evidenciar a aceitação das boas práticas na gestão de sistemas digitais; os critérios a seguir; e o modelo de referência OAIS (*Open Archival Information System*).

O Pórtico é uma das referências do presente projeto dado que se constituiu como repositório digital confiável em 2010, através da auditoria levada a cabo pelo *Center for Research Libraries*.

¹⁴ CENTER OF RESEARCH LIBRARIES (2010). Global Resources Network. Portico Audit Report 2010. Consultado em Mar 03, 2015 em <http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories/portico>

Entre Novembro e Dezembro de 2010, o mesmo *Center of Research Libraries* (CRL)¹⁵ realizou uma auditoria de preservação ao repositório *HathiTrust* com o objetivo de o tornar num repositório digital confiável.

Esta certificação foi baseada na avaliação de uma extensa documentação recolhida pelo CRL; dos dados e documentos fornecidos pelo *HathiTrust*¹⁶ entre novembro de 2009 e dezembro de 2010; e uma visita ao local, realizada em maio de 2010. A análise da CRL foi orientada pelos critérios incluídos na *checklist* do TRAC e outras métricas desenvolvidas pela CRL através das suas diversas atividades de avaliação de repositórios digitais.

O objetivo da auditoria foi o de obter um nível de segurança razoável oferecida pelo *HathiTrust*, ficando como provável a continuidade do fornecimento de serviços adequados às necessidades apresentadas, sem falhas ou defeitos de materiais.

Segue-se, entre Novembro de 2010 e Dezembro de 2011, a auditoria de preservação ao *Chronopolis*¹⁷ pelo *Center for Research Libraries* (CRL) com o objetivo de o tornar um repositório digital de confiança. Esta auditoria também foi levada a cabo usando a *checklist* do TRAC. O CRL concluiu que as práticas e serviços descritos nas comunicações públicas do *Chronopolis* e a documentação publicada eram adequadas ao conteúdo que estava a ser arquivado e às necessidades gerais da designada comunidade *Chronopolis*. Além disso, o Painel do CRL espera que, no futuro, o *Chronopolis* continue a ser capaz de oferecer o conteúdo que é administrável e utilizável por essa comunidade.

Mais recentemente a auditoria ao *CLOCKSS*¹⁸ (repositório de conteúdo de *e-journal*) foi feita entre Setembro de 2013 e Maio de 2014, também pelo CRL e usando a mesma *checklist* do TRAC. As conclusões retiradas desta auditoria confirmam que as práticas e os serviços descritos em comunicações públicas do *CLOCKSS* e a documentação publicada correspondem na generalidade às operações do mesmo e são apropriados para o conteúdo de um *e-journal* e às necessidades expressas da designada comunidade *CLOCKSS*. Além disso, o painel espera que, no futuro, *CLOCKSS* seja capaz de garantir a entrega dos conteúdos que preserva a terceiros que estão preparados para torná-lo disponível para o uso da comunidade. Esta

¹⁵ O CRL foi fundado em 1949 caracteriza-se por ser um consórcio que apoia a investigação avançada e o ensino nas humanidades ciências e ciências sociais, através da preservação e disponibilização aos investigadores o material de fonte primária para quem pretenda estudar essas disciplinas.

¹⁶ CENTER OF RESEARCH LIBRARIES (2011). Global Resources Network. HathiTrust Audit Report 2011. Consultado em Mar 03, 2015 em <http://www.crl.edu/reports/hathitrust-audit-report-2011>

¹⁷ CENTER OF RESEARCH LIBRARIES (2012). Global Resources Network. Chronopolis Audit Report 2012. Consultado em Mar 03, 2015 em <http://www.crl.edu/reports/chronopolis-audit-report-2012>

¹⁸ CENTER FOR RESEARCH LIBRARIES (2014). Global Resources Network. *Certification report on CLOCKSS*. Consultado em Mar 20, 2015 em http://www.crl.edu/sites/default/files/reports/CLOCKSS_Report_2014.pdf

certificação aplica-se à capacidade do repositório para preservar e gerir conteúdos digitais depositados pelos participantes, neste caso editores de publicações eletrónicas, a partir de maio de 2014.

A avaliação da CRL ao *CLOCKSS* e as informações fornecidas no relatório de auditoria refletem as políticas, sistemas e procedimentos que estavam em vigor no *CLOCKSS* para gerir conteúdo de *e-journal* a partir de 1 de junho de 2014.

3. O caso em estudo: MULTICERT S.A

3.1 A Certificação Digital

Certificação Digital é o nome genérico de um conjunto de tecnologias que viabilizam diversas formas de proteção para transações eletrónicas realizadas através de redes abertas tais como a Internet. Este tipo de tecnologia tem como principais aplicações a proteção contra alterações não autorizadas em documentos eletrónicos, para que sejam tão amplamente aceites como meio de prova de atos jurídicos como são os documentos em papel; e a substituição da identificação via “nome e senha” comuns em *sites* de serviços, tais como bancos via Internet, lojas virtuais, etc. - hoje fortemente alvo de emails fraudulentos que exploram uma eventual ingenuidade do utilizador final. (Resende, D 2009)

A certificação digital é um tipo de tecnologia de identificação que permite que transações eletrónicas dos mais diversos tipos sejam realizadas considerando a sua integridade, autenticidade e confidencialidade de maneira a evitar que ocorram adulterações, captura de informações privadas ou outros tipos de ações indevidas.

A certificação digital tem como um dos seus pilares a garantia da confidencialidade na troca de mensagens pretendendo garantir que apenas o destinatário dos dados transmitidos pelo emissor terá acesso a esses dados, não havendo a possibilidade de um intruso se intrometer na comunicação e conseguir aceder aos dados transmitidos. (Correia, M. 2003)

Baseia-se no conceito de hierarquia de confiança com recurso a algoritmos criptográficos, mais conhecido por Infraestrutura de Chaves Públicas (PKI) e permite a autenticação/identificação; integridade; não-repúdio; autenticação/origem.

- Autenticação/identificação: permite a autenticação e identificação única da pessoa, obrigando cada uma das partes envolvidas na comunicação a utilizar um *token* digital que promove a sua identidade.
- Integridade: pode garantir a integridade da mensagem, ou seja, se a mensagem for alterada por uma terceira entidade isso é detetável, pois a assinatura é corrompida.
- Não-repúdio: pode garantir o não-repúdio se uma mensagem chegar ao destinatário assinada digitalmente pelo emissor. Este não pode negar que a enviou e que o conteúdo que transmitiu foi o que de facto chegou ao destinatário. Desta forma, se a mensagem chegar ao destinatário com a

assinatura corrompida ou sem assinatura, o remetente pode repudiá-la, pois não há provas que foi efetivamente ele quem produziu e enviou os dados em questão.

- Autenticação/origem: pode garantir a veracidade da origem da mensagem. (MULTICERT, 2014c)

A certificação digital funciona com base num documento eletrónico chamado certificado digital e em um recurso denominado assinatura digital.

Um certificado digital é uma credencial que valida a identidade do detentor do certificado, mais ou menos como um passaporte faz. Liga um indivíduo a uma identidade que pode ser reconhecida e verificada por vias eletrónicas por outras entidades. Este fornece os meios para assinar *emails*, documentos, transações ou para verificar assinaturas de outros. Permite ainda fazer *emails*, documentos ou transações que são apenas legíveis pelos destinatários que forem designados. (MULTICERT, 2014c)

É um documento eletrónico acessível em ambiente informático a qualquer interessado na sua consulta, que cria a certeza de que a pessoa que apõe a assinatura é a titular da respetiva chave pública e também da respetiva chave privada. Trata-se pois de um documento dotado de um especial valor probatório, cuja emissão, conteúdo e condições de validade, revogação e suspensão são detalhadamente especificados pelos artigos 28º a 31º da versão atual do DL nº 290-D/99 (Correia, M. 2003).

Um certificado digital pode ser utilizado para autenticar o seu detentor; assinar e cifrar um conjunto de dados. São ficheiros eletrónicos que são usados para identificar pessoas e recursos através das redes como a internet. Promovem a segurança e a comunicação confidencial entre duas partes usando a criptografia. São baseados em chaves públicas criptográficas que usam um par de chaves para a encriptação e desencriptação. Com a criptografia de chaves públicas as chaves funcionam em pares (pública e privada) (MULTICERT, 2014c)

Os certificados qualificados devem conter uma indicação de que o certificado é emitido como um certificado qualificado; o identificador do prestador de certificação e do Estado em que está estabelecido; o nome do signatário ou um pseudónimo, que deve ser identificado como tal; provisão para um contributo específico do signatário, se relevante, dependendo da finalidade para o qual o certificado se destina; os dados de verificação de assinaturas, que correspondem aos dados de criação de assinaturas, sob o controlo do signatário; a indicação do início e do final do período de validade do certificado; o código de identificação do certificado; a assinatura eletrónica

avançada do provedor de serviços de certificação que o emite; as restrições ao âmbito de utilização do certificado, se aplicável; as restrições ao valor das transações nas quais o certificado pode ser utilizado, se for o caso. (DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2000)

Pode-se enumerar muitas vantagens para o uso de certificados digitais. Uma delas é dar agilidade aos processos burocráticos, reduzir custos, promover uma maior segurança nas transações pela internet. Para além da economia de tempo e dinheiro, o impacto ambiental é preservado, devido à imensa economia de papel. (Resende D, 2009).

A assinatura digital consiste no uso da função de *hash* junto ao documento a ser transmitido e na aplicação do esquema de chaves. No processo de conferência, deve-se calcular o *hash* e efetuar a decifragem com a chave pública do emissor, sendo de frisar que qualquer alteração na informação fará com que o resumo seja diferente, indicando a ocorrência de modificações (Alecrim, E. 2011).

A assinatura eletrónica avançada é o resultado de um processamento eletrónico de dados suscetíveis de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico ao qual seja aposta, de modo que:

- i. Identifique de forma unívoca o titular como autor do documento;
- ii. A sua aposição ao documento dependa apenas da vontade do titular;
- iii. É criada com meios que o titular pode manter sob seu controlo exclusivo;
- iv. A sua conexão com o documento permita detetar toda e qualquer alteração superveniente do conteúdo deste. (Correia, M. 2003)

Por sua vez, a assinatura digital apresenta-se como um mecanismo eletrónico que usa a criptografia¹⁹, mais precisamente chaves criptográficas²⁰ que se apresentam como um conjunto de bits²¹ que se baseiam num determinado algoritmo capaz de cifrar e decifrar as informações. Estas chaves apresentam-se como chaves simétricas e chaves assimétricas.

¹⁹ A criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

²⁰ Uma chave é um pedaço de informação que controla a operação de um algoritmo de criptografia. Na codificação, uma chave especifica a transformação do texto puro em texto cifrado, ou vice-versa, durante a decodificação. Chaves são também usadas em outros algoritmos criptográficos, tais como esquemas de assinatura digital e funções hash (também conhecidas como MAC), algumas vezes para autenticação.

²¹ Do inglês "binary digit" é a menor unidade de informação que pode ser armazenada ou transmitida, usada na Computação e na Teoria da Informação.

As chaves simétricas são mais simples, pois com elas o emissor e o recetor utilizam a mesma chave para, respetivamente, cifrar e decifrar uma informação.

O esquema assimétrico, por sua vez, trabalha com duas chaves: a chave privada e a chave pública. A chave privada é o elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública. A chave pública é o elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves. (DL 290-D/99, art 2º)

Neste modo, uma pessoa ou uma Organização deve utilizar uma chave e disponibilizá-la a quem for enviar informações a ela. Esta é a chave pública. Uma outra chave deve ser usada pelo recetor da informação. Essa é a chave privada, que é sigilosa e individual. Ambas as chaves são geradas de forma conjunta, portanto, uma está associada à outra. (Alecrim, E. 2011)

Este método considera dois importantes aspetos: confidencialidade e autenticidade. A confidencialidade permite fazer com que a informação esteja acessível somente a pessoas ou organizações que estão devidamente autorizadas. A autenticidade fornece a certeza de que a informação provém da origem e forma esperadas, de forma que o recetor perceba isso. (Alecrim, E. 2011) Permite associar o documento ao seu autor, afastando qualquer dúvida quanto à sua autoria.

No que se refere à confidencialidade, é necessário que o emissor tenha a chave pública do destinatário. Por meio de algoritmos apropriados, o documento é então cifrado de acordo com esta chave pública. A partir daí, o recetor usará a sua correspondente chave privada para a decifragem e consequente obtenção da informação. (Alecrim, E. 2011)

Assinatura digital ou criptográfica comporta duas modalidades, consoante os sistemas em que se baseia:

- a) Criptografia simétrica com chave única: funciona a partir de uma mesma chave possuída pelo emitente e pelo recetor da mensagem e que serve simultaneamente para codificá-la e decodificá-la. Apresenta como inconvenientes a necessidade da multiplicação das chaves consoante os vários interlocutores de uma mesma pessoa ou empresa; a maior facilidade de a chave cair em poder de um terceiro e a possibilidade de uma das partes

atribuir falsamente declarações à outra, uma vez que a chave é a mesma para ambas.

b) Criptografia assimétrica com chave pública: utiliza uma “chave pública” e uma “ chave privada” a primeira das quais descodifica as mensagens encriptadas com a segunda. Qualquer uma das chaves serve para cifrar ou decifrar uma mensagem, porem o que uma das chaves cifrou somente a outra decifrá. (Almeida V, 2004)

O objetivo da assinatura digital não é o de tornar a mensagem ilegível, pois a mensagem a si mesma não é cifrada. A assinatura digital é apenas adicionada à mensagem eletrónica, mantendo esta intacta e perfeitamente legível.

A assinatura digital é portanto:

- i) Autêntica, pois prova ao destinatário que o subscritor assinou o documento e este é uma manifestação da sua vontade;
- ii) Não pode ser falsificada, pois prova o facto de o documento ter sido assinado pelo subscritor e não por outra pessoa;
- iii) Não pode ser usada de novo. Constitui-se como parte do documento e não pode ser transferida para outro documento;
- iv) Impede que o documento seja modificado depois de assinado;
- v) Não pode ser contestada, por ser uma prova de que o signatário marcou o documento.

A verificação positiva de uma assinatura digital (assimétrica) conduz, portanto, a um elevado grau de autenticidade da autoria e da integridade do documento ao qual ela seja aposta, portanto comprova seguramente que a assinatura foi aposta pelo seu titular e que o documento não foi alterado desde o seu envio ao destinatário. (Correia, M. 2003)

As três funções e respetivos efeitos práticos e jurídicos da assinatura eletrónica são:

- *Função identificadora*, pela qual a assinatura atribui inequivocamente a declaração ao signatário, estabelecendo a autoria deste, ou em seu nome próprio, ou como representante de uma pessoa coletiva;
- *Função finalizadora ou confirmadora*, que não só exprime a conclusão espacial do documento escrito, mas também o assentimento do signatário quanto às declarações de vontade e/ou de conhecimento nele constantes, assumindo-as como sendo próprias dele e estando correta e completamente expressas no texto precedente;

- *Função de inalterabilidade*, já que a verificação positiva de uma assinatura digital pelo destinatário comprova que o documento ao qual ela foi aposta não foi alterado depois da aposição da assinatura, até à sua receção pelo destinatário. (DL n 290-D/99 nº1 do art 7º)

Usar um certificado digital é a certeza da negociação segura, da confiança na mensagem que envia ou recebe.

3.1.1 Contexto legal e regulamentar

No que toca a entidades de certificação digital existem normas e regulamentação e legislação, que atuam como um conjunto de boas praticas que as entidades devem seguir no decorrer da sua atividade.

- a) Despacho nº 27008/2004, de 14 de Dezembro, publicado no D.R II, nº 302, de 28 de Dezembro;
- b) Portaria nº 1350/2004, de 23 de Outubro;
- c) Despacho nº 16445/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- d) Aviso nº 8134/2004, de 29 de Julho, publicado no D.R II, nº 190 de 13 de Agosto;
- e) Decreto Regulamentar nº. 25/2004, de 15 de Julho;
- f) Decreto-Lei nº 290-D/99, de 2 de Agosto republicado pelo Decreto-Lei nº88/2009, de 9 de Abril;
- g) Decreto-lei nº 62/2003, de 3 de Abril
- h) Portaria nº 1370/2000, publicada no D.R. Nº 211, II série de 12 de Setembro;
- i) GNS/NT-D 02 - Requisitos mínimos de Segurança Física de Instalações de Entidades Certificadoras;
- j) GNS / NT-D 03 - Requisitos para Entidades Certificadoras que emitem Certificados Qualificados (MULTICERT, 2014b)

3.1.2 Provedores, produtos e serviços

Um provedor de serviço de certificação digital fornece soluções completas de segurança e/ou certificação digital para todo o tipo de transações eletrónicas que exigem segurança. Uma entidade certificadora é uma entidade ou pessoa singular ou coletiva que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respetiva publicidade e presta outros serviços relativos a assinaturas eletrónicas. (Alecrim, E. 2011)

Uma entidade certificadora é uma entidade ou pessoa coletiva ou singular que cria ou fornece meios para a criação e verificação das assinaturas, emite os certificados, assegura a respetiva publicidade e presta outros serviços relativos a assinaturas eletrónicas. (DL 62-2003) Entidade ou pessoa singular ou coletiva credenciada que cria ou fornece meios para a criação das chaves, emite os certificados de assinatura, assegura a respetiva publicidade e presta outros serviços relativos a assinaturas digitais. (DL 290-d/99)

Uma entidade certificadora tem a função de associar uma identidade a uma chave e “inserir” esses dados num certificado digital. (Alecrim, E. 2011)

Organismo de certificação é uma entidade pública ou privada competente para a avaliação e certificação da conformidade dos processos, sistemas e produtos de assinatura eletrónica com os requisitos a que se refere a alínea c) do nº1 do artigo 12º do DL 62/2003

É concedida a credenciação a entidades certificadores de assinaturas eletrónicas qualificadas, mediante pedido apresentado à autoridade credenciadora, que satisfaçam os seguintes requisitos:

- Estejam dotadas de capital e meios financeiros;
- Deem garantias de absoluta integridade e independência no exercício da atividade de certificação e assinaturas eletrónicas qualificadas;
- Disponham de recursos técnicos e humanos que satisfaçam os padrões de segurança e de eficácia que sejam previstos na regulamentação a que se refere o artigo 39º;
- Mantenham contrato de seguro valido para cobertura adequada da responsabilidade civil emergente da atividade de certificação. Art. 12º

Compete à entidade certificadora que emite certificados qualificados:

- a) Estar dotada dos requisitos patrimoniais estabelecidos no artigo 14º;
- b) Oferecer garantias de absoluta integridade e independência no exercício da atividade de certificação;
- c) Demonstrar a fiabilidade necessária para o exercício da atividade de certificação;
- d) Manter um contrato de seguro valido para a cobertura adequada da responsabilidade civil emergente da atividade de certificação;
- e) Dispor de recursos técnicos e humanos que satisfaçam os padrões de segurança e eficácia, nos termos do diploma regulamentar;

- f) Utilizar sistemas e produtos fiáveis protegidos contra qualquer modificação e que garantam a segurança técnica dos processos para os quais estejam previstos;
- g) Adotar medidas adequadas para impedir a falsificação ou alteração dos dados constantes dos certificados e, nos casos em que a entidade certificadora gere dados de criação de assinaturas, garantir a sua confidencialidade durante o processo de criação;
- h) Utilizar sistemas fiáveis de conservação dos certificados de forma que estes possam ser consultados pelo público, que apenas pessoas autorizadas possam inserir dados e fazer alterações, a autenticidade da informação possa ser verificada e que quaisquer alterações de carácter técnico suscetíveis de afetar os requisitos de segurança sejam imediatamente detetáveis;
- i) Verificar rigorosamente a identidade dos requerentes titulares dos certificados;
- j) Conservar os elementos que comprovem a verdadeira identidade dos requerentes titulares de certificados com pseudónimo;
- k) Informar os requerentes sobre o processo de emissão de certificados qualificados e os termos e condições exatos de utilização do certificado qualificado, incluindo eventuais restrições à sua utilização;
- l) Cumprir as regras de segurança para tratamento de dados pessoais estabelecidos na legislação respetiva;
- m) Não armazenar ou copiar dados de criação de assinaturas do titular a quem a entidade certificadora tenha oferecido serviços de gestão de chaves;
- n) Assegurar o funcionamento de um serviço que permita a consulta do registo informático dos certificados emitidos, revogados suspensos ou caducados e garanta de revogação, suspensão ou caducidade dos certificados;
- o) Proceder à publicação imediata da revogação ou suspensão dos certificados;
- p) Assegurar que a data e a hora da emissão, suspensão e revogação dos certificados possam ser determinadas através de validação cronológica;
- q) Conservar os certificados que emitir por um período não inferior a 20 anos. (DL 62-2003 artigo 24º)

No que toca à emissão das chaves e dos certificados:

A entidade certificadora, a pedido de uma pessoa singular ou coletiva interessada, cuja identidade e poderes de representação, quando existam, verificará por meio legalmente idóneo e seguro, emitirá a favor daquela um par de chaves, privada e pública, ou porá à disposição dessa pessoa, se esta o solicitar, os meios técnicos necessários para que ela crie o par de chaves. (DL 290-D/99, DL 62-2003)

A entidade certificadora emitirá, a pedido do titular do par de chaves, uma ou mais vias do certificado de assinatura e do certificado complementar.

A entidade certificadora deve tomar medidas adequadas para impedir a falsificação ou alteração dos dados constantes dos certificados e assegurar o cumprimento das normas legais e regulamentares aplicáveis recorrendo a pessoal devidamente habilitado. (DL 290-D/99, DL 62-2003)

A entidade certificadora fornecerá aos titulares dos certificados as informações necessárias para a utilização correta e segura das assinaturas digitais, nomeadamente as respeitantes às obrigações do titular do certificado e da entidade certificadora; ao procedimento de aposição e verificação de uma assinatura digital; e à conveniência de os documentos aos quais foi aposta uma assinatura digital serem novamente assinados quando ocorrerem circunstâncias técnicas que o justifiquem.

A entidade certificadora organizará e manterá permanentemente atualizado um registo informático dos certificados emitidos, suspensos ou revogados, o qual estará acessível a qualquer pessoa para consulta, inclusivamente por meio de telecomunicações, e será protegido contra alterações não autorizadas. (DL 290-D/99, DL 62-2003)

As entidadesificadoras têm o dever de fornecer à autoridade credenciadora, de modo pronto e exaustivo, todas as informações que ela lhes solicite para fins de fiscalização da sua atividade e facultar-lhe-ão para os mesmos fins a inspeção dos seus estabelecimentos e o exame local de documentos, objetos, equipamentos de *hardware* e software e procedimentos operacionais, no decorrer dos quais a autoridade credenciadora poderá fazer as cópias e registos que sejam necessários. Estas deverão comunicar sempre todas as alterações relevantes que sobrevenham nos requisitos. Até ao último dia útil de cada semestre, as entidadesificadoras enviarão à autoridade credenciadora uma versão atualizada das relações de todos os sócios com especificação das respetivas participações, bem como dos membros dos órgãos de administração e de fiscalização, e, tratando-se de

sociedade anónima, relação de todos os acionistas com participações significativas diretas ou indiretas. (DL 290-D/99)

De maneira a aumentar a confidencialidade nas comunicações e correio eletrónico, os provedores de serviços de certificação devem observar a legislação de proteção de dados e a privacidade individual.

DigitalSign²²

Apresenta-se como uma empresa de segurança eletrónica destacando-se como uma Entidade Certificadora Portuguesa para a emissão de certificados digitais qualificados, em conjunto com a British Telecommunication, estando ambas registadas no Gabinete Nacional de Segurança como entidades acreditadas. Tem também como parceiro a VeriSign, a nível dos certificados de servidor e de segurança eletrónica, sendo líder internacional na operação de infraestruturas e serviços de comunicação inteligentes, o que permite à DigitalSign oferecer o “state of art” de inúmeros produtos e serviços já prestados a diversas companhias multinacionais. Procura ainda complementar a oferta de produtos e serviços dos dois parceiros com outros serviços e produtos que foram desenvolvidos internamente e feitas novas parcerias internacionais com a SafeNet e a Ascertia para que possam oferecer aos clientes soluções cada vez mais completas e abrangentes. Como missão, pretende facilitar a segurança e confiança aos clientes para que possam otimizar os benefícios da revolução que esta em curso nas áreas do comércio eletrónico e de comunicações.

Planeia e desenvolve processos personalizados para a segurança de redes identificando, certificando e possibilitando a cifragem da comunicação entre ambas as partes. Comercializa produtos diferenciados para os utilizadores de redes de comunicação, como servidores web, lojas virtuais e Bancos, Seguradoras, Telecomunicações, Administração pública, e todos aqueles que necessitem de segurança aquando das suas comunicações de dados.

ECEE - Entidade de Certificação Eletrónica do Estado

A Entidade de Certificação Eletrónica do Estado²³ é a entidade certificadora de topo da cadeia de certificação do SCEE (sistema de certificação eletrónica do estado), executora das políticas de certificados e diretrizes aprovadas pela Entidade Gestora de Políticas de Certificação. Compete a esta prestar os serviços de

²² DIGITALSIGN (2015). Certificadora Digital. Institucional. Consultado em Abr 23, 2015 em <https://www.digitalsign.pt/>

certificação às Entidades Certificadoras do Estado no nível hierárquico imediatamente inferior ao seu na cadeia de certificação em conformidade com as normas aplicáveis às entidades certificadoras estabelecidas em Portugal na emissão de certificados digitais qualificados. Compete à entidade de certificação do estado admitir a integração das entidades certificadoras que obedeçam aos requisitos estabelecidos no decreto-lei 88/2009 bem como prestar os serviços de certificação às entidades certificadoras, no nível hierárquico imediatamente inferior ao seu na cadeia de certificação, em conformidade com as normas estabelecidas em Portugal na emissão de certificados digitais qualificados. (DL 88/2009 Art 5º)

A Entidade de Certificação Eletrónica do Estado disponibiliza exclusivamente os seguintes serviços de certificação digital:

- a) Processo de registo das entidades certificadoras;
- b) Geração de certificados, incluindo certificados qualificados, e gestão do seu ciclo de vida;
- c) Disseminação dos certificados, das políticas e das práticas de certificação;
- d) Gestão de revogações de certificados;
- e) Disponibilização do estado e da situação das revogações referidas na alínea anterior.

A Entidade de Certificação Eletrónica do Estado emite exclusivamente certificados para as entidades certificadoras do Estado subordinadas, não podendo emitir certificados destinados ao público.

Compete ainda à Entidade de Certificação Eletrónica do Estado: ART.5º

- a) Garantir o cumprimento e a implementação enquanto entidade certificadora de todas as regras de todos os procedimentos estabelecidos no documento de políticas de certificação do SCEE;
- b) Implementar as políticas e práticas do conselho gestor do SCEE;
- c) Gerir toda a infraestrutura e os recursos que compõem e garantem o funcionamento da entidade certificadora raiz do Estado, nomeadamente o pessoal, os equipamentos e as instalações,
- d) Gerir todas as atividades relacionadas com a gestão do ciclo de vida dos certificados por si emitidos para as entidades certificadoras de nível imediatamente inferior ao seu;

²³ CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO (2006). Certificação Eletrónica. Sistema de Certificação Electrónica do Estado e Segurança Electrónica. Consultado em Abr 23, 2015 em <http://www.ceger.gov.pt/certificacao-eletronica.aspx>

- e) Garantir que o acesso às suas instalações principal e alternativa é efetuado apenas por pessoal devidamente autorizado e credenciado;
- f) Gerir o recrutamento de pessoal tecnicamente habilitado para a realização das tarefas de gestão e operação da entidade certificadora de raiz do estado;
- g) Comunicar imediatamente qualquer incidente, nomeadamente anomalias ou falhas de segurança, ao conselho gestor do SCEE (DL 88/2009)

3.2 A MULTICERT S.A.

A Multicert, Serviços de Certificação Eletrónica, S.A. iniciou a sua atividade em 2002, posicionando-se no mercado como fornecedor de soluções completas de segurança e/ou certificação digital para todo o tipo de transações eletrónicas que exigem segurança (*e-commerce, e-banking, e-government, email, etc.*). Atualmente, a Multicert desenvolve a sua atividade nas seguintes áreas: Identidade; Desmaterialização; Serviços Profissionais e Investigação/Desenvolvimento. Na área da Identidade destacam-se os documentos de identificação como o Cartão de Cidadão Português e o Cartão Nacional de Identificação de Cabo Verde, bem como o Passaporte Eletrónico Português e Cabo-Verdiano. Ainda a personalização de Cartões e Cédulas profissionais que permitem aos seus associados a possibilidade de autenticação e assinatura digital na sua qualidade profissional.

Na área da desmaterialização, o objetivo é garantir a produtividade da Organização promovendo processos mais rápidos, ágeis e com menos custos associados. Aqui destaca-se a desmaterialização dos documentos; a faturação eletrónica; o *Web Security Broker*; os mandatos eletrónicos e o *Mobile signature*.

Na área dos Serviços Profissionais destacam-se a Plataforma de Emissão de Certificados, que torna o processo de emissão de certificados mais fácil e ágil; os Testes de Intrusão para avaliar a segurança de um sistema simulando um ataque de um *hacker* malicioso; Auditorias de Segurança às instalações físicas permitindo assim garantir que as regras e políticas de segurança da Organização estão a ser cumpridas. Nesta área encontram-se ainda as TSL's (*Trust-Service Status List*). A Multicert também aposta na área da Investigação e Desenvolvimento pois o mundo está em constante evolução e o que está hoje em voga não é o que estará amanhã, por isso é necessário corresponder aos novos requisitos de mercados apostando por isso nos melhores especialistas investindo nesta área.

A Multicert desenvolve a sua atividade em diversos sectores, Financeiro (como bancos, instituições de investimento ou crédito e seguradoras), Governos e entidades estatais (Governo Electrónico), Telecomunicações, Educação, Associações e Ordens Profissionais e Empresas.

Participou no projeto do Cartão de Cidadão e do Passaporte Eletrónico em Portugal, ocupando assim um prestigiado lugar entre as poucas empresas do mundo com *know-how* para desenvolver soluções tanto para a identificação eletrónica de cidadãos, como para outros sistemas de segurança digital.

A Multicert constitui-se como a primeira entidade privada portuguesa de certificação credenciada pelo Gabinete Nacional de Segurança para a emissão dos certificados qualificados (MULTICERT, 2010a).

A sua missão, como empresa de soluções tecnológicas e serviços de Certificação Eletrónica, é participar ativamente no desenvolvimento da Sociedade de Informação e da Economia Digital.

Tem como visão ser uma empresa líder no negócio de certificação eletrónica e a principal referência para todos os setores da sociedade, no domínio das relações e transações eletrónicas seguras.

A Multicert tem como principais objetivos:

- Desenvolvimento de soluções completas de segurança e certificação digital;
- Apostar nos sectores de atividade que exigem segurança nas suas transações eletrónicas;
- Manter a vanguarda na área de atividade;
- Parcerias com Universidades e Laboratórios de Investigação, com o objetivo de “investigar para inovar”;
- Ser a Autoridade de Certificação Eletrónica de referência que dinamize o desenvolvimento da Economia Digital no País;
- Cumprir rigorosamente o quadro legal do negócio de certificação eletrónica;
- Fornecer uma infraestrutura de confiança destinada a todo o tipo de utilizadores finais, em transações nacionais a internacionais;
- Constituir uma plataforma de suporte a negócios eletrónicos seguros entre empresas, instituições bancárias, administração e consumidores, baseada em serviços especializados próprios e a funcionarem sobre arquiteturas de confiança de chaves públicas (MULTICERT, 2010a).

A Multicert apresenta-se como uma empresa que visa:

1. Proporcionar uma estrutura de confiança eletrónica que proporcione a realização de transações eletrónicas seguras, autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio para os seus clientes diretos
2. Promover a melhoria contínua dos seus processos, produtos e serviços associados aos Certificados Digitais Qualificados para clientes diretos de forma a superar as expectativas dos clientes e inovar nos serviços

fornecidos.

3. Proteger os melhores interesses, segurança e bem-estar dos clientes diretos, assegurando o correto tratamento dos seus dados, garantindo a completa confidencialidade dos mesmos. (MULTICERT, 2014a)

A Equipa Multicert garante, no seu serviço de emissão de certificados digitais qualificados para clientes diretos, o cumprimento dos seguintes princípios:

- Exigência;
- Qualidade;
- Confidencialidade;
- Rapidez;
- Assertividade;
- Integridade;
- Disponibilidade. (MULTICERT, 2014a)

3.2.1 Produtos e serviços

Sendo um fornecedor de produtos e serviços, a Multicert oferece um conjunto de produtos que promovem a segurança no meio digital tais como:

- **Certificados qualificados** com o mais alto nível de segurança e confiança;
- **Certificados SSL** que se apresenta como um certificado digital que garante a autenticidade de um sítio web, a titularidade de um domínio ou a confidencialidade da informação que é transacionada.
- **Certificado de fatura eletrónica** que se destina às empresas que possuem uma plataforma de fatura eletrónica, e que por isso necessitem de certificado digital para a assinatura eletrónica da fatura eletrónica.
- **Certificado para aplicação** que certifica as aplicações que cria um certificado para assinatura de documentos para a identificação de VPNs ou para outro tipo de serviços como B2B ou C2B.
- **Certificado CodeSigning** para certificar o código e aplicações informáticas, ficheiros de instalação ou outro tipo de conteúdos.
- **Certificado avançado** é emitido para particulares e profissionais e permite a assinatura eletrónica de documentos e a identificação eletrónica segura e clara de uma pessoa.
- **Selos & Aposições** a emissão de *selos & aposições* que estão em conformidade com a legislação Portuguesa e Europeia e com um período de validade de 6

anos e 4 meses. Estes têm características interoperáveis sendo por isso aceites em todas as plataformas eletrónicas de contratos públicos como a da Ano, Miroma, Saphety, Gatewit, Vortal, Acin e Mercado eletrónico. Um selo temporal gere evidências do momento temporal em que um documento eletrónico foi assinado. Os selos temporais garantem a segurança, transparência e fiabilidade na contratação pública eletrónica, garantindo por isso que se determine com rigor absoluto em que momento a documentação e as propostas são submetidas, tal como o momento em que as ações foram realizadas na plataforma eletrónica. O serviço de aposição é um mecanismo que garante o pedido de selo e respetiva utilização nas plataformas eletrónicas sempre que é solicitado.

- **Aposições Gatewit** é um mecanismo que garante o pedido do selo e respetiva utilização nas plataformas eletrónicas sempre que é solicitado. Estes são na totalidade geridos pelas plataformas eletrónicas de contratação pública. Estas oposições apenas funcionam na plataforma de compras públicas da Gatewit.
- **Voto eletrónico** permite garantir a confiança e fiabilidade nas votações, permitindo também a coexistência com o voto presencial em papel e por correspondência. Este voto eletrónico permite a autenticação do eleitor; privacidade dos eleitores; confidencialidade dos votos; evita extravio dos votos; permite o controlo e autenticação dos utilizadores do sistema de votação e ainda a integridade e auditabilidade do sistema de voto. O voto eletrónico da Multicert já foi utilizado em diversas eleições em instituições bancárias, ordens e associações profissionais, assembleias gerais de acionistas e ainda em experiências piloto de eleições do parlamento europeu e legislativas.
- **E4DOC** - solução de fatura eletrónica que se insere num conjunto de soluções que permitem uma maior consistência ambiental, permitindo às empresas reduzir a utilização do papel na empresa. É uma solução simples e rentável que permite às empresas encarar com seriedade o impacto ambiental das suas ações. Desde as vantagens obtidas através da desmaterialização das faturas, à agilização da utilização do comércio eletrónico, a Fatura eletrónica apresenta-se como uma opção de valor para o negócio de qualquer empresa.

A Multicert especialista em PKI²⁴ oferece um conjunto de serviços profissionais aos seus clientes que garantem os mais altos níveis de segurança e confiança em todas as soluções que oferecem:

- **Plataforma de emissão de certificados:** foi criada uma plataforma para a emissão de Certificados Digitais de forma mais fácil e ágil, sem a necessidade de se recorrer a processos complexos.
- **Testes de intrusão:** são um método para avaliar a segurança de um sistema simulando ataques de um *hacker* malicioso para verificar a dificuldade que um intruso tem em aceder indevidamente aos sistemas de informação de uma Organização. Estes são testes controlados pelos operadores de segurança da Multicert.
- **Auditorias de segurança:** auditorias feitas às instalações físicas que permitem garantir que as regras e políticas de segurança da Organização estão a ser corretamente aplicadas e que a informação e os recursos estão devidamente protegidos.
- **Trust-service status list:** A Multicert é o fornecedor exclusivo da TSL do *European Payments Council* que contem a lista de autenticação de *Routing Service* e *Validation Service* para o serviço europeu de e-Mandates. A TSL está incluída na oferta de serviços de confiança da Multicert, sendo operados de acordo com as melhores práticas de segurança e em conformidade com *standards* reconhecidos, de maneira a oferecer a máxima confiança nos processos e controlos implementados.
- **Entidades certificadoras de raiz:** fornece a infraestrutura e serviços “chave na mão” no âmbito da certificação digital, na criação de Entidades de Certificação Raiz, para a emissão de Cartões de Cidadão, Títulos de Residência e Passaportes Eletrónicos.

Entre os projetos desenvolvidos pela empresa destacam-se:

- **Cartão do cidadão:** Permite assinar digitalmente o documento garantindo assim a autenticidade, integridade e não-repúdio.

²⁴ Public Key Infrastructure (Infraestrutura de chaves públicas) é um órgão ou iniciativa pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais. A principal função do ICP é definir um conjunto de técnicas, práticas e procedimentos a serem adotados pelas entidades a fim de estabelecer um sistema de certificação digital baseado em chave pública

- **SAM-VV** - Sistema do cartão de cidadão e processo de alteração de morada. O sistema SAM disponibiliza dois serviços distintos: o registo de um novo pedido de alteração de morada e a escrita dos dados no chip do Cartão do Cidadão.
- **eID-CV** - O projeto eID enquadra-se no objetivo do Governo de Cabo Verde de dotar os seus cidadãos e estrangeiros residentes de documentos de identificação eletrónica, nomeadamente:
 - Cartão Nacional de Identificação (CNI)
 - Título de Residência (TR)
 - Passaporte Eletrónico

A MULTICERT preparou toda a Infraestrutura de Chaves Públicas (PKI) de acordo com as melhores práticas de segurança. Entre outros, implica a seleção, instalação e configuração do *hardware* e *software* e a definição dos processos e respetivos procedimentos que os suportam. A PKI inclui serviços de Entidade Certificadora, OCSP e Validação Cronológica

- **MDDE** - marca do dia eletrónica- protege a integridade de um *email* ou conjunto de dados usando: *timestamping*; assinaturas digitais e resumos de dados. É um selo com a data e hora em que foi enviado o documento garantindo ao remetente e destinatário que a mensagem foi enviada naquele dia e aquela hora; garante assim a integridade e não repúdio do conteúdo da mensagem
- **SCAP**: No âmbito do “Concurso Público Internacional para a Celebração de Contratação para Implementação de Solução Tecnológica de Certificação de Atributos Profissionais com Cartão de Cidadão”, foi adjudicada à MULTICERT, a implementação de um sistema que possibilite certificar de forma eletrónica a associação entre um cidadão e um conjunto de atributos profissionais, devidamente reconhecidos por uma ordem ou empresa, tendo como base a infraestrutura do Cartão de Cidadão (CC). Desta forma será possível potenciar a utilização do cartão de cidadão, permitindo ao seu detentor a realização de assinaturas digitais qualificadas. Adicionalmente, o SCAP permitirá a um cidadão detentor do Cartão de Cidadão, através da utilização do certificado digital existente no mesmo, possa autenticar-se num *site* (ou sistema) com o mesmo

conjunto de atributos profissionais que lhe foram devidamente reconhecidos por uma ou mais entidade fornecedora de atributos (p.e. Ordem dos Médicos).

Esta solução vai permitir que o cidadão consiga autenticar-se num *site*/sistema usando o seu certificado de autenticação do CC; assinar eletronicamente um ficheiro; validar assinaturas eletrónicas

- **STORK 2.0** - projeto de três anos que visa facilitar a criação e generalização de um sistema único de identificação e autenticação eletrónica interoperável e sustentável para a Europa, para cidadãos e empresas. Este projeto tem como objetivos acelerar o desenvolvimento de serviços de identificação digital para serviços públicos; maximizar a apropriação das soluções de identificação digital em toda a Europa; Facilitar a convergência dos setores privados e públicos numa arquitetura e infraestrutura operacional que use a identificação eletrónica para uma autenticação segura de cidadãos e empresários; operacionalizar quatro pilotos transfronteiriços para testar e demonstrar as capacidades e os benefícios de um sistema de identificação digital em ambiente de identificação real. (Sargento, C. 2012)

3.2.2 Estrutura organizacional

Na estrutura orgânico-funcional da Multicert, a Direção-Geral abarca a área da Segurança da Informação e dos Recursos Humanos, sendo que estas duas áreas respondem diretamente ao Diretor Geral. É composta ainda pela Direção de Marketing e Comercial que comporta as áreas de Marketing, Comercial e Apoio ao Cliente. Composta pela Direção de Soluções Avançadas, Direção de Organização e Financeiro e a Direção de Meios que é constituída pela área de Inovação e Desenvolvimento, área de Produção, Sistemas e Serviços e área de Operações

Esta estrutura orgânico-funcional foi recentemente estruturada devida à reformulação que se tem vindo a fazer na Multicert.



Figura 2 Organograma da Multicert

A estrutura acionista da Multicert conta com quatro acionistas sendo:

- SIBS que detém 40% da empresa;
- CTT que detém 20% da empresa;
- INCM que detém 20% da empresa;
- Portugal Telecom com 20% da empresa.

A estrutura é, assim, constituída pelo Conselho de Administração; a Assembleia Geral; um Fiscal Único e uma Direção Geral.

Relativamente aos parceiros de negócio da Multicert (anexo 3), estes beneficiam de formação e de uma linha de apoio direta da Multicert o que lhes permite beneficiar de produtos de segurança de valor acrescentado oferecido pela Multicert.

Todos têm uma possibilidade de integração de produtos e serviços de segurança da Multicert em soluções e produtos próprios; de apoios direto na escolha dos produtos e serviços de segurança que melhor se enquadrem nos requisitos dos seus clientes e ainda incentivos financeiros que condizem com o volume de vendas de serviços e produtos da Multicert.

3.2.3 O software Alfresco

Para auxiliar nos processos e serviços da Multicert é usado o software Alfresco que se constitui como o objeto base desta dissertação.

O Alfresco Apresentado em 2005 pelo cofundador da Documentum John Newton e por John Powell, proporciona uma alternativa *open source* para ECM (*Enterprise Content Management*).

De acordo com um estudo realizado por Manish Nath e Anuja Arora, em 2010, que envolveu uma análise comparativa de treze sistemas de gestão documental, o sistema de gestão documental “Alfresco” mostrou-se ser o melhor dos sistemas em *open source*. A sua implementação resulta na criação de um repositório central, por parte da organização/empresa, com uma tecnologia de indexação e pesquisa de conteúdos, assim como uma ferramenta capaz de circular os documentos (*workflow*), a qual se torna na parte central de todo o seu funcionamento. Sendo uma aplicação inteiramente Java, o sistema “Alfresco” funciona em praticamente qualquer sistema que pode ser executado através da *Java Enterprise Edition*.

O “Alfresco” é, pois, um sistema de gestão documental de código aberto e tem como objetivo fornecer um conjunto de módulos para a gestão documental, sendo que o seu tratamento digital é desencadeado através do processo de workflow, permitindo assim aumentar a produtividade da Organização, uma vez que disponibiliza a informação completa, no momento certo e ao utilizador indicado. O Alfresco reconhece a informação como um recurso que surge na Organização sobre as mais variadas formas, que é criada e gerida por todas as pessoas na Organização, fomentando assim um verdadeiro ambiente colaborativo e contribuindo para a desmaterialização da informação e das relações. (MULTICERT, 2008)

Inicialmente, começou por ser utilizado como uma solução direcionada à gestão documental, sendo que, atualmente, se assume como uma solução válida na área da Gestão de Conteúdos Empresariais (ECM), dado permitir gerir um documento em todas as suas fases desde a criação do mesmo, passando pelo armazenamento, organização e recuperação. (Alfresco, 2012)

Nesta perspetiva um ECM convoca mais os aspetos da captura, organização e partilha de informação entre toda a Organização e menos sobre a tecnologia. A gestão de conteúdos incide no controlo de versões com bloqueio num ambiente de unidade compartilhada, se um colaborador tem um documento particular e outro colaborador está a fazer uma pesquisa, esse não deve ser capaz de encontrar o documento ou até mesmo saber que ele existe. A solução para este problema passa,

por exemplo, pelo controle dos resultados da pesquisa que são restritos com base em configurações de segurança (Alfresco, 2012).

A meta principal do ECM é eliminar processos *ad hoc* que podem expor uma Organização a riscos de conformidade regulatória e outros potenciais problemas, incluem recursos como gestão de registos, taxonomias de conteúdo, recursos de auditoria, *check-in / check-out* e outros controlos de fluxo de trabalho e mecanismos de segurança. Um ECM eficaz pode agilizar o acesso, otimizar a segurança, manter a integridade e minimizar a sobrecarga. (Rouse, M. 2013)

A Multicert tem vindo a utilizar o Alfresco internamente desde que este foi implementado em 2006, e com isso surgiu o reconhecimento e convite para uma associação como *Partner*. É considerado simples de usar e que diminui a curva de aprendizagem, minimizando o impacto de mudança, rápido e intuitivo de implementar e adaptar as necessidades da empresa, diminui o custo e esforço do projeto. Foi esta confiança, motivação e boas práticas que levaram a Alfresco a atribuir o estatuto de *Partner* Certificado à Multicert, sendo portanto a primeira empresa 100% nacional a ser reconhecida como tal (MULTICERT, 2008)

Assume-se como uma solução *Open Source* para *Enterprise Content Management*, reconhece a informação como um recurso que surge na Organização sobre as mais variadas formas, que é criada e gerida por todas as pessoas na Organização, fomentando assim um verdadeiro ambiente colaborativo e contribuindo para a desmaterialização da informação e das relações e facilitando a gestão documental e de conteúdos. (MULTICERT, 2008)

Dada a sua versatilidade e flexibilidade, a solução Alfresco pode ser implementada sob diferentes perspetivas contendo funcionalidades de: gestão de documentos/*records management*, gestão de conteúdos Web, gestão colaborativa, gestão de conhecimento e *imaging* (digitalização)/*image management* apresentando-se como uma solução integrada para a gestão de informação em diferentes formatos. O Alfresco permite gerir cada uma das fases do ciclo de vida da informação - criação, armazenamento, disponibilização, organização, recuperação - através de funcionalidades como o controlo automático de versões, definição e gestão de categorias e definição de meta-informação e *workflows*. (MULTICERT, 2008)

A utilização da solução Alfresco na gestão dos documentos da Entidade de Certificação da Multicert permite:

- Identificar e restringir a criação/atualização de documentos de acordo com os perfis de utilizadores definidos e respetivas permissões;
- Identificar o estado de aprovação em que o documento se encontra;

- Controlar automaticamente as diferentes versões do documento, de forma a garantir não só que a versão mais atual do documento se encontra disponível como também que não há perda das versões anteriores;
- Assegurar que os documentos que se encontram em atualização/edição são identificados, garantindo assim que os conflitos de edição sejam minimizados;
- Garantir que todos os documentos se encontram classificados;
- Garantir que todos os documentos são validados e aprovados (MULTICERT, 2009).

Funcionalidades para a gestão documental:

- Sistema de ficheiros virtual, tornando o ECM tão simples como uma pasta partilhada;
- Acesso por Portal JSR-168;
- Extração de meta-informação e classificação automática a partir de qualquer interface;
- Formato *OpenSearch* que permite pesquisar nos diferentes repositórios Alfresco e através de outros repositórios *OpenSearch* utilizando o Firefox ou IE7;
- Pesquisa simples e avançada tendo por base a meta-informação;
- Serviços de conversão do *Office* para ODF/PDF e de *PowerPoint* para *Flash*;
- Check-in/out com controlo de versões com distinção entre alterações significativas e de menor impacto;
- Audit, para perceber quem criou, quem atualizou, quando foi criado e quando foi atualizado o documento;
- Criação de relações (*linking*) entre documentos através dos diferentes espaços;
- Assistente para criação de espaços com implementação de boas práticas na criação de estruturas de pastas, conteúdos, *templates*, regras e processos;
- Fórum para seguimento de discussões;
- *Workflow* básico baseado em *emails*;
- Integração com Jbpm, um *workflow* avançado e complexo;
- Notificação de alterações via *email* ou RSS;
- Painel de gestão de tarefas;
- Acesso único via NTLM ou LDAP;

- Integração com o MS Office que faz com que guardar um documento seja tão simples como um “save as”;
- Integração com *email*, para arquivar emails e controlar discussões sobre documentos, e ainda associar emails a documentos. (MULTICERT, 2008)

Funcionalidades para a Gestão de Conteúdos *web*

- Sistema de ficheiros virtual em que todos os conteúdos podem ser disponibilizados com um simples *drag-drop*;
- Controlo de versões *Roll-back* com a disponibilização automática de uma nova versão do *website* que permite visualizar o estado exato do website em qualquer ponto do tempo;
- *Disaster recovery* permite rapidamente recuperar a última versão do *site* que se encontra estável;
- Validação de conteúdos com integração de *workflow* customizável para aprovação editorial e validação da disponibilização ao cliente;
- Sistema único que não necessita de servidores/sistemas separados para gerir conteúdos e código;
- *Sites web 2.0* que gere a aplicação web de uma forma integrada os conteúdos e o código;
- Integração do processo de *Quality Assurance* para código e conteúdos;
- Gestão Multi-site onde muitos *websites* com características diferentes podem ser gerados através de um só local;
- Controlo de alterações onde cada utilizador tem uma “*sandbox*” isolada e pode pré-visualizar o impacto das suas alterações no *site*;
- Áreas de trabalho independentes onde os criadores de conteúdo podem reduzir a sua dependência relativamente aos programadores e desenvolver o seu trabalho mais rapidamente;
- *Staging* e virtualização que é a capacidade para pré-visualizar as alterações de qualquer aplicação web dentro de um contexto, incluindo PHP, *Ruby*, JSF, *Tiles*, *Struts*, *Groovy* e .NET;
- Publicação simultânea de diferentes tipos de conteúdos e reutilização de conteúdos em diferentes *websites*;
- Criação de modelos de conteúdos em XML;
- Criação de múltiplas páginas numa única ação suportando múltiplas vistas sobre o mesmo conteúdo incluindo a criação automática de HTML e de PDFs. (MULTICERT, 2008)

Funcionalidades para *Image Management*

- Integração com *Kofax Ascent Capture*;
- Repositório integrado para documentos digitalizados e documentos electrónicos;
- Regras de negócio para a classificação automática;
- Extração de meta-informação;
- Conversão de formatos;
- Pré-visualização;
- Gestão de formatos (MULTICERT, 2008)

Funcionalidades para *Records Management* (funcionalidade não utilizada pela Multicert)

- Planos de classificação que proporciona a classificação automática e agenda de tarefas de retenção através de planos de classificação e de retenção pré-definidos;
- Armazenamento de documento com um simples “*drag and drop*” garantindo as regras de negócio e extração automática de meta-informação;
- Gestão de ciclo de vida automática fornecendo uma agenda de ações automáticas sobre os documentos e meta-informação;
- Políticas de arquivo e retenção como gestão de documentos com baixos níveis de utilização e importância para a Organização, recuperação de documentos arquivados, e completa destruição de documentos, baseando-se em políticas de retenção;
- Conformidade com os requisitos da DOD 5015.2;
- Validação de meta-informação e gestão de *workflow* com a garantia da integridade dos documentos através da associação de *workflows* de validação;
- Conversão automática de formatos proprietários (MS Office) para formatos de preservação a longo prazo como *Open Document Format* (ODF) e *Portable Document Format* (PDF);
- Associação de documentos com a criação de ligações entre eles;
- Auditoria, controlo e monitorização das ações sobre os documentos;
- Funcionalidades para *Social Computing Enterprise 2.0*;
- Integração com o *Facebook*;
- Integração com o *iGoogle*;
- Integração com *Blogs* onde o conteúdo criado e armazenado no Alfresco pode ser rapidamente publicado em blogs;

- Integração com o *MediaWiki*;
- Discussão sobre documentos e colaboração ativa e controlada na produção de documentos;
- Gestão de tarefas, calendários e contactos, partilhada por todos os colaboradores. (MULTICERT, 2008)

A empresa criadora do Alfresco disponibiliza todas as funcionalidades de duas formas, através do Alfresco *Community Labs* e o Alfresco *Enterprise Edition*.

A versão *Community Labs* é uma ferramenta em constante inovação e experimentação. É vocacionada para *developers* e entusiastas da tecnologia em ambientes não críticos. Esta versão apresenta-se como uma oportunidade para que todos possam dar o seu contributo na melhoria do ECM, identificando oportunidades e apontar bugs. Está em constante evolução visto ser muito dinâmico funcionando até como “laboratório de investigação” e como fonte de novas funcionalidades e necessidades.

Já a versão *Enterprise* denomina-se como a “versão de produção” que é submetida a exigentes testes, é certificada e consegue reunir todas as condições necessárias para fornecer uma solução de confiança, fiável e ao mesmo tempo inovadora. Esta versão encontra-se projetada para que as organizações consigam poupar tempo, investimento e recursos na implementação de um ECM. Oferecendo o acesso à rede de parceiros experientes e certificados, bem como ao suporte técnico e à equipa de *development* da Alfresco, esta versão é indicada para organizações que desejam ver resultados rapidamente, encarando o ECM com seriedade na Multicert e que desejam suporte e apoio quando as dificuldades surgirem (MULTICERT, 2008).

Ao nível da simplificação da gestão de documentos é destacado no Alfresco:

- Substituição de *shared files drives* por *virtual file system*
- Integração com *office*
- Extração de meta-informação
- Regras de negócio para automatizar processamento manual
- Integração com portais
- Pesquisa *Google-like*, *browsing Yahoo-like*
- *Workflow* baseado em pastas
- *Smartspace*s (pastas, tipos de conteúdos, regras)

- *Zero footprint* cliente²⁵.

A abordagem do Alfresco pode ser resumida da seguinte forma:

- **Fácil de usar:** A filosofia do Alfresco é que a facilidade de uso é sobre o uso de conceitos já conhecidos. Tem uma interface bastante simples e fácil de utilizar, funcionando como um motor de busca semelhante ao Google
- **Interface de unidade compartilhada:** o repositório Alfresco tem uma unidade nativa de interface compartilhada CIFS que foi conseguido usando Java puro. Isso permite que um utilizador, vá para a sua unidade C: ou o conteúdo da área de trabalho e *drag-and-drop* no Alfresco, ou podem simplesmente selecionar Arquivo / Salvar como. Podem até mesmo arrastar o conteúdo para fora do Alfresco direto para uma pasta e ele funciona porque a pasta pensa que está a aceder a uma unidade do arquivo compartilhado da Microsoft.
- **Workflow:** Alfresco também queria criar um fluxo de trabalho que era lógico e refletiu a forma como as equipas realmente funcionam. As pessoas muitas vezes não usam o fluxo de trabalho, pois é muito difícil. As pessoas geralmente criam uma pasta, colocam um documento no seu interior com um adesivo amarelo na parte da frente com um monte de nomes escritos para baixo. Então o Alfresco espelhou esta abordagem quando projetou um fluxo de trabalho muito simples, baseado em pastas.
- **Smart Space:** para o lançamento de um produto ou qualquer projeto repetível uma Organização terá uma série de pastas, uma série de documentos modelo que eles precisam e uma série de processos que devem percorrer para rever ou produzir garantias, definições de produtos, etc.. Com um espaço inteligente todos os elementos do lançamento de um produto podem ser encapsulados e um utilizador pode desenvolver regras em torno dos formatos em que estão distribuídos.
- **Extração de propriedades e meta-informação:** Se um utilizador arrasta um documento do Word a partir de seu desktop para o Alfresco, eles podem extrair automaticamente a meta-informação ou propriedades. Pode haver conteúdo proprietário, nome e palavras-chave ou títulos de documentos e tudo pode ser extraído sem ser reintroduzidos no Alfresco, permitindo que o utilizador possa pesquisar sobre eles numa data futura.
- **True Zero footprint client:** Alfresco acredita que a "facilidade de uso" deve alargar-se para fora da aplicação. O Alfresco criou esta simples

²⁵ Apresentação interna sobre o Alfresco

funcionalidade, porque não há nada para instalar na área de trabalho do utilizador. Isso é chamado de um verdadeiro cliente pegada zero. (ALFRESCO)

Na Multicert, o Alfresco é visto como uma boa aposta para a Gestão dos Conteúdos, contudo, é necessário fazer ajustes para que a sua abordagem promova a desejada preservação e acesso à informação no longo prazo.

4. A GI na MULTICERT - Capítulo Confidencial

Este capítulo não se encontra em acesso público por conter informação confidencial da Multicert.

5. Bases para a implementação do Repositório Digital Seguro

5.1 A conformidade nos serviços de Gestão Documental via Alfresco

Na Multicert, grande parte da informação é criada em formato electrónico, tornando-se impossível colocar como alternativa a impressão em papel para a sua preservação futura. Nesse sentido, a Multicert procurou uma solução que agregasse toda essa informação num só local e garantisse a sua disponibilização a quem necessitasse de a consultar. A escolha recaiu no Alfresco considerado como um Sistema de Gestão Documental, ou seja, um sistema tecnológico usado pela Multicert que permite aos seus utilizadores a gestão dos fluxos dos documentos, bem como proceder ao seu arquivo para posterior utilização e gestão.

O objetivo a atingir passa pela vontade em estruturar o seu sistema de informação como um Sistema de Informação Ativa e Permanente (SIAP) constituindo o Alfresco, ou outra solução que lhe suceda, um componente de *software* que integra o Sistema de Gestão de Informação Ativa e Permanente (SGIAP), capaz de gerir eficazmente o grande volume informacional e proceder à sua preservação a longo prazo.

Na base deste objetivo está o modelo sistémico e informacional SIAP, um modelo teórico que orienta a operacionalização do SIAP especificando conceitos, papéis e envolvendo a Organização e os seus colaboradores no processo de adequação da GI com vista à sua transformação, desde logo, numa Organização “aprendente” e, posteriormente, numa “Organização inteligente”.

Para a GI é fundamental que se garanta o controlo do processo de produção, fluxo, organização, armazenamento, preservação, acesso e uso dos documentos, assegurando a aplicação de instrumentos normativos, de técnicas de autenticação e certificação digital, de captura de meta-informação adequada à produção dos documentos em formatos específicos para a sua preservação mas que, por isso, não limitem o seu uso, e que finda a sua utilização se decida a sua inclusão ou não no repositório digital.

Por outro lado, na perspetiva de um sistema de Gestão de Informação, e como afirmam Pinto e Silva (2005), as organizações precisam de uma abordagem que “congregue desde a fase de concepção da plataforma tecnológica (Hardware e

Software), até à produção, circulação, avaliação, armazenamento, disponibilização e preservação da informação, toda a Organização e os seus processos de negócio”.

Neste modelo sistémico é fundamental que se congregue todo o ciclo de vida da informação e a pluridimensionalidade e interoperabilidade da mesma. No caso da Multicert, a informação não passa por todo o ciclo de vida. Há a fase da produção e disponibilização da informação, mas nenhuma é eliminada ou descartada quando termina a sua tramitação administrativa.

O estudo e especificação desenvolvidos pretendeu, pois, perceber os requisitos que são suportados pelo Alfresco e fazer uma análise comparativa com o MoReq 2010, adequando-o aos requisitos exigidos para a constituição de um Sistema de Informação Ativa e Permanente (SIAP), como componente de *software* do Sistema de Gestão de Informação Ativa e Permanente (SGIAP) a implementar na Multicert e, seguidamente com o auxílio da norma ISO 16363:2012, partir desta adequação e promover a futura certificação do componente repositório (estrutura de gestão, *hardware*, *software* e serviços), constituindo um repositório digital confiável.

5.1.1 O Modelo de Requisitos Modulares para a Gestão de Documentos: Moreq 2010

No modelo de especificação de requisitos europeu MoReq2010, estão sistematizados os *Requisitos Modulares para Sistemas de Gestão de Documentos* (SGD), abarcando princípios e funcionalidades que as aplicações destinadas à Gestão Documental devem apresentar para promover a captura, acesso e gestão dos documentos que circulam na organização. Estes requisitos estão divididos em funcionais e não funcionais e servem de orientação para a elaboração de um conjunto de funcionalidades que são essenciais para o bom funcionamento e cumprimento dos objetivos de um Sistema de suporte à Gestão de Informação.

Visa-se desenvolver uma arquitetura adequada que permita garantir a visão integrada do Sistema de Informação; a possibilidade de módulos específicos para alargar funcionalidades de atividades mais especializadas; garanta a rastreabilidade permanente com ações periódicas de auditoria; migração da informação entre sistemas quando se verifica uma evolução da tecnologia estabelecendo por isso políticas de preservação digital; e ainda realizar auditorias que comprovem a conformidade ao MoReq2010 ou outras especificações.

O MoReq2010 está organizado por serviços que o SGD deve contemplar no seu todo, entre os quais se encontram: o Serviço do Sistema; o Serviço de Utilizadores e Grupos; o Serviço de Perfis; o Serviço de Classificação; o Serviço de Registo de

Documentos; o Serviço de Meta-Informação; o Serviço de Seleção e Eliminação; o Serviço de Retenção; o Serviço de Pesquisa; o Serviço de Exportação.

Com base na análise da maturidade optou-se por analisar os serviços mais relacionados com funcionalidades usadas no Alfresco e relevantes para a função de Repositório: Registo de Documentos; Meta-informação; Classificação; Seleção e Eliminação e Retenção.

5.1.2. Especificação e conformidade aos requisitos MoReq2010

O Sistema de Gestão Documental deve garantir a “autenticidade, fidedignidade e integridade dos documentos ao longo de todo o ciclo de vida, que não se extingue com a conclusão do correspondente processo de decisão mas obriga a uma preservação prolongada, conforme a importância probatória que lhe é intrínseca”. (MoReq2010).

Com isto pode-se destacar os principais requisitos funcionais que um SGD deve permitir de acordo com o MoReq 2010:

- Criação, eliminação e destruição de utilizadores e grupos;
- Alteração de lista de controlo de acesso de qualquer entidade;
- Criação, eliminação e destruição de classes e alteração dos seus meta-informação;
- Alteração da tabela de seleção associada a uma classe;
- Substituição de uma classe já associada por outra classe;
- Criação, eliminação e destruição de agregações e alteração da sua meta-informação;
- Criação de documentos de arquivo e alteração da sua meta-informação;
- Reclassificação de um documento de arquivo;
- Eliminação de meta-informação de um documento de arquivo residual desde que a ação seja justificada e o evento fique registado;

O Sistema de Gestão Documental deve também:

- Promover a desmaterialização dos processos - Registo, digitalização, circulação e armazenamento de documentos em formato eletrónico;
- Reduzir os custos;
- Promover a segurança no acesso aos documentos;
- Melhorar os fluxos de trabalho - Tratamento de processos com maior rapidez e controlo na circulação para tomadas de decisão, o que aumenta a produtividade e origina significativas melhorias na gestão de recursos;

- Melhorar o acesso à informação;
- Eliminar informação duplicada;
- Diminuir tempo gasto na pesquisa e recuperação da informação;
- Promover a qualidade dos serviços prestados - Ao promover um maior desempenho de toda a Multicert, o controlo de prazos e a integridade da informação, melhoraria a qualidade do serviço prestado ao cliente.

A arquitetura de serviços do Sistema de Gestão Documental baseado no Moreq2010 deverá:

- Abranger todo o ciclo de vida dos documentos de arquivo;
- Garantir as características específicas dos documentos de arquivo;
- Controlar os prazos de conservação estabelecidos;
- Desenvolver estratégias de Preservação Digital dos Documentos;
- Disponibilizar o acesso aos documentos de arquivo.

Os requisitos incluídos na especificação devem resultar num sistema capaz de gerir documentos digitais com os níveis de confiança e integridade pretendidos. Além disso, devem combinar as vantagens dos processos electrónicos de trabalho com a teoria clássica de gestão de documentos, ao nível das operações de avaliação e seleção da informação, apesar de a Multicert considerar que toda a informação que produz é para conservar de forma permanente.

A análise aos requisitos está representada no *Documento de Especificação de Requisitos* disponibilizado em anexo (anexo 11).

5.2. A conformidade no serviço de Repositório

Terminada a análise da conformidade aos requisitos do Moreq2010, com o intuito de fazer uma comparação com o MoReq 2010, adequando-o aos requisitos exigidos para a estruturação do componente de software de um Sistema de Gestão de Informação Ativa e Permanente (SGIAP) a implementar na Multicert, recorreu-se à norma ISO16363:2012, para promover a futura certificação do componente repositório (estrutura de gestão, *hardware*, *software* e serviços) como um repositório digital confiável.

5.2.1 A ISO 16363:2012

Para a certificação do Repositório Digital, procedeu-se à realização de um diagnóstico de conformidade do Alfresco na perspetiva do repositório (numa das arquiteturas previstas no MoReq2010: *“in place” records management* ou *“in app” records management*) aos requisitos da norma ISO 16363:2012. Na proposta desenvolvida são sugeridos documentos que poderão ser criados para que o requisito venha a ser cumprido parcialmente ou na sua totalidade.

A norma ISO 16363 é o instrumento de referência para a realização deste trabalho resultando da revisão da *checklist* do TRAC - *Trustworthy Repositories Audit Certification: Criteria and Checklist*. A norma é um instrumento para a certificação que, de acordo com os seus critérios, não obsta a que seja necessário uma constante monitorização, planeamento e manutenção, assim como a implementação de uma estratégia e ações para que os repositórios consigam levar a cabo a missão contínua de preservar digitalmente os documentos.

5.2.2 Especificação e conformidade aos requisitos ISO 16363

Grande parte da informação da Multicert é criada em formato electrónico, tornando-se impossível colocar como alternativa a impressão em papel para a sua preservação futura, centrando-se as necessidades na existência de um repositório digital de confiança para o seu armazenamento e acesso continuado no longo prazo.

Numa definição abrangente pode-se definir um **repositório digital de confiança** como um repositório que tem como missão fornecer o acesso confiável, seguro e no longo prazo aos recursos informacionais digitais da comunidade que serve, neste caso a Multicert e o seu negócio, agora e no futuro (ISO 16363).

Existem várias possibilidades para criar o repositório digital de confiança/seguro. Uma delas é fazer com que o Alfresco possa interagir com um repositório digital certificado, mantendo a informação que se pretende preservar a longo prazo nesse mesmo repositório, mantendo a ligação ao Alfresco, ou então fazê-lo agir como um repositório digital seguro obedecendo a determinados requisitos, nomeadamente:

- ter uma declaração de missão que reflita um compromisso com a preservação, a preservação a longo prazo, a gestão e acesso à informação digital;
- ter um Plano Estratégico de Preservação que define a abordagem que o repositório terá no apoio a longo prazo da sua missão;

- ter mecanismos de revisão, atualização e desenvolvimento das suas Políticas de Preservação em curso, à medida que o repositório cresce e a tecnologia e a prática da comunidade evolui;
- comprometer-se com os princípios de transparência e responsabilidade em todas as ações de apoio à operação e gestão do repositório que afetam a preservação de conteúdos digitais ao longo do tempo;
- ter e manter contratos ou acordos de depósito apropriados para materiais digitais que gere, preserva e/ou aos quais fornece acesso;
- ter mecanismos em vigor para controlar o seu ambiente de preservação;
- identificar e gerir os riscos das suas operações de preservação e os objetivos associados à infraestrutura do sistema;
- manter uma análise sistemática dos fatores de risco de segurança associado a dados, sistemas, pessoal e instalações físicas.

Um repositório digital de confiança deve entender ameaças e riscos dentro de seus sistemas. Ao repositório são exigidas uma monitorização, planeamento e manutenção constantes, bem como ações conscientes e a implementação da estratégia adotada para concretizar a sua missão no âmbito da preservação digital.

Todos aqueles que depositarem informação no repositório terão que contar com um ambiente de preservação digital colaborativo para que essa informação seja preservada e garantida a sua acessibilidade no longo prazo.

Para manter o estado de confiança, o repositório deve realizar frequentemente auditorias e comunicá-las ao seu público-alvo que são essencialmente os colaboradores internos da Multicert. Ao realizar frequentemente as auditorias ao repositório e divulgá-los aos principais interessados (Colaboradores), estes vão criar um “laço” de confiança com o Alfresco, incentivando-os a colocar toda a informação produzida no repositório e também a procurar a informação de que necessitam.

O *Documento de Especificação Requisitos* tem como objetivo especificar um conjunto de requisitos para a implementação e gestão do Repositório Digital da Multicert.

Este encontra-se dividido em duas partes fundamentais: a primeira, e como referido) diz respeito à análise da conformidade com os requisitos do MoReq2010 e a segunda à análise dos requisitos com a norma ISO 16363:2012 - *Space Data and Information Transfer System - Audit and certification of trustworthy digital repositories*. As duas análises serão especificadas mais detalhadamente a seguir.

O documento de especificação de requisitos encontra-se dividido em quatro partes nomeadamente:

- *Introdução;*
- *Perspetiva do repositório;*
- *Requisitos de Melhoria;*
- *Requisitos para a Certificação.*

Na Introdução são definidos os objetivos da elaboração do documento, assim como o âmbito em que se insere, o público-alvo a que se destina e ainda a forma como está estruturado o documento.

Seguidamente é apresentada a descrição do objeto de estudo, o Alfresco. Aqui faz-se uma descrição das suas funções e principais características, a arquitetura do *software* e ainda restrições que são aplicadas ao sistema. Esta parte é importante para que se perceba como funciona o sistema e assim poder fazer-se uma correta análise dos requisitos, direcionados essencialmente à componente de *software*.

Apresenta-se depois a análise dos requisitos de melhoria referentes ao Moreq2010. Este estudo teve como base a análise de alguns dos serviços descritos no Moreq2010 e estão estruturados numa tabela com duas colunas, a primeira das quais refere-se aos requisitos do MoReq2010 e a segunda ao nível de conformidade do Alfresco. Esta é apenas uma primeira avaliação ao sistema, no entanto o trabalho deverá ter continuidade com a colaboração dos diversos serviços da Multicert para que a avaliação seja mais aprofundada.

Por fim apresenta-se a análise relativa aos requisitos para a certificação. Como salientado, esta análise visou perceber a maior ou menor conformidade da situação atual da Multicert face à criação de um repositório confiável, utilizando-se para o efeito a norma ISO 16363:2012.

Efetuada a análise aos requisitos, procedeu-se ao estudo da conformidade com a documentação existente na Multicert para perceber se esta cumpria esse requisito na totalidade. Foram encontrados vários documentos que no fundo cumpriam o requisito mas alguns só parcialmente.

Para uma leitura e compreensão mais inteligível dos requisitos, estes foram dispostos tal e qual aparecem na norma, estruturados nas três grandes secções: Infraestrutura Organizacional; Gestão de Objetos Digitais e Infraestrutura e Gestão de Riscos de Segurança.

Estas secções estão divididas em três colunas, sendo que na primeira coluna temos a referência aos requisitos da norma. Na segunda coluna aparece-nos a conformidade a nível documental do requisito. Aqui é referido o documento/documentos que

comprovam a conformidade daquele requisito. A conformidade é referida a cor “azul”, sendo que ainda há a referencia a documentos que se poderão criar para proceder à conformidade dos requisitos que não estão contemplados no Repositório, a cor “vermelha”.

Por último encontra-se a terceira coluna que diz respeito ao nível de conformidade do Requisito, pois embora existam evidências da existência do mesmo, esta evidência pode não ser total ou não estar bem implementada.

Concluiu-se pois que foi necessário aplicar todos os requisitos da norma para que o repositório possa ser certificado internacionalmente.

Após a elaboração deste estudo e da consequente criação do documento de especificação de requisitos, tornou-se claro que a Multicert ainda tem algum caminho a percorrer para que possa Certificar o Repositório. O primeiro passo foi dado nesta dissertação pois faz-se o diagnóstico necessário para perceber como as coisas estão a ser feitas atualmente. Os dois estudos iniciais da maturidade da Gestão da Informação e do ECM tornaram-se vitais para se ter a real noção da gestão que é feita a nível dos processos documentais.

Também a enunciação da estrutura documental de suporte é fundamental para apontar os próximos passos.

Deve-se ter também em conta a rápida inovação a nível tecnológico com que somos diariamente confrontados e neste sentido há que fazer um esforço contínuo para manter o SGD atualizado nesse sentido para que não se torne obsoleto e que a preservação da Informação a nível digital seja uma prática constante na Multicert para que seja disponibilizada a quem precisa, ou seja, criar também as bases para a preservação em meio digital.

A necessidade de certificar o Repositório Digital da Multicert tornou evidente a necessidade de criar um Plano de Preservação da Informação e consequentemente a base documental de suporte que será fundamental para o processo de certificação.

Partindo do levantamento dos instrumentos normativos, nomeadamente da ISO 16363 e de modelos e guias de boas práticas existentes na área da Preservação (OLIVEIRA, 2014; Sousa, 2013; Oliveira e Sousa, 2014) foi esboçada a estrutura de Documentos de Suporte à Especificação (anexo 7).

Esta estrutura contempla os documentos a criar, apresentando-se nesta dissertação os guias de suporte à especificação elaborados.

Na Multicert já existem alguns documentos (assinalados a preto) que são essenciais para servir de base ao Plano de Preservação da informação em meio Digital

da Multicert, como: o Plano de Contingência, Plano de Recuperação de Desastres, Plano de Formação; Ata de Reunião; Política de *Backups*; Identificação e Avaliação de Formatos; Matriz de competências e funções (anexo 7).

Os documentos a criar são (assinalados a azul): Declaração de Missão; Acordo de Custódia; Identificação de Sistemas de Informação; Plano de Preservação; Política de Preservação; Estratégia de Preservação; Registo de Eliminação:

Declaração de Missão: Apresenta-se como um guia para a definição de uma declaração de missão para a elaboração do plano de preservação da informação em meio digital da Multicert. Embora já exista uma missão definida na Multicert, esta não é especificamente dirigida ao repositório pelo que se decidiu criar um documento novo com base noutras declarações de missão nomeadamente dos Arquivos Metropolitanos de Londres.

Acordo de Custódia: Este documento de suporte à especificação apresenta-se como um guia para a definição de um acordo de custódia da informação para a elaboração do Plano de Preservação da Informação em meio digital da Multicert.

Identificação de Sistemas de Informação: este documento de suporte à especificação serve de guia para a definição de um diagnóstico dos sistemas tecnológicos e informacionais, para a elaboração do Plano de Preservação da Informação Digital da Multicert.

Plano de Preservação: apresenta-se como um guia para a definição de uma estrutura base para a construção do Plano de Preservação da Informação da Multicert. Este documento contém as principais diretrizes a serem seguidas para a elaboração de um Plano de Preservação da Informação. Foi ainda elaborado como suporte ao conteúdo informacional um anexo sobre as várias e possíveis estratégias de preservação.

Estratégia de Preservação: documento de suporte à especificação que fornece as bases para a definição de uma estratégia de preservação da informação a longo prazo, para a elaboração do Plano de Preservação da Informação em meio digital da Multicert.

Política de Preservação: documento que serve de guia para a definição de uma Política de Preservação em meio digital, para a elaboração do plano de preservação da informação em meio digital da Multicert, fornecendo os tópicos base a abordar para a elaboração deste documento.

Registo de Eliminação: Este documento de suporte à especificação apresenta-se como um guia para a definição de um auto de eliminação de documentos criando assim um registo desta fase do ciclo de vida informacional, para a elaboração do Plano de Preservação da Informação em meio digital da Multicert.

Os Documentos que irão ser criados têm como base um documento interno da Multicert, que está disponível no Alfresco, que apenas é acessível aos colaboradores.

Os documentos base da Multicert são constituídos por:

- Uma capa com o nome do documento,
- Identificação do tipo de documento,
- Identificação do documento (que é o seu identificador);
- Identificação do nível de acesso (publico, restrito ou confidencial);
- Número de versão e data de criação.

Na folha de rosto, há a indicação:

- Do identificador do documento;
- Palavras-chave ou meta-informação de pesquisa;
- Tipologia documental (plano, politica, processo,...);
- Título do documento;
- Língua original e de publicação (que pode ser distinta);
- Nível de acesso;
- Data e versão (tal como contém a capa);
- Identificador do modelo de documento usado e qual a versão do modelo.
- Autoria do documento;
- Data de criação;
- Indicação de quem aprovou o documento e respetiva data.

Seguidamente encontram-se 3 caixas distintas. Na primeira encontra-se a indicação do histórico de versões. Cada vez que se altera o documento deve-se registar nesse campo o que foi alterado e quando foi alterado. Assim consegue-se ter a perceção de todas as alterações efetuadas.

Também é feito referência aos documentos relacionados com esse documento e os apêndices associados.

No sumário encontramos referência ao Resumo Executivo; Introdução que é dividida em Objetivos, Público-alvo e estrutura do documento; Contexto geral do documento; e os seguintes capítulos que irão constituir o documento. Ainda as conclusões e as referências bibliográficas.

Os guias de suporte à especificação que foram criados no âmbito desta dissertação obedecem ao mesmo modelo documental, e estão disponíveis em anexo.

Após a identificação e elaboração dos documentos que servem de suporte à especificação, passa-se para o desenvolvimento do respetivo documento de requisitos.

5.3 Bases para o planeamento da preservação em meio digital

A capacidade de preservar a informação é indissociável da existência de um repositório confiável e de um plano de preservação alinhado com a Política de GI no contexto do negócio.

5.3.1 Planos de preservação

De acordo com Becker et. al (2009) um plano de preservação define uma série de ações de preservação a ser tomadas por uma instituição responsável, devido a um risco identificado para um determinado conjunto de objetos digitais ou registos. O Plano de Preservação leva em conta as políticas de preservação, obrigações legais, restrições organizacionais e técnicas, requisitos de utilizador e objetivos de preservação e descreve o contexto da preservação, as estratégias de preservação e a decisão resultante de uma estratégia, incluindo a fundamentação da decisão. Ele também especifica uma série de etapas ou ações (chamado plano de ação de preservação), juntamente com as responsabilidades, regras e condições para a execução na coleção. Desde que as ações e sua implantação, bem como o ambiente técnico permitirem, este plano de ação é uma definição de *workflow* executável.

Encontra-se também na literatura, na opinião de Barbedo, et. al (2010) que um Plano de Preservação Digital é um documento estratégico que contém políticas e procedimentos para a constituição de uma estrutura técnica e organizacional que permita preservar continuamente os documentos dos arquivos eletrónicos através de ações realizadas sobre os objetos digitais que os compõem. Este permitirá identificar quais as funcionalidades que devem ser implementadas e a forma de as implementar, para manter a integridade e usabilidade dos documentos eletrónicos ao longo do tempo.

Um *Plano de Preservação Digital* deve, assim, conter os seguintes elementos:

- Identificação
- Estado e *triggers*
- Descrição da configuração institucional
- Descrição do acervo
- Requisitos para a preservação
- Comprovação de decisão relativo à estratégia de preservação
- Custos
- Funções e responsabilidades
- Plano de ação de preservação (Becker et.al. 2009).

5.3.2 O Projeto PLANETS e o Modelo de Planeamento PLANETS/OAIS

O PLANETS (*Preservation and Long-term Access through NETworked Services*) foi um projeto financiado pela União Europeia, coordenado pela *British Library* tendo envolvido bibliotecas e arquivos nacionais bem como bibliotecas de universidades e organizações comerciais de toda a Europa. O objetivo deste projeto foi construir ferramentas e serviços de preservação para bens culturais e científicos.

A arquitetura de preservação desenvolvida pelo projeto é conhecida como o *Planets Interoperability Framework*. Esta arquitetura foi desenhada e projetada para funcionar em paralelo com os *software* de repositórios existentes, proceder à ingestão de material diretamente do repositório e tornar os resultados de preservação disponíveis para nova ingestão no repositório (Becker et.al. 2009).

O projeto PLANETS concentra-se nas questões de preservação lógica (em oposição à preservação de *bit-stream*), fornecendo ferramentas para a caracterização e migração de objetos digitais, bem como ferramentas de emulação para aceder aos objetos digitais originais. Sendo que uma das suas visões é fornecer a maioria dos resultados do projeto num único pacote para *download*, que deve ser simples de instalar, configurar e administrar - o *Planets Software Suite* (King, et.al. 2009).

A um nível superior, a arquitetura PLANETS centra-se num servidor *gateway*, sendo que este possui dois conjuntos de interfaces: o *Portal Serviços*, que fornece um meio seguro para os utilizadores interagirem com o servidor, e a *API WFlow*, que permite ao servidor interagir com serviços de preservação como uma parte de um fluxo de trabalho de preservação. Os principais componentes subjacentes ao servidor *gateway* são o *Core Registry* (contendo informações de representação e informações significativas sobre os tipos de propriedades de objetos digitais e formatos,

conjuntamente com ferramentas de caracterização e ação de preservação), o *Service Registry* (contendo informações sobre serviços compatíveis com o Planets) e do *Data Registry* (contendo os objetos digitais modificados pelo sistema) (King, et. al. 2009).

Como foi referenciado anteriormente, o projeto PLANETS na fase final do planeamento do plano de preservação baseia-se no modelo OAIS.

O objetivo principal de um SAAI (Sistema Aberto de Arquivo de Informação) é preservar informações para uma designada comunidade durante um longo período de tempo.

O método de planeamento do PLANETS implementa as estratégias de preservação, as normas, os projetos e planos de migração e funções do modelo OAIS. A função de desenvolver estratégias e normas de preservação é responsável por desenvolver e recomendar estratégias e normas para preservar as atuais explorações e novas apresentações para o futuro (Becker, et.al, 2009).

As entidades funcionais do modelo OAIS fornecem possíveis restrições e requisitos para as etapas dentro da abordagem de planeamento e podem desencadear outras atividades de planeamento.

Neste modelo foram destacadas as seguintes funções:

- O *Monitor Designated Community* e *Monitor Technology* fornecem relatórios sobre a evolução e as mudanças na comunidade designada e tecnologias relevantes.
- O *Manage System Configuration* e o *Consumer Service* fornecem um relatório com informações do sistema de arquivo e comentários de desempenho de consumo para a função de *Develop Preservation Strategies and Standards*. Estes comentários podem implicar requisitos em matéria de acesso, comportamento e uso dos objetos digitais no sistema. As informações de desempenho podem, assim, aumentar as exigências que devem ser cumpridas por potenciais estratégias de preservação.
- A função *Monitor Technology* oferece a funcionalidade para avaliar tecnologias emergentes por pedidos de protótipo. Os resultados são os primeiros sinais de uma reflexão aprofundada sobre as novas e não testadas ferramentas e serviços na etapa de definir alternativas do método de planeamento. O resultado das três primeiras fases é uma recomendação para a ação de preservação.
- Por último, a função de *Develop Packaging Designs and Migration Plans* é responsável por fornecer os planos de migração detalhados. Usa a

recomendação da função de desenvolver estratégias e normas de preservação, como base para a construção de um plano de preservação, incorporando aspectos organizacionais, tais como os papéis e as pessoas responsáveis para realizar o plano. Cria ainda um plano de preservação executável que inclui mecanismos de garantia da qualidade e captura de meta-informação. (Becker, 2009)

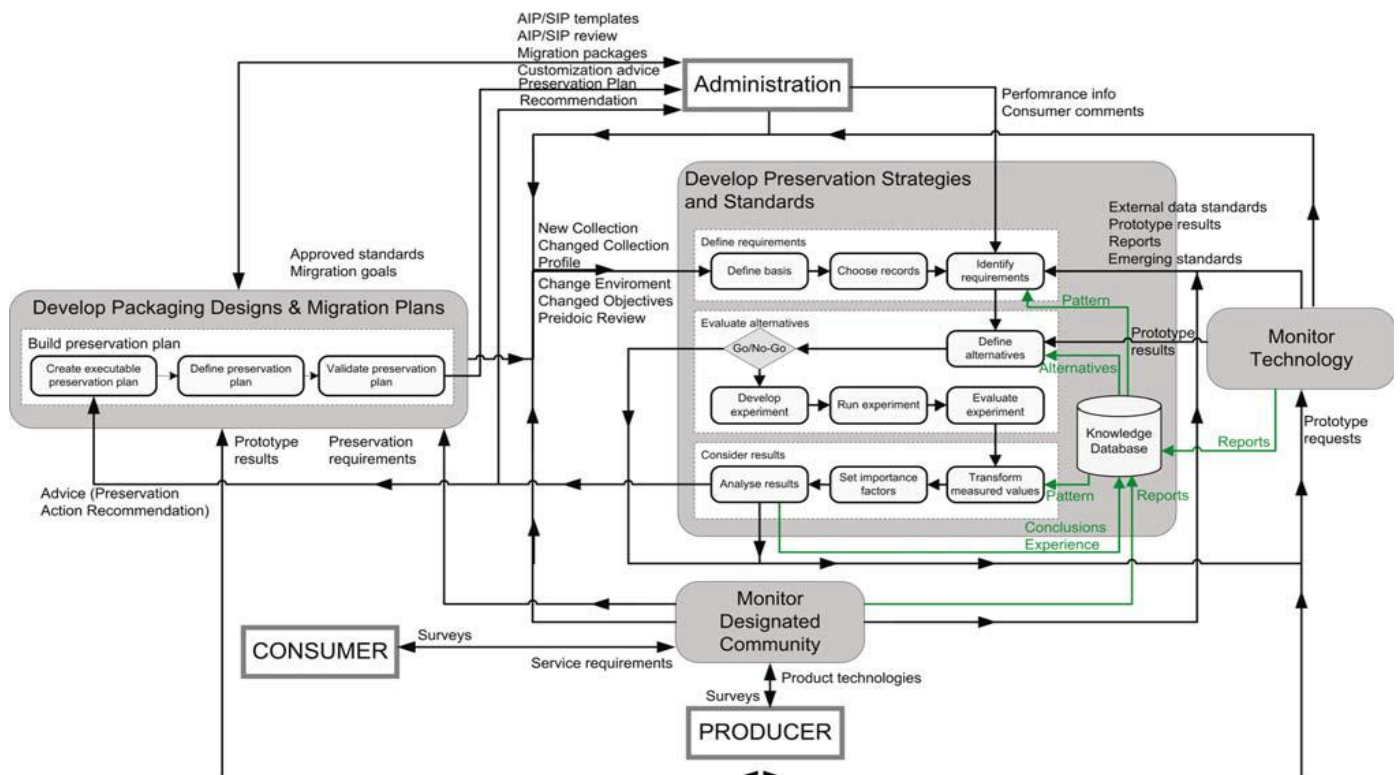


Figura 5 O modelo de planeamento PLANETS segundo o OAIS (Becker, et.al, 2009)

Becker, et al. (2009) apresentam também os critérios que consideram fundamentais para um repositório se tornar confiável. São eles:

- Procedimentos, políticas e transparência na documentação;
- Monitorização, envolvimento e histórico de alterações;
- Propriedades significantes.

a) Procedimentos, políticas e transparência na documentação

Políticas bem definidas e transparência na documentação são condições consideradas essenciais pelo TRAC e o Nestor. O relatório TRAC afirma que a transparência é a melhor garantia que o repositório opera em conformidade com as normas aceites e a prática. A transparência é essencial para a

prestação de contas, e ambos são atingidos por meio de documentação ativa, em curso.

A abordagem de planejamento de preservação avalia estratégias de preservação de forma consistente, permitindo decisões informadas e bem documentadas. Isso impõe a definição explícita dos requisitos de preservação sob a forma de objetivos específicos.

A ferramenta *Plato* implementa a abordagem de planejamento, suporta toda a documentação automatizada dessa atividade. Os potenciais efeitos das estratégias de preservação de objetos digitais são descritos, e a história dos planos de preservação é criada, revisada e atualizada.

b) Monitorização, envolvimento e histórico de alterações

As políticas institucionais precisam definir serviços para a Coleção, para o seu desenvolvimento e para as alterações na tecnologia e comunidades designadas.

Ao rever os planos afetados usando o *workflow* do planejamento, o repositório é capaz de avaliar o impacto das mudanças de maneira a reagir em conformidade. A avaliação verifica o plano de preservação implementado, considerando as mudanças nos requisitos e na prática ou as alterações na coleção que pode resultar numa atualização do plano de preservação, substituindo o plano existente.

c) Propriedades significantes

A árvore de objetivos, falada anteriormente, especifica requisitos, soluções e metas para a preservação. A parte central desta é formada pela especificação das propriedades significativas dos objetos que devem ser preservados. Esses requisitos documentam as propriedades dos objetos que precisam ser preservados e alinhá-los com as ferramentas de medição automatizadas, sempre que estas estejam disponíveis.

Processo de planejamento da preservação

No que concerne ao processo de planejamento da preservação, o projeto PLANETS pressupõe uma avaliação de ações potenciais e passos específicos a serem considerados que estão divididos em quatro fases que resultam num plano de preservação, são eles de acordo com Becker, et. al (2009):

1. Definir os requisitos;

2. Avaliar alternativas;
3. Analisar os resultados;
4. Criar o plano de preservação.

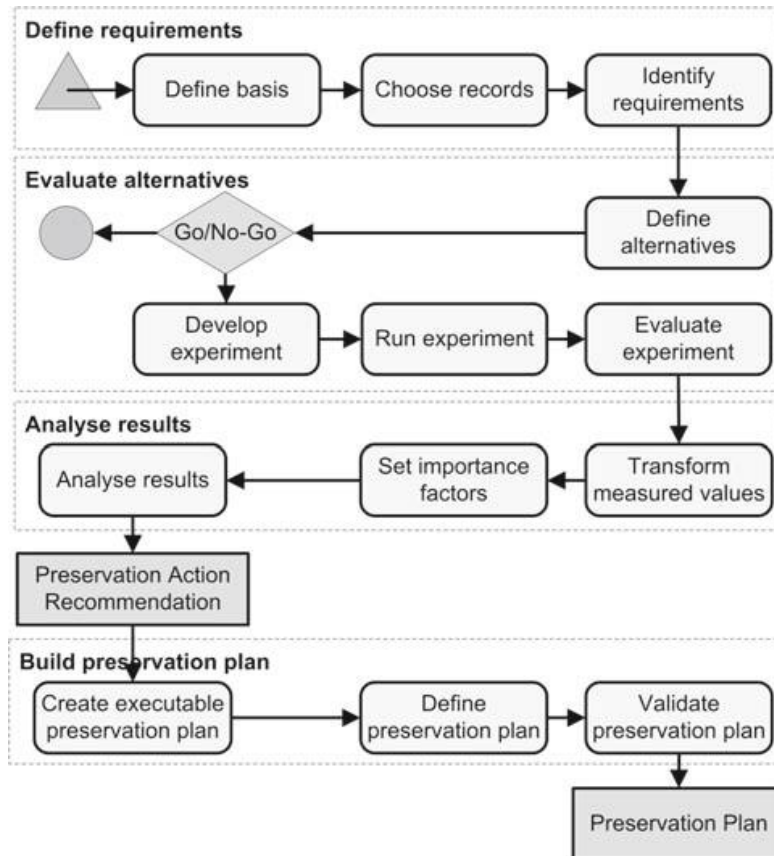


Figura 6 Workflow do planeamento da Preservação (Becker, 2009)

1. **Definir os requisitos** - esta é a primeira fase do *workflow* definido no projeto PLANETS. Começa por colecionar e documentar os fatores de influência e restrições sobre possíveis ações e procedimentos, então descreve o conjunto de objetos sob consideração e finalmente define o conjunto completo dos requisitos a ter em conta. Esta fase contempla três subfases, nomeadamente definição das bases; a escolha dos registos e identificação dos requisitos. (Becker, 2009)

Definição das bases: O primeiro passo do procedimento documenta os principais elementos subjacentes à atividade de planeamento. Recolhe e documenta os fatores de influência primária, restringindo o espaço de decisão e, assim, estabelece as bases para uma documentação completa e certifica-se de que todos os aspetos relevantes são estabelecidos e considerados. Experiência tem mostrado que uma definição abrangente de fatores de influência é um pré-requisito

importante para o planeamento de sucesso. A documentação de restrições que podem limitar a escolha de opções aplicáveis nesta fase simplifica e agiliza o processo de seleção e garante que o resultado é realmente em sintonia com as necessidades da instituição.

Isto pode acontecer de forma não estruturada, mas de preferência, esses fatores são capturados de forma mais formal, tornando mais fácil para derivar as decisões nas etapas do fluxo de trabalho respetivos.

Os exemplos incluem condições de definir formatos de ficheiro permitidos para ingerir, e políticas relacionadas com os direitos de propriedade intelectual e acesso legal aos regulamentos. Ainda mais importante, elementos de política pertencem às características da ação de preservação, serão dadas preferência a ações de preservação que são em código aberto, ou se apenas uma classe específica de ação de preservação pode ser aplicada, tais como emulação. Este último pode ocorrer em casos onde a instituição não tem o direito de autor e, assim, qualquer modificação dos objetos digitais está proibida.

Escolha dos registos: A segunda etapa na definição de requisitos é descrever o conjunto de objetos que forma o objetivo do plano atual e seleciona um subconjunto de objetos representativos para a experimentação, como exigido no tópico 4 do plano de conservação.

Uma descrição geral das características do conjunto de objetos, chamado coleção, inclui propriedades básicas tais como o tamanho da coleção, a classe de objetos e os formatos de objeto em que atualmente são representados. Enquanto isto pode ser feito de forma manual e descritiva, uma representação formal sendo o mais desejável. Coleção de ferramentas de criação de perfil pode fornecer descrições automatizadas das características técnicas dos objetos.

Características de interesse incluem não só objeto de formatos, tamanhos de arquivo e a sua variação dentro da coleção, mas também aspetos como uma avaliação dos riscos de cada tipo de objeto e de cada objeto, provocando assim um perfil de risco da coleção.

A fim de reduzir o esforço mínimo, esse subconjunto deve ser tão pequeno quanto possível. No entanto, os objetos de amostra são usados como um representante definido para testar os efeitos da aplicação de ações de preservação de todo o conjunto de objetos.

Identificação dos requisitos: Definição de requisitos é o coração do planeamento de preservação. É a base para as decisões a serem tomadas. Esta etapa inscreve-se a todos os requisitos para uma ótima solução para a preservação digital.

Esses requisitos são recolhidos da vasta gama de *stakeholders* e influenciam os fatores que devem ser considerados para um determinado ambiente institucional. Isto pode incluir a participação de curadores e especialistas de domínio, bem como os administradores e os consumidores. São especificados de forma quantificável, começando com objetivos de alto nível e quebrando-as em critérios mensuráveis, criando assim uma árvore de objetivos que constitui a base da avaliação de estratégias alternativas.

A definição de requisitos tem provado ser a fase mais crítica e complicada do processo de planeamento. Uma especificação incompleta leva a uma avaliação distorcida e conseqüentemente a más decisões.

Um passo essencial da definição de requisitos é a atribuição de efeitos mensuráveis para os critérios em cada nível da árvore de objetivos.

- 2. Avaliar alternativas:** Esta constitui-se como a segunda fase do planeamento de processo em que são avaliadas ações potenciais de forma quantitativa e aplicá-las ao conteúdo de amostra previamente definido e analisando os resultados em relação aos requisitos especificados na árvore de objetivos. Este procedimento de avaliação empírica resulta numa base de evidências que sustenta as decisões a adotar nas fases sucessivas. Esta fase pressupõe cinco subfases, nomeadamente, definição de alternativas; Go/no-go decision; desenvolvimento de experiências; execução da experiência; e avaliação da experiência. (Becker, 2009)

Definição de alternativas - O primeiro passo natural da avaliação é definir os possíveis fluxos de ações a serem tomadas em consideração. Podem ser aplicadas diferentes estratégias; para cada ação, são desejados uma especificação completa dos passos implicados e a configuração da ferramenta de *software* empregue. A descoberta de potenciais ações aplicáveis varia em complexidade, de acordo com o tipo de conteúdo. Muitas vezes, isso implica uma fase de extensa pesquisa, investigando quais ferramentas estão disponíveis para tratar o tipo de objetos. Registos mantendo ferramentas de ação de preservação podem ser consultados para referência e são potencialmente muito benéficos para apoiar a pesquisa. O resultado é uma lista de potenciais candidatos para a realização de ações de preservação, que serão avaliadas empiricamente durante os próximos passos. A

descrição de uma alternativa inclui o nome da ferramenta e versão usada, o sistema operacional em que ele será executado e as bibliotecas de especificação instalado como ambiente técnico e fontes.

Go/no - Go decision: Antes de continuar com o processo de experimentação, esta etapa reconsidera a situação atual e avalia se é viável e rentável para continuar o processo de planejamento. Em casos onde a avaliação é considerada inviável ou muito cara, uma redução das ferramentas pode ser necessária. A avaliação de algumas ferramentas também pode ser adiada devido à indisponibilidade ou questões de custo, ou por causa do desempenho ruim conhecido. Este é individualmente descrito e documentado.

Desenvolvimento de experiências: Esta etapa configura e documenta a configuração das ferramentas em que são realizadas as experiências e, assim, constrói a base para a execução da experiência na próxima etapa. Isso inclui procedimentos de instalação, a documentação do ambiente de *hardware* e *software* e etapas adicionais necessárias para realizar a avaliação de experimentações, tais como instalação de medição de tempo e facilidades de login.

Execução da experiência: nesta etapa, todas as ferramentas consideradas são aplicadas ao conjunto de objetos de amostra que foram definidas na primeira fase. Isto produz uma série de resultados de experiências que podem ser analisados e, em seguida, são armazenados como prova. No caso de conversão do objeto, isto significa que os documentos resultantes da experiência serão armazenados para consulta. Ao avaliar os emuladores, é necessária uma documentação detalhando a experiência de representação do objeto. Além disso, qualquer ocorrência de erros ou mensagens de log serão documentadas.

Avaliar a experiência: a avaliação das experiências baseia-se nos requisitos especificados na árvore de objetivos. São avaliados todos os critérios no nível da folha de uma árvore de objetivos, tendo em conta as provas empíricas, resultantes de experiências realizadas.

- 3. Análise de resultados** é a terceira parte do *workflow* em que os resultados são analisados, agregados e consolidados. Esta fase pressupõe três subfases

nomeadamente transformação dos valores medidos; definição dos fatores de importância; e a análise de resultados. (Becker, 2009)

Transformação dos valores medidos: o resultado da fase anterior é uma árvore de objetivos totalmente preenchida com valores de avaliação para todos os critérios considerados. Contudo as medições desta árvore são de diferentes escalas e, assim, não podem ser agregadas e comparadas diretamente. Assim, a transformação das regras são definidas, as quais resultam num mapeamento de todas as escalas de medida possível para algo uniforme.

Definição dos fatores de importância: Esta etapa leva em conta o fato de que nem todos os requisitos são de igual importância e atribui fatores de peso para os nós na árvore de objetivos. Houve uma discussão considerável sobre a questão da importância de ponderação nos métodos de seleção. Vários métodos usando métodos de Pontuação ponderada ganhou críticas pelo fato de que as configurações de peso precisam ser inicialmente especificados em uma situação onde pouco ou nada é conhecido sobre o desempenho real e diferenças dos componentes do candidato. Além disso, a redução a um único número e o ranking correspondente é considerada demasiado simplista por muitos.

Na abordagem apresentada, a importância e os fatores relativos são balanceados em cada nível da árvore de objetivos, num tempo em que os valores de avaliação para todos os candidatos já são conhecidos.

Isso desvia o fluxo de trabalho padrão do utilitário de análise, mas provou-se mais útil no cenário de seleção de componente, representado pela preservação de planejamento em numerosos estudos de caso.

Analisar resultados: é a etapa final da fase de avaliação que considera a completa base de evidência de informações produzidas durante as fases anteriores do fluxo de trabalho. Analisa o desempenho dos componentes do candidato na avaliação da experimentação para chegar a uma conclusão e recomendar a melhor ferramenta a ser empregue e a correspondente configuração.

Todas as medidas que foram descritas acima são transformadas e multiplicadas com os pesos dos requisitos correspondentes.

Isso resulta numa avaliação da árvore de objetivos onde os critérios de folha foram preenchidos. Agregar esses valores leva a um valor de desempenho alternativo de

cada ação em todos os níveis da hierarquia de árvore, que é diretamente comparável.

4. **Criação do plano de preservação** é a quarta e final fase de planeamento, baseada na decisão para uma ação de preservação. Na terminologia OAIS isso corresponde à funcionalidade de *Develop Packaging Designs* e *Migration Plans*. Especifica uma série de medidas concretas ou ações, juntamente com responsabilidades organizacionais, regras e condições para executar a ação de preservação na coleção. Esta fase pressupõe três subfases nomeadamente a criação do plano de preservação que vai ser executado; definição do plano de preservação; e a validação do plano. (Becker, 2009)

Criação do plano de preservação: Esta etapa do fluxo de trabalho define os gatilhos para a execução e as condições sob as quais a ação de preservação será realizada. Requisitos de *hardware* de *software*, bem como as dependências em outros sistemas são documentadas a fim de permitir a execução da ação de preservação, configurações da ferramenta e detalhes sobre a localização da coleção na qual a execução da ação são definidos, resultando assim num plano de ação de preservação. Para realizar a garantia da qualidade das ações executadas, pode ser selecionado um subconjunto dos critérios utilizados para avaliar as soluções. Estes devem ser avaliados automaticamente durante a execução do plano de ação para validar que os limiares definidos nesses critérios foram atendidos. A documentação necessária que tem de ser guardada/gravada ao executar a ação também é definida nesta etapa.

Definição do plano de preservação: Enquanto muitas partes do *workflow* do planeamento de preservação trata dos aspetos técnicos do plano de preservação, esta etapa define procedimentos organizacionais e responsabilidades.

Os fatores de custo influenciam a decisão sobre uma alternativa específica. Nesta etapa, é realizado um cálculo mais detalhado dos custos usando um modelo de custo aprovado.

A atribuição de responsabilidades também está documentada nesta etapa. O acompanhamento do processo de aplicação das ações de preservação tem de ser feito por um papel diferente do que executar o plano de preservação. Também tem que ser monitorizada se ocorrer um evento que se torna necessário reavaliar o plano. As possíveis ações para esta etapa é uma revisão periódica programada,

mudanças no ambiente, tais como novas ferramentas disponíveis que foram detetadas através de vigilância tecnológica, objetivos alterados (tais como requisitos de comunidade de destino alterado) ou um perfil de coleção alterado, quando os objetos considerados mostram novas características divergentes do perfil especificado anteriormente.

Validação do Plano de preservação: Nesta fase final, toda a documentação sobre o plano de preservação e as decisões tomadas durante o processo de planeamento são revistos. Podem ser efetuados ensaios sobre um alargado conjunto de objetos de exemplo nesta etapa para verificar a validade do plano de preservação.

Finalmente, o plano validado tem que ser aprovado pela pessoa responsável. Depois de aprovado o plano, não deve ser feita nenhuma alteração sem se rever formalmente todo o plano.

5.3.3 Ferramentas para o planeamento da preservação

Estas ferramentas de apoio ao planeamento da preservação são uma ajuda fundamental para garantir a autenticidade e confiabilidade de um repositório digital.

São diversas e em constante desenvolvimento oferecendo cada uma destas ferramentas soluções para problemas que aparecem ou podem aparecer quando se cria um repositório.

O planeamento é uma questão complexa e há que pensar atempadamente sobre como se quer apresentar o repositório, definir o tipo de documentos a incorporar e que tipo de acessos se quer oferecer aos utilizadores. Além disso o planeamento da preservação é algo contínuo e sistemático num processo de tomada de decisão.

Assim, e direcionada ao apoio do planeamento da preservação, e com vista à criação de um repositório digital seguro, uma das ferramentas de referência é o *Plato*.

Trata-se de uma ferramenta Web de código aberto que suporta e automatiza o processo de especificação de requisitos, avaliando as possíveis soluções e constrói um plano para a preservação de um determinado conjunto de objetos digitais. Esta ferramenta implementa a metodologia de planeamento de preservação *PLANETS* e integra os registos e serviços para ações de preservação e caracterização.

A ferramenta baseia-se num trabalho anterior realizado pelo *DELOS Digital Preservation Cluster* e nos resultados da avaliação do desempenho de várias

soluções, face a requisitos e objetivos bem definidos. A metodologia pode ser aplicada a qualquer tipo de estratégia - migração, emulação, normalização, etc. - e foi validada numa série de estudos de caso (Strodl & Becker, 2007).

No que se refere aos serviços de planeamento e ações de preservação a solução de código aberto *SCAPE* mostra ser a melhor opção. O *SCAPE* desenvolveu uma infraestrutura e ferramentas para ações de preservação escaláveis, desde um quadro de fluxos de trabalho automatizados, de preservação de qualidade garantida, e integrando esses componentes com um planeamento de preservação com base em políticas e sistema de relógio.

Estes resultados do projeto foram validados no prazo de quatro *Testbeds* numa grande escala de diversas áreas de aplicação. O *SCAPE* teve um impacto significativo sobre a comunidade e a prática da preservação digital através de melhorias de escalabilidade nos instrumentos já existentes, por exemplo, Platão, e Fedora 4; novas ferramentas escaláveis como *Nanite*, *Hawarp* e *C3PO*; novas ferramentas de controlo de qualidade, como *Jpylyzer*, *Pagelyzer*, *XcorrSound* e *Matchbox*; APIs para um repositório de interoperabilidade; dezenas de *workflows* e fluxos de trabalho baseados em *Hadoop*; documentos de boas práticas; e um alto grau de aceitação dos resultados do projeto em instituições parceiras.

Nas ferramentas de Gestão de Processos e Fluxos é de referenciar o projeto *E-ARK*, que baseado na cooperação com fornecedores de sistemas comerciais, pretende criar uma metodologia pan-europeia para arquivo de documentos eletrónicos, sintetizando as melhores práticas nacionais e internacionais existentes para a manutenção de registos e bases de dados autênticos e utilizáveis ao longo do tempo. A metodologia será implementada num sistema aberto em vários contextos nacionais, usando ferramentas existentes, próximo do mercado, e serviços desenvolvidos pelos parceiros. Isso vai permitir que as instituições de memória e os seus clientes (público e do setor privado) possam avaliar, num contexto operacional, a adequação dessas tecnologias *state-of-the-art*.

O objetivo desta ferramenta é proporcionar uma abordagem única, escalável e robusta capaz de atender às necessidades das diversas organizações, públicas e privadas, grandes e pequenas, e capazes de suportar tipos de dados complexos. O *E-ARK* visa demonstrar os potenciais benefícios para as administrações públicas, órgãos públicos, serviços públicos, os cidadãos e as empresas, proporcionando um acesso simples e eficiente para os fluxos de trabalho para as três principais atividades de um arquivo - adquirir, preservar e possibilitar a reutilização da informação.

As práticas desenvolvidas no âmbito do projeto irão reduzir o risco de perda de informação devido a abordagens inadequadas para conservação e arquivo dos registos. É um projeto voltado para o público, oferecendo um serviço de arquivo completamente operacional de acesso à informação para os seus utilizadores. Os resultados do projeto serão genéricos e escaláveis, a fim de construir uma infraestrutura de arquivo em toda a UE e em ambientes em que os diferentes sistemas jurídicos e tradições de gestão de arquivo são aplicáveis.

Além disso, o parceiro do projeto, *The Preservation Coalition Digital* irá promover as melhores práticas nesta área, assim como outros parceiros de instituições governamentais.

Por fim, será também de acompanhar o Projeto *APARSEN*.

Sabe-se que a preservação em meio digital oferece benefícios económicos e sociais associados à preservação a longo prazo da informação, conhecimento e *know-how* a reutilizar pela mesma ou pelas gerações seguintes. No entanto, e apesar do percurso dos últimos 10 anos, existe um grande problema, ou seja, as estruturas de apoio à preservação encontram-se sustentadas em projetos que são de curta duração e são fragmentadas.

O projeto *APARSEN*²⁹ surge em 2011 ligado à Aliança para o Acesso Permanente (APA) um consórcio que envolve os principais intervenientes europeus na temática da preservação em meio digital que visa criar uma visão compartilhada e uma estrutura de suporte à criação de uma infraestrutura de informação digital sustentável e que proporcione o acesso permanente a informação codificada digitalmente.

Este projeto pretende alargar-se a outros especialistas em preservação em meio digital, incluindo investigadores e indústria, bem como investigadores de outras organizações intereuropeias, no sentido da articulação e integração de programas de preservação em meio digital num programa comum de trabalho, criando assim, um centro virtual de investigação no domínio da preservação em meio digital na Europa.

O projeto pretende abarcar estratégias e metodologias técnicas para a preservação, acesso e reutilização de coleções de dados ao longo de todo o ciclo de vida, sendo este aspeto considerado o mais importante; questões jurídicas e económicas, incluindo custos e questões de governança, bem como de direitos digitais dentro e fora do consórcio para ajudar a criar uma disciplina do que designam por “curadores de dados” com qualificações adequadas.

²⁹SBA RESEARCH. Competence Centers for Excellent Technologies. *APARSEN - Alliance Permanent Access to the Records of Science in Europe Network: a project within the Digital Preservation area*. Consultado em Outubro 25, 2014 em <https://www.sba-research.org/research/projects/aparsen/>

Conclusões e perspectivas futuras

Com o mundo das tecnologias em constante mudança, os ciclos de rápida obsolescência e a grande dependência das organizações face à informação que possuem em meio digital, é necessário que estas pensem na segurança e preservação da sua informação no longo prazo.

Também o aumento do fluxo informacional em formato digital e a necessidade de recuperar essa informação fez com que se criassem mecanismos de armazenamento e recuperação da informação que garantam a sua segurança, acessibilidade e comunicabilidade.

Sendo a Multicert um provedor de serviços de certificação eletrônica, tem uma grande preocupação com a segurança da informação e pretende que esta se mantenha autêntica, íntegra, fidedigna, acessível e inteligível no longo prazo. A estruturação de um repositório confiável/seguro constitui um passo decisivo para a concretização deste objetivo, potenciando a informação como memória, ativo operacional e estratégico, evidência da qualidade do serviço e oportunidade de inovação organizacional. Um repositório digital confiável é, pois, um repositório digital que é capaz de manter autêntica a informação, de preservá-la e prover o acesso à mesma pelo tempo necessário.

O principal objetivo desta dissertação visou contribuir para a estruturação do repositório digital da Multicert desenvolvendo um detalhado diagnóstico organizacional e informacional e consequente elaboração de um *Documento de Especificação de Requisitos*.

O uso da norma 16363:2012 fez com que se percebesse quais os requisitos essenciais para tornar o Repositório Digital Seguro. Esta norma constitui-se como uma *checklist* onde são apresentados os requisitos e se analisa a sua conformidade com o Repositório. Apresenta como objetivo essencial fornecer uma lista de requisitos a partir da qual se possam realizar auditorias aos repositórios no sentido do controlo de ameaças e riscos à sua segurança com base em 109 critérios.

Conforme foi analisado, o Alfresco não obedece a vários requisitos da norma, nomeadamente na parte da Gestão dos Objetos Digitais. É necessário que se realizem frequentemente testes de conformidade (testes de certificação) ao Alfresco para se ir verificando a sua adequação aos requisitos. Por isso, é também necessário que se criem os documentos de suporte à especificação para que sejam criadas as evidências de conformidade com os requisitos da norma.

Após a elaboração deste estudo e da consequente criação do documento de especificação de requisitos, tornou-se claro que a Multicert ainda tem algum caminho a percorrer para que possa Certificar o Repositório. O primeiro passo foi dado com esta dissertação pois fez-se o diagnóstico necessário para perceber como as coisas estão a ser feitas atualmente. Os dois estudos iniciais da maturidade da Gestão da Informação e do ECM tornaram-se vitais para se ter a real noção da gestão que é feita a nível dos processos documentais. No primeiro estudo, percebeu-se que a Multicert está empenhada em manter a informação atualizada e disponível para quem dela necessita, neste caso os seus Colaboradores. No segundo estudo verificou-se que tem havido um esforço por parte da Multicert controlar a sua produção informacional e que as noções de gestão do ciclo de vida da informação começam a ser incorporados na Organização.

Também a elaboração da estrutura documental de suporte é fundamental para o processo de Certificação do Repositório pois assim já se sabe que caminho se pretende seguir. Na Multicert já existem documentos que obedecem a diretrizes referenciadas na Política de Preservação e na Estratégia de Preservação, nomeadamente o Processo de Controlo de Acesso; Processo de Continuidade de Negócio; Manual de Funções; Processo de acesso a Visitantes, entre outros. O que se pretende com a elaboração da estrutura documental de suporte é complementar o que já existe e promover a criação do Repositório Digital Seguro.

Quando se fala em Repositório Digital Seguro, tem que se falar obrigatoriamente em Preservação da Informação em meio Digital e em estratégias que devem ser associadas ao Repositório para promover essa preservação.

Seja qual for a plataforma de suporte ou as estratégias de preservação adotadas, um Repositório deve corresponder às expectativas criadas pelos seus utilizadores. Afirmar que se é capaz de garantir o acesso continuado à informação digital não é suficiente para estabelecer um clima de confiança junto dos vários intervenientes que interagem com o repositório, como os prosumidores, administradores do sistema e a administração da empresa.

É necessário adotar estratégias de preservação que passam desde logo pela criação de meta-informação (dimensão essencial), pois os documentos digitais podem sofrer com a instabilidade dos formatos (dimensão lógica e dimensão conceptual), do meio e suporte material (dimensão lógica e física), por exemplo em termos de condições de armazenamento e refrescamento de suportes, requerendo não uma mas várias estratégias.

É necessário, igualmente, que se pense numa estratégia de preservação que tenha em conta vários fatores como a qualidade e tipo de objetos digitais, a relação custo/benefício, o ambiente computacional e as aplicações utilizadas. A obsolescência tecnológica é um fator a ter em conta, pois, com as constantes mudanças, a informação se não estiver num formato adequado pode perder-se para sempre. Estas estratégias podem ser usadas simultaneamente, mas requerem um esforço por parte de todos os envolvidos na preservação digital, pois não são feitas automaticamente requerendo uma análise prévia e um planeamento que adequa o plano de ação às necessidades da Multicert.

São diversas as variáveis que influenciam a segurança e a preservação da informação em todo o seu ciclo de vida. A durabilidade e confiabilidade dos suportes utilizados (CDs e DVDs) e a estabilidade ao nível da temperatura e humidade relativa são tão importantes quanto a inteligibilidade, autenticidade e integridade da informação neles registada. Também a definição de uma política de preservação, a tomada de decisão sobre a normalização dos formatos, a criação de procedimentos e processos de submissão/ingestão que preveem a criação de pacotes de informação que incluam a meta-informação necessária para a descrição, acesso, gestão e preservação dos documentos no repositório são ações importantes para o processo de preservação da informação e para a segurança e confiabilidade do repositório. Essas ações passam por passos tão simples como a decisão da adoção do formato PDF/A na empresa integrado numa política que prevê a estratégia de normalização de formatos.

É necessário aplicar estratégias e desenvolver ações que valorizam o contexto, focam cada vez mais o conteúdo, a par da forma, e não atendem apenas ao suporte físico/material em que a informação foi registada.

Numa visão sistémica a estratégia global sugerida foi a de criar um Repositório Digital Seguro que, com outras estratégias, seja capaz de garantir o controlo dos processos de criação, ingestão, armazenamento, gestão, preservação e disseminação dos registos digitais à comunidade de prosumidores que serve.

Esta visão alinha com o planeamento global da GI na Multicert e esta pelas opções estratégicas e operacionalização do seu negócio. À empresa e aos seus Colaboradores são exigidos um esforço contínuo que, para além da certificação do repositório pode chegar à certificação do próprio sistema de gestão da informação, o SGIAP, no qual o repositório e aplicações como as de GDE ou ECM são alguns dos componentes.

Elaborar o Plano de Preservação e identificar, seleccionar e especificar os requisitos exigidos aos produtos e serviços de certificação eletrónica com vista à

integração num repositório digital (do fornecedor ou do cliente) são os desafios que se seguem e que poderão abrir portas para novas áreas de negócio para a própria empresa.³⁹

³⁹ Esta dissertação originou ainda um artigo que foi aceite no 12º Congresso BAD que terá lugar nos dias 21 a 23 de Outubro de 2015 em Évora, cujo título é: “O repositório digital seguro: diagnóstico e especificação”

Referências Bibliográficas

Alfresco (2012). Alfresco Software, Inc. Consultado em Março de 2015 em <http://www.alfresco.com>

Almeida, V. (2004) Contratos Eletrônicos. São Paulo: Centro Universitário das Faculdades Metropolitanas Unidas - UniFMU. Monografia de graduação em direito. Consultado em Maio 23, 2015 em <http://arquivo.fmu.br/prodisc/direito/vida.pdf>

Aretio, L. G. (2005) - *Objetos de aprendizagem. Características y repositorios*. Editorial del BENED Consultado em Novembro 9, 2014 em <http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:327&dsID=editabril2005.pdf>

ARQUIVO NACIONAL DO BRASIL (2005). Dicionário brasileiro de terminologia arquivística. Publicações técnicas: Rio de Janeiro. 232p. ISBN: 85-7009-075-7. Consultado em Dezembro 8, 2014 em <http://www.arquivonacional.gov.br/Media/Dicion%20Term%20Arquiv.pdf>

Barbedo, F. (2010) Recomendações para a produção de Planos de Preservação Digital. Consultado em Outubro, 26 2014, em http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf

Becker, C. Brown, A., Kulovits, H. (2008) - Report on service integration in Plato 2. Consultado em Janeiro 11, 2015, em http://www.planets-project.eu/docs/reports/Planets_PP4-D3_ReportonServiceIntegrationInPlato-final.pdf

Becker, C.; et.al (2009) Systematic planning for digital preservation: evaluating potential strategies and building preservation plans. Springer: Verlag. Consultado em Janeiro 9, 2015 em <http://www.ifs.tuwien.ac.at/~becker/pubs/becker-ijdl2009.pdf>

Becker, C;et.al (2007) Long-term preservation of electronic theses and dissertations: a case study in preservation planning. In: Proceedings of the 9th Russian Conference on Digital Libraries. Consultado em Janeiro 12, 2015 em http://www.ifs.tuwien.ac.at/~becker/pubs/becker_rcdl07.pdf

Câmara Municipal de Alijó. Gerar documentos PDF/A utilizando o PDFCreator. Município de Alijó. Consultado em Junho 13, 2014, em http://www.cm-alijo.pt/uploads/assets/Autarquia/Divisao_Obras_Urbanismo/SIRJUE/Gerar_Documentos_PDF-A_com_PDFCreator.pdf

Carvalho, J. et.al (2014) Auditoria ISO 16363 a Repositórios Institucionais. Cadernos BAD, nº2, Julho-Dezembro. Consultado em Maio 15, 2015 em <http://www.bad.pt/publicacoes/index.php/cadernos/article/view/1175/pdf>

CENTER OF RESEARCH LIBRARIES (2010). Global Resources Network. Portico Audit Report 2010. Consultado em Mar 03, 2015 em <http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories/portico>

CENTER OF RESEARCH LIBRARIES (2011). Global Resources Network. HathiTrust Audit Report 2011. Consultado em Mar 03, 2015 em <http://www.crl.edu/reports/hathitrust-audit-report-2011>

CENTER OF RESEARCH LIBRARIES (2012). Global Resources Network. Chronopolis Audit Report 2012. Consultado em Mar 03, 2015 em <http://www.crl.edu/reports/chronopolis-audit-report-2012>

CENTER FOR RESEARCH LIBRARIES (2014). Global Resources Network. Certification report on CLOCKS. Consultado em Mar 20, 2015 em http://www.crl.edu/sites/default/files/reports/CLOCKSS_Report_2014.pdf

CENTRO DE GESTÃO DA REDE INFORMÁTICA DO GOVERNO (2006). Certificação Eletrónica. Sistema de Certificação Electrónica do Estado e Segurança Electrónica. Consultado em Abr 23, 2015 em <http://www.ceger.gov.pt/certificacao-eletronica.aspx>

CONARQ (2014). Conselho Nacional de Arquivos. Diretrizes para a Implementação de Repositórios Digitais Confiáveis de Documentos Arquivísticos. Consultado em Mar 15, 2015 em <http://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>

Consultative Committee for Space Data Systems (CCSDS) (2012) Reference model for an Open Archival Information System (OAIS). Magenta Book. Consultado em Novembro 23 2014 em <http://public.ccsds.org/publications/archive/650x0m2.pdf>

Correia, M. (2003) Assinatura eletrónica e certificação digital. Lisboa: Universidade Lusíada. Consultado em Fevereiro 12, 2015 em: http://www.apdi.pt/pdf/Assinatura_elect.pdf

DATA ARCHIVING AND NETWORKED SERVICES. Data Seal of Approval. Consultado em Mar 20. 2015 em <http://www.datasealofapproval.org/en/>

Decreto-Lei nº 62/2003, de 3 de Abril. Diário da Republica nº 79 - série I-A. Regime Jurídico da Assinatura Digital estabelecido no Decreto-Lei nº 290-D/99, de 2 de Agosto. Lisboa

Decreto-Lei n.º 88/2009, de 9 de Abril. Diário da Republica n.º 70 - série I. Regime Jurídico dos Documentos Eletrónicos e da Assinatura Digital, e Sistema de Certificação Eletrónica do Estado. Lisboa

Decreto-Lei 290-D/99, de 2 de Agosto. Diário da Republica nº 178 - serie I-A. Regime Jurídico aplicável aos Documentos Eletrónicos e Assinatura Digital. Lisboa

DICIONARIO PRIBERAM DA LINGUA PORTUGUESA (2013). Priberam dicionário. *Informação*. Consultado em Dezembro 8, 2013, em <http://www.priberam.pt/DLPO/>

DIGITALSIGN (2015). Certificadora Digital. Institucional. Consultado em Abr 23, 2015 em <https://www.digitalsign.pt/>

DIGITAL PRESERVATION COALITION (2008) Preservation Management of Digital Materials: The Handbook. Consultado em Novembro 7, 2014, em <http://www.dpconline.org/advice/preservationhandbook>

DIGITAL CURATION CENTRE E DIGITAL PRESERVATION EUROPE (2007) Digital Repository Audit Method Based on Risk Assessment (DRAMBORA). Consultado em 4 Janeiro, 4 2015, em <http://www.repositoryaudit.eu>

Direção Geral de Arquivos - Apoio a elaboração de plano de preservação digital. Consultado em Outubro 23, 2014 em <http://dgarq.gov.pt/servicos/consultorias/preservacao-digital/>

DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2000) Community framework for electronic signatures. Official Journal of European Communities. Consultado em Março 22, 2015 em: http://www.icts.org/Working_Groups/EESSI/Documents/e-sign-directive.pdf

DLM Forum (2013) Information Governance across Europe: MoReq - Modular Requirements for Records Systems. Consultado em Novembro 3, 2014, em <http://www.dlmforum.eu/moreq/4577372922>

Fanning, B. (2010) PDF/ARCHIVE: preserving electronic assets. Washington, DC : NACRC. ALLM Consultado em Maio 5, 2015, em: http://www.nacrc.org/assets/Presentations/LC/2010/pdfa_preserving_electronic_assets.pdf

Ferreira, M. (2006) Introdução à Preservação Digital: Conceitos, estratégias e actuais consensos. Guimarães: Escola de Engenharia da Universidade do Minho. ISBN 972-8692-30-7. Consultado em Outubro, 23 2014 em <http://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf>

Gaspar, J. (2012) Análise de Problemas em Especificações de Requisitos de Referência. Dissertação de Mestrado em Engenharia de Informática e de Computadores. Instituto Superior Técnico. Lisboa. Consultado em Fevereiro 27, 2015 em <https://fenix.tecnico.ulisboa.pt/downloadFile/395144231121/JGaspar%20-%20An%C3%A1lise%20de%20Problemas%20em%20Especificac%C3%A7%C3%B5es%20de%20Requisitos%20de%20Referencia.pdf>

Henriksen, S. L.; Seuskens, W.; Wijers, G. (2013) Best practices for a digital storage infrastructure for the long-term preservation of digital files. Digitising Contemporary Art. Consultado em Novembro 3, 2014, em http://www.dca-project.eu/images/uploads/banners/DCA_D62_Best_practices_for_a_digital_storage_infrastructure_20130506_Version1.pdf

Hofman, H. (2001) How to keep digital records understandable and usable through time? Consultado em Outubro 16, 2014 em http://www.interpares.org/display_file.cfm?doc=ip1_dissemination_cp_hofman_ltp_r_2001.pdf

INTERNATIONAL COUNCIL OF SCIENCE. World Data System (WDS). Consultado em Mar 20. 2015 em: <http://www.icsu.org/what-we-do/interdisciplinary-bodies/wds/?icsudocid=about>

ISO 14721:2003 - Space data and information transfer systems. Open archival information system (OAIS). Reference model

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

ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements. Geneva, Switzerland: ISO/IEC, 2005

ISO/IEC 27002:2005. Information technology - Security techniques: Code of practice for information security management. Geneva, Switzerland: ISO/IEC, 2005

ISO/IEC 27003:2010. Information technology - Security techniques - Information security management system implementation guidance. Geneva, Switzerland: ISO/IEC, 2010

ISO 30300:2011. Information and documentation - Management systems for records - Fundamentals and vocabular. Geneva, Switzerland: ISO, 2011

ISO 30301:2011. Information and documentation - Management systems for records - Requirements. Geneva, Switzerland: ISO, 2011

ISO TC 46/SC 11 (2010) Digital Records Preservation: Where to Start Guide. Consultado em Novembro 3, 2014, em http://www.niso.org/apps/group_public/download.php/7273/Digital%20records%20reservation%20-%20Where%20to%20start%20guide%20-%20EN.pdf

ISO/TR 18492:2005. Long-term preservation of electronic document-based information. Geneva, Switzerland: ISO/TR, 2005

JISC INFONET (2014). Infokits. *Repositórios*. Consultado em Abril 21. 2015 em <http://www.jiscinfonet.ac.uk/infokits/repositories>

Keefer, A.; Gallart, N. (2007) La preservación de recursos digitales: El retro para las bibliotecas del siglo XXI. Barcelona: Book Print Digital, S.A., ISBN 978-84-9788-567-6

Lopes, L. (2004) Um Modelo de Processo de Engenharia de Requisitos para Ambientes de Desenvolvimento Distribuído de Software. Dissertação (Mestrado) - Fac. de Informática, PUCRS. Porto Alegre. Consultado em Fevereiro 17, 2015 em <https://www.inf.pucrs.br/munddos/docs/DisseLTLopes.pdf>

LURATECH (1995a). Document Processing Solutions. *Overview*. Consultado em Mai 20, 2015 em <https://www.luratech.com/en/products/luratech-pdf-compressor-enterprise/>

LURATECH (1995b). Document Processing Solutions. *Advantages*. Consultado em Mai 20, 2015 em <https://www.luratech.com/en/products/luratech-pdf-compressor-enterprise/>

Martins, A.; Rodrigues, E.; Nunes, M. B. Repositórios de informação e ambientes de aprendizagem: Criação de espaços virtuais para a promoção da literacia e da responsabilidade social. Nº 3 Consultado em Novembro, 5, 2014 em <http://www.rbe.min-edu.pt/news/newsletter3/repositorios.pdf>

Masson, S. M. (2008) Os Repositórios digitais no âmbito da Sociedade Informacional. Prisma.com Nº 7 Consultado em Novembro 15, 2014 em http://prisma.cetac.up.pt/105_Repositorios_digitais_no_ambito_da_Sociedade_Informacional_Silvia_Masson.pdf

MULTICERT (2008) Manual Alfresco

MULTICERT (2009) Política do ambiente de informação

MULTICERT (2010a) Empresa

MULTICERT (2010b) Projetos

MULTICERT (2011) Política de gestão da segurança da informação

MULTICERT (2012) Política de gestão da informação

MULTICERT (2014a) Manual da qualidade

MULTICERT (2014b) Declaração de práticas de certificação

MULTICERT (2014c) Certificação Digital

MULTICERT (2015) Política de desenvolvimento de *software* da Multicert

Nath, M. Arora, A (2010) Content Management System : Comparative Case Study. 978-1-4244-6055-7. Consultado em Maio, 15 2015 em <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5552271>

NP ISO 31000:2012. Gestão do Risco: princípios e linhas de orientação. Caparica, Portugal: Instituto Português da Qualidade

O'brian, R.(1998) An Overview of the Methodological Approach of Action Research. Faculty of Information Studies, University of Toronto

Oliveira, H. (2014) A Preservação da informação: um contributo para a implementação de um arquivo digital certificável no Município do Porto. Porto: Faculdade de Engenharia da Universidade do Porto, 2014. Dissertação de Mestrado em Ciência da Informação. Orientadora: Maria Fernanda Martins; coorientadora: Maria Manuela Pinto.

Oliveira, H; Pinto, M (2014) A gestão da produção informacional: o formato PDF e a comunicação via email. Páginas a&b: arquivos e bibliotecas, nº2. Lisboa.ISSN 0873-5670. S. 3 Consultado em Junho 20, 2015, em http://sigarra.up.pt/flup/en/pubs_pesquisa.FormView?P_ID=104685

Pelz-Sharpe, A. et al. (2009). ECM3: Ecm Maturity Model. V. 1.0. Consultado em Mar 03, 2015 em https://ecmmaturity.files.wordpress.com/2009/02/ec3m-v01_0.pdf>

Pinheiro, O. (2003) Sistema de Apoio à Decisão no Planeamento da Produção de Produtos Complexos: Identificação e Especificação de Requisitos. Porto: Faculdade de Engenharia da Universidade do Porto, Dissertação de Mestrado.

Pinto, M. M. (2005) Uma era, uma visão, um paradigma: da teoria à prática. Revista da Faculdade de Letras: Ciências e técnicas do património. Porto. I Série, vol. 4, pp. 101-123. ISSN: 1645- 4936

Pinto, M. M. (2007a) Da ação à informação: o desafio digital. Congresso Nacional de Bibliotecários Arquivistas e Documentalistas, 9, Ponta Delgada. Bibliotecas e Arquivos: Informação para a cidadania, o desenvolvimento e a inovação: atas. Lisboa: BAD. Consultado em Outubro 29, 2014, em <http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/560/370>

Pinto, M. (2009) PRESERVMAP : Um roteiro da preservação na Era Digital. Porto: Edições Afrontamento; CETAC.Media (Coleção CAI; 7). ISBN 978-972-36-1070-3. 2009

Pinto, M. M. (2013) Gestão de Documentos e meio digital: um posicionamento urgente e estratégico. 3º Seminário de Estudos da Informação. Gestão do Conhecimento, Gestão da Informação e Gestão de Documentos em Contextos informacionais. Rio de Janeiro: Universidade Federal Fluminense

Pinto, M. M.; Silva, A. M. (2005) - Um modelo sistémico e integral de gestão da informação nas organizações. In CONTECSI - CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 2º, São Paulo, 2005 - Actas do congresso. [CD-ROM]. São Paulo: TECSI-FEA-USP, 2005. Consultado em Novembro 3, 2014, em em: <http://ler.letras.up.pt/uploads/ficheiros/3085.pdf>

Pinto, M. M. (2007a) Da acção à informação: o desafio digital. *Congresso Nacional de Bibliotecários Arquivistas e Documentalistas, 9, Ponta Delgada*. Bibliotecas e Arquivos: Informação para a cidadania, o desenvolvimento e a inovação: atas. Lisboa: BAD. Consultado em Novembro 23, 2014, em <http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/560/370>

Potts, J. (2008) Alfresco developer guide: From technologies to solutions. Birmingham: Packt Publishing. ISBN 978-1-847193-11-7

Proença, A.; Lopes, S. - Digital Preservation. Consultado em Outubro 27, 2014 em http://www.di.ubi.pt/~api/digital_preservation.pdf

PUBLIC RECORD OFFICE VITORIA (2014) Information Management Maturity Measurement Tool - IM3 Consultado em Janeiro 30, 2014 em <http://prov.vic.gov.au/government/information-management/information-management-maturity-measurement-tool-im3>

Resende, D.(2009) Certificação Digital. Revista Juridica UNIGRAM, V.11, nº22 Consultado em Fevereiro 16, 2015, em http://www.unigran.br/revista_juridica/ed_anteriores/22/artigos/artigo09.pdf

RLG, NARA, & OCLC. (2007) Trustworthy repositories audit & certification: Criteria & Checklist. Consultado em Novembro 23, 2014, em http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

RLG, OCLC (2002) Trusted Digital Repositories: Attributes and Responsibilities. Consultado em Novembro 23, 2014, em <http://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf?urlm=161690>

Rouse, M.(2013) Enterprise Content Management (ECM). Consultado em Março 15, 2015 em <<http://searchwindowsserver.techtarget.com/definition/enterprise-content-management-ECM>>

Saramago, M. L.(2002) Preservação Digital a longo prazo: Boas práticas e estratégias. Cadernos de Biblioteconomia Arquivística e Documentação Cadernos BAD. Nº002, p.54-68. Consultado em Novembro 26, 2014 em <<http://redalyc.uaemex.mx/redalyc/html/385/38505106/38505106.html>>.ISSN0007-9421

Sargento, C. (2012) Stork 2.0 facilita identificação digital na Europa. Semana Informática. Consultado em Fevereiro 10, 2015 em:

<http://www.semanainformatica.xl.pt/administracao-publica/administracao-publica/stork-2-0-facilita-identificacao-digital-na-europa>

SBA RESEARCH. Competence Centers for Excellent Technologies. APARSEN - Alliance Permanent Access to the Records of Science in Europe Network: a project within the Digital Preservation área. Consultado em Outubro 25, 2014 em <https://www.sba-research.org/research/projects/aparsen/>

SECRETARIA-GERAL. Ministério das Finanças. O PDF/A-1 como meio de preservação de documentos eletrónicos a longo prazo. Consultado em Junho 12, 2015, em http://www.sgmf.pt/_zdata/PDF/ARQ/ESTUDOS/ARQ_EST_PFD.pdf

Sharpe, A. et.al. (2010) ECM3: ECM Maturity Model. Versão 2.0. Consultado em Maio 13, 2015, em http://www.fredonia.edu/pr/web/pdf/ECM3-Maturity_model_v2_0.pdf

Silva, A. M. (2006) A Informação: da compreensão do fenómeno e construção do objecto científico. Porto: Edições Afrontamento, ISBN 972-36- 0859-6

Silva, A. M. da (2009) Arquivologia e Gestão da Informação/Conhecimento. In Informação & Sociedade: Estudos, Vol. 19, Nº 2, Maio/Agosto 2009. ISSN: 0104- 0146. Consultado em Novembro 13, 2014 em <http://periodicos.ufpb.br/ojs2/index.php/ies/article/view/3712/3024>

Silva, et. al, (1998) Arquivística: teoria e prática de uma ciência da informação. Vol 1. Porto: Edições Afrontamento. ISBN 972-36-0483

Skinner, K., Schultz, M. (2010) A Guide to Distributed Digital Preservation. Atlanta: Educopia Institute. ISBN: 978-0-9826653-0-5. Consultado em Novembro 3, 2014, em http://open.bu.edu/xmlui/bitstream/handle/2144/1351/GDDP_Educopia.pdf?sequence=1

Sousa, P. (2013) Segurança e preservação da informação: um modelo para os Municípios. Dissertação de mestrado, Universidade do Porto, Porto, Portugal

Strodl, S., Becker, C., Neumayer, R., Rauber, A.(2007) How to choose a digital preservation strategy: evaluating a preservation planning procedure. Consultado em

Janeiro 12, 2015 em
http://www.ifs.tuwien.ac.at/~becker/pubs/strodl_choose_JCDL07.pdf

Strodl, S., Rauber, A. (2008) Preservation planning in the OAIS model. Consultado em Janeiro 12. 2015 em http://www.ifs.tuwien.ac.at/~strodl/paper/Strodl_IPRES07.pdf

Svård, P. (2013) Enterprise Content Management and the Records Continuum Model as strategies for long-term preservation of digital information. *Records Management Journal*. vol.23, nº3

THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (2014) Recommendation for Space Data System Practice (Magenta Book). Requirements for Bodies providing Audit and Certification of Candidate Trustworthy Digital Repositories. Washington DC, USA. Consultado em Outubro 29, 2014 em <http://public.ccsds.org/publications/archive/652x1m2.pdf>

THE NATIONAL ARCHIVES (a) Digital Preservation Policy. Consultado em Outubro 24, 2014, em <http://www.nationalarchives.gov.uk/information-management/projects-andwork/digital-preservation-policy.htm>

THE NATIONAL ARCHIVES (b) Digital Preservation Strategy. Consultado em Outubro 27, 2014, em <http://www.nationalarchives.gov.uk/information-management/projects-andwork/digital-preservation-strategy.htm>

Thibodeau, K. (2002) Overview of technological approaches to digital preservation and challenges in coming years. Consultado em Novembro 3, 2014, em: <http://www.clir.org/PUBS/reports/pub107/thibodeau.html>

Thomaz, K. P., Soares, A. J. (2004). A preservação digital e o modelo de referência Open Archival Information System (OAIS). *Data Gram Zero - Revista de Ciência da Informação*, vol. 5, nº 1 (fev. 2004) - Artigo 01. ISSN: 1517-3801. Consultado em Outubro 30, 2014, em http://www.dgz.org.br/fev04/F_I_art.htm

UNESCO (2003) - Guidelines for the preservation of digital heritage. Consultado em Outubro 30, 2014 em <http://unesdoc.unesco.org/images/0013/001300/130071e.pdf>

Vieira, R.; Borbinha, J. (2011) MoReq2010 - Uma Apresentação. 10º Encontro Nacional de Arquivos Municipais, Leiria, 4 e 5 Novembro, 2011: atas. Lisboa: BAD. Consultado em Novembro 2, 2014, em <http://bad.pt/publicacoes/index.php/arquivosmunicipais/article/view/19/9>

Vieira, R. et al. (2012) A requirements engineering analysis of MoReq. Records Management Journal, Vol. 22 No. 3, pp. 212-228

Witt, M., et al. (2012) ISO 16363: Trustworthy Digital Repository Certification in Practice. Libraries Faculty and Staff Presentations. Paper 4. Consultado em Novembro 3, 2014, em http://docs.lib.purdue.edu/lib_fspres/

Anexos Públicos

Anexo 1 - Árvore de Objetivos

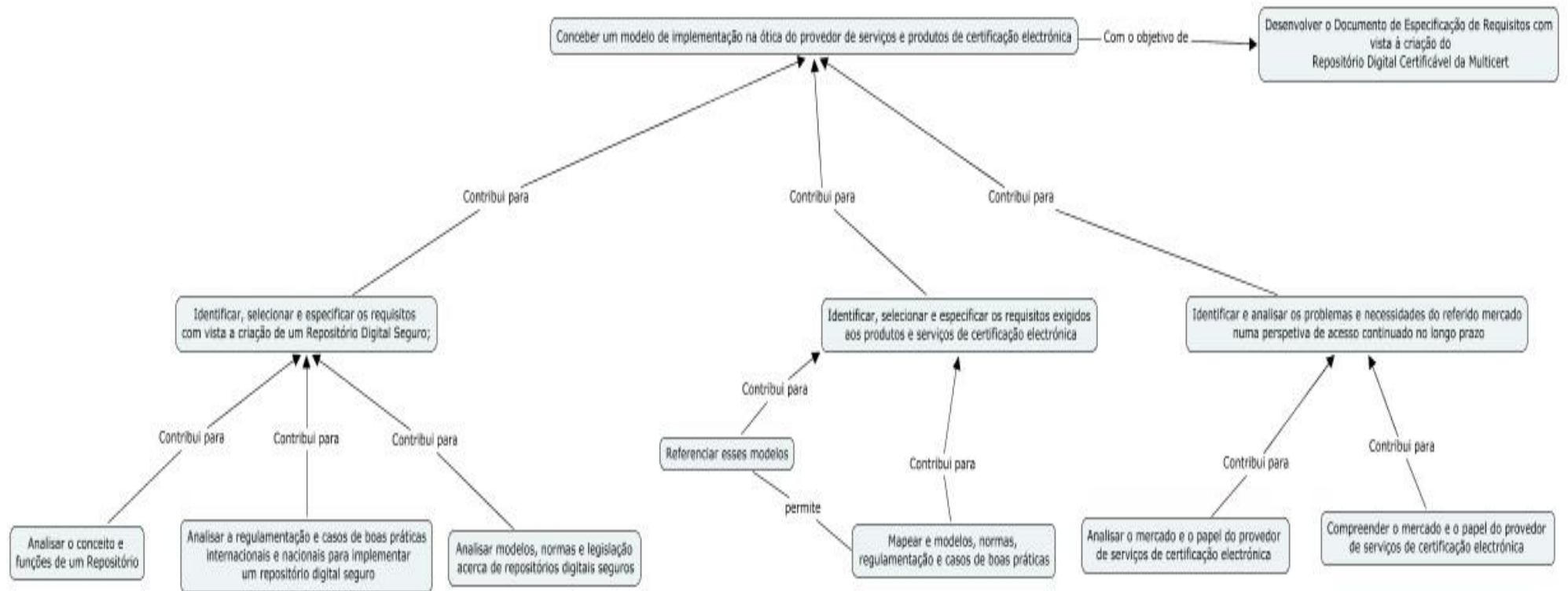
Anexo 2 - Legislação usada pela Multicert

Anexo 3 - Principais parceiros da Multicert

Anexo 4 - Questionário IM3 Tool

Anexo 5 - Poster apresentado nas XIII Jornadas de Ciência da Informação

Anexo 1 - Árvore de Objetivos



Anexo 2 - Legislação usada pela Multicert

Normas Nacionais	Normas Internacionais	Regulamentação e Legislação Nacional	Regulamentação e Legislação Internacional
GNS / NT-D 03 - Requisitos para Entidades Certificadoras que emitem Certificados Qualificados	ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures, v1.1.1	Decreto-Lei nº 62/2003	Directiva 1999/93/CE do Parlamento Europeu e do Conselho
	ETSI EN 319 411-2 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates, v1.1.1	Decreto-Lei nº 88/2009	
	ETSI EN 319 411-3 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates, v.1.1.1	Decreto-Lei 290-D/99 (republicado pelo Decreto-Lei nº88/2009)	
	ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate Profile	Decreto Regulamentar nº 25/2004	
	ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities		

Normas Nacionais	Normas Internacionais	Regulamentação e Legislação Nacional	Regulamentação e Legislação Internacional
	ETSI TS 102 176-1, 2007-11. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, v.2.0.0		
	ETSI TS 119 403 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General requirements and guidance, v1.1.1		
	ETSI TS 119 412-2 - Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons, v1.2.1		
	FIPS PUB 186-4 (2013) - Digital Signature Standard		
	ISO/IEC 27001:2005 (Information technology. Security techniques. Information security management systems. Requirements		
	RFC 1421. 1993, Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures		
	RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management		
	RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers		
	RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related		

Normas Nacionais	Normas Internacionais	Regulamentação e Legislação Nacional	Regulamentação e Legislação Internacional
	Services		
	RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP		
	RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework,		
	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.		
	ETSI TS 119 412-2 - Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons, v1.2.1		
	FIPS PUB 186-4 (2013) - Digital Signature Standard		
	RFC 1421. 1993, Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures		
	RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management		
	RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers		
	RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services		

Normas Nacionais	Normas Internacionais	Regulamentação e Legislação Nacional	Regulamentação e Legislação Internacional
	RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP		
	RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework,		
	RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.		

Anexo 3 - Principais parceiros da Multicert

- **AcinGov**: esta empresa queria ver resolvido um problema na qual os documentos eletrónicos que eram enviados para a plataforma de compras públicas acinGov careciam de assinatura digital qualificada, e neste sentido criaram uma parceria com a Multicert de forma a oferecer aos utilizadores da plataforma eletrónica a possibilidade de adquirirem esses certificados digitais qualificados da Multicert e ainda de associarem selos temporais aos documentos que são carregados na plataforma e também às transações que estão sujeitas a prazos.
- **ANO**: criada em 1994, sediada no Porto, tem como produto a produção e comercialização de *software*, bem como serviços de implementação do software e consultoria. As suas principais áreas de negócio são os sistemas para governo electrónico; sistemas de gestão da via pública (contraordenações, multas de trânsito, reboques e bloqueios)
- **APEMIP**: Associação Portuguesa das Empresas de Mediação Imobiliária, é uma entidade sem fins lucrativos que ocupa nos dias de hoje uma posição destacada no mercado do imobiliário nacional, quer pela aposta contínua na afirmação do papel do profissional de mediação imobiliária, quer pela conquista de uma maior quota de mercado das transações de imóveis. Associou-se à Multicert através de um protocolo de acordo visando uma parceria institucional a qual permite que todas as empresas de mediação imobiliária possam adquirir certificados digitais qualificados.
- **Forum B2B**: surgiu de uma iniciativa conjunta de varias empresas nacionais entre os quais se destacam dois dos maiores grupos empresariais nacionais, a EDP e a GalpEnergia. Tem como missão controlar custos relacionados com transações de bens e serviços entre empresas contribuindo para uma maior eficiência operacional, como redução de custos por transação e parcerias comerciais mais efetivas.
- **Gecorpa**: é o grémio das empresas de conservação e restauro do património arquitetónico o qual pretende reunir as empresas e as pessoas que procuram promover a excelência e prosseguir em todas as intervenções de salvaguarda dos monumentos e do património construído e a sua transmissão às futuras gerações.

- **Generix Group**: editora de *software* que oferece soluções de comércio colaborativo permitindo o intercâmbio de dados, gerir fluxos, otimizar o custo de disponibilidade dos bens de consumo em toda a cadeia de valor de maneira a aumentar as vendas. É uma oferta única de mercado que se destina às empresas dos setores de bens de grande consumo, distribuição alimentar e especializada, automóvel, saúde, publicidade, e-commerce, transportes e da logística.
- **Iberomail**: Organização especialista em distribuição nacional e internacional de correio e encomendas, licenciada pela ANACOM. Em 2010 lançou o SIGEC, uma aplicação web que permite a impressão, envelopagem e envio de documentos e faturas assinadas digitalmente.
- **Janela Digital**: empresa que se dedica exclusivamente ao desenvolvimento e investigação de soluções tecnológicas para o imobiliário estando presente em vários países afirmando-se como um *player* internacional nas áreas de gestão e marketing imobiliário.
- **M&A Digital**: dedicando-se em exclusivo à área das novas tecnologias, tem por objetivo ser uma empresa prestadora de serviços digitais com desenvolvimento integrado, criando *software* próprio e soluções digitais à medida. Fornece ao abrigo do protocolo criado com a Multicert um conjunto alargado de soluções de certificação digital ou certificação eletrónica. Através desta parceria com a Multicert a M&A digital passa a integrar no seu portfólio de serviços a solução de fornecimento e instalação de certificados digitais que garantem digitalmente uma Assinatura Qualificada com todo o valor probatório legal.
- **Miroma**: criada em 1994 integra um grupo de empresas na área das tecnologias da informação com especial enfoque no setor público no qual se destacam as juntas de freguesia, associações, câmaras municipais que utilizam a plataforma eletrónica de contratação pública.
- **Netgocio**: criada em 1998, a Netgocio desenvolve a sua atividade na criação de soluções de internet para o mercado empresarial e institucional. Aposta na inovação e criatividade o que faz dela uma empresa impar no mercado das novas tecnologias.

- **Sourcebiz**: tem como *core business* o mercado eletrónico e tudo aquilo que se relaciona com transações eletrónicas que estão ao abrigo de legislação própria como é o caso da contratação pública, gestão urbanística, transação de imóveis, licenciamento eletrónico e autenticação de documentos. Com a parceria à Multicert, a Sourcebiz pode apoiar e transacionar os certificados digitais qualificados para o mercado nacional, oferecendo apoio logístico e técnico junto dos seus clientes que necessitam de os obter.
- **YET**: Your Electronic Transactions é uma empresa especializada na implementação e desenvolvimento de produtos e serviços na área das transações eletrónicas, desde a digitalização de dados, ao arquivo digital, à integração de ERP's com diferentes sistemas de informação, certificação digital e acesso a redes nacionais e internacionais de empresas do setor da grande distribuição.
- **Informa D&B**: é uma empresa especialista no conhecimento do tecido empresarial, fornecendo informação atualizada e rigorosa sobre a atividade comercial, financeiro e de marketing de empresas e gestores. Através de uma análise inovadora disponibilizam o acesso à informação relevante para a condução dos negócios dos seus clientes. Com a parceria à Multicert permitiu que a Organização proporcionasse aos seus clientes uma oferta mais diversificada e completa de serviços.
- **FortConsult**: tem como *core business* os testes de penetração e avaliações de segurança. Realizou testes em milhares de sistemas e aplicativos em configurações simples e complexas como bancos *online*, sistemas de pagamento, *single sign-on* e sistemas de *back-end*. É especialista em avaliar a segurança das Tecnologias de Informação, fornecendo-lhe uma proteção acrescida contra ameaças à segurança e à tranquilidade que são necessárias para desenvolver soluções de TI controlando o nível de risco.

Data: 10/02/2015
Projeto: Certificação do Repositório Digital
Nível de Acesso: Confidencial ☐ Restrito ☒ Público ☐ Outro ☐ - "Indicar qual"
Assunto: Avaliação da maturidade da Gestão da Informação – IM3 tool
Observações:

INQUÉRITO

1. PESSOAS

Perguntas sobre o conhecimento, habilidade, experiência e atitude dos Colaboradores da Multicert de maneira a contribuir para uma boa Gestão da Informação.

1.1. Literacia da Informação e responsabilidade

PERGUNTA: Os profissionais responsáveis pela Gestão da Informação estão conscientes das suas responsabilidades? A Informação é considerada e tratada como um bem valioso?

1. Os Colaboradores estão em grande parte inconscientes do valor potencial da informação e das suas responsabilidades.
2. Os Colaboradores estão cientes da informação produzida pela sua equipa ou apenas da área. Os Colaboradores reconhecem que o seu papel envolve uma certa quantidade de Gestão da Informação, mas aplicam-no apenas a um nível pessoal ou de equipa.
3. Os Colaboradores aplicam práticas de Gestão de Informação adequadas para o seu papel, na medida em que as políticas disponíveis, procedimentos e tecnologias o permitem. Os Colaboradores estão cientes da informação produzida pela sua equipa ou área e por outras áreas.
4. Os Colaboradores consideram a Gestão da Informação como parte integrante do seu papel; eles entendem a importância de práticas de gestão adequadas e agem em conformidade. A maioria dos Colaboradores estão cientes da informação produzida pela Organização.
5. Os Colaboradores estão plenamente conscientes da importância da Gestão da Informação para a Organização e as suas responsabilidades em relação a ela. Os Colaboradores são educados e encorajados a explorar a informação ao máximo.

Desconhecido / Necessita de obter mais informação

Não aplicável à Organização

Notas (opcional):

1.2. Aptidão e Competência

PERGUNTA: A aptidão e competência de Gestão de Informação da Organização são suficientes para desenvolver e apoiar uma boa Gestão da Informação?

1. Não existem especialistas de Gestão da Informação na Organização e existe pouca consciência da necessidade de construir competências nesta área. A Empresa baseia-se no conhecimento local para resolver os desafios de Gestão de Informação.
2. A experiência em Gestão da Informação na Organização está presente, mas inconsistente. Há consciência de que é necessário desenvolver competências de Gestão da Informação.
3. Especialistas em Gestão de Informação foram nomeados e são, por vezes consultados por outras áreas do negócio. As lacunas na aptidão e competência de Gestão da Informação podem ter sido identificadas.
4. Requisitos de aptidão e competência de Gestão de Informação da Organização foram adequadamente identificados. Especialistas de Gestão de Informação foram nomeados e estão envolvidos numa série de iniciativas de negócios.
5. A Organização dá prioridade ao recrutamento de especialistas de Gestão de Informação para ajudar a desenvolver a competência de Gestão da Informação da Organização e são regularmente avaliados em termos de competência, habilidades e conhecimentos. São profissionais respeitados que são consultados no desenvolvimento e implementação de todas as iniciativas de negócios.

Desconhecido / Necessita obter mais informação

Não aplicável à Organização

Notas (opcional):

1.3. Formação e Suporte

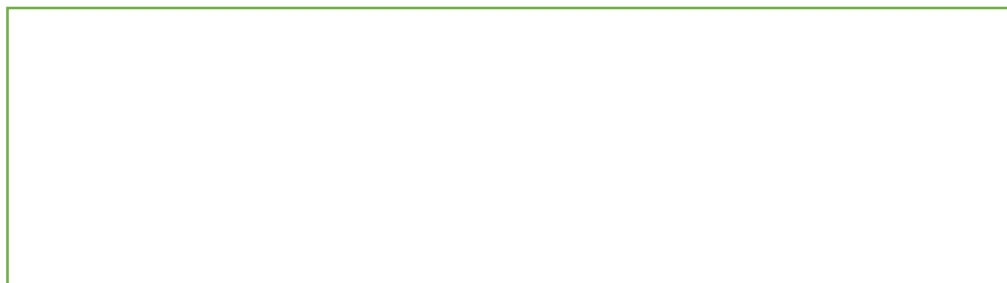
PERGUNTA: Que formação e suporte estão disponíveis na Organização para ajudar os Colaboradores no cumprimento das suas atividades de Gestão da Informação?

1. Nenhuma formação ou suporte específico está disponível para apoiar os Colaboradores no acesso e uso da informação. A maioria dos conselhos é recebido informalmente a partir de colegas ou da equipa de suporte técnico.
2. Alguma formação em Gestão de Informação está disponível para a equipa, mas só é fornecido no processo de acolhimento ou em resposta a uma atividade de negócio por exemplo, a implementação de um novo sistema de gestão.
3. Os requisitos de formação para o uso de tecnologias e recursos de informação foram identificados. Um programa de formação de Gestão de Informação foi proposto ou está a ser desenvolvido, com o apoio de especialistas da área.
4. É oferecida aos Colaboradores, formação nas tecnologias usadas para a Gestão de Informação. A formação é baseada na análise das necessidades e feedback dos Colaboradores. Está disponível um suporte para ajudar os Colaboradores com questões acerca da Gestão da Informação.
5. Os Colaboradores estão totalmente informados sobre os princípios, papéis e responsabilidades específicas da Gestão da Informação. Os Colaboradores têm acesso a formações de Gestão de Informação internas e / ou externas relevantes para o seu cargo.

Desconhecido / Precisa de mais informação

Não aplicável na empresa

Notas (opcional):



2. ORGANIZAÇÃO

As perguntas nesta secção vão incidir sobre o papel da Gestão da Informação na Organização

2.1. Visão e estratégia da Gestão de Informação

PERGUNTA: A Organização tem formulada e articulada a sua visão para a Gestão da Informação?

1. A Gestão da Informação não é considerada como parte das atividades de planeamento estratégico. Planeamento e desenvolvimento da Gestão de Informação não é uma prioridade na Organização.
2. Embora os planos estratégicos e de negócio estejam preparados para a Organização, eles não tratam especificamente de Gestão da Informação. A Gestão da Informação é reconhecida por alguns como sendo de importância estratégica, mas isso não tem sido adotado em toda a Organização.
3. A necessidade de uma Estratégia de Gestão da Informação é reconhecida. A formulação de resultados desejados, prioridades estratégicas e recursos na área de Gestão da Informação estão a começar.
4. Uma estratégia de Gestão da Informação foi desenvolvida e implementada, adequada às necessidades da Organização, à cultura corporativa, ao ambiente tecnológico e exposição ao risco. Ela destaca questões de Gestão de Informação de toda a Organização, como grandes riscos, os resultados desejados e as implicações de recursos.
5. O desenvolvimento da estratégia entre Gestão de Informação e o negócio são feitos de forma colaborativa e simultânea, utilizando métricas adequadas. O Planeamento de Gestão da Informação liga a visão e objetivos estratégicos da Organização para a sua gestão global de informação. Conhecimento de Gestão de Informação sustenta estratégias de tomada de decisão de negócios e proporciona benefícios comerciais tangíveis.

Desconhecido / Necessita de mais informação

Não aplicável à Organização

Notas (opcional):

2.2. Auditoria e Conformidade

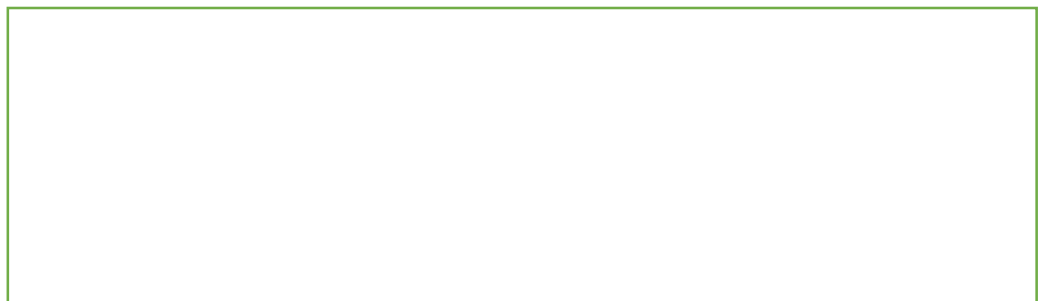
PERGUNTA: Como é que a Organização monitoriza a conformidade com os seus próprios padrões de Gestão da Informação e com a legislação e os requisitos normativos?

1. A Organização não tem qualquer processo de auditoria ou processo de revisão para garantir a conformidade com políticas, legislação e padrões de Gestão de Informação.
2. A Organização iniciou um programa para o cumprimento da legislação, políticas e normas. O processo de auditoria e de revisão não foi totalmente implementado em toda a Organização.
3. O processo de auditoria e revisão garante um nível adequado de conhecimento e cumprimento da legislação, políticas e normas aplicáveis.
4. Os requisitos de conformidade são comunicados a toda a Organização e são aplicados de forma coerente com as iniciativas de manutenção e Gestão de Informação. As ações corretivas são realizadas de forma sistemática e oportuna.
5. A Organização está confiante de que está em conformidade com toda a legislação, políticas e normas pertinentes. As ações corretivas combatem as causas das não-conformidades. Oportunidades para melhorar o cumprimento destas são exploradas e implementadas.

Desconhecido / Precisa de mais informação

Não aplicável na Organização

Notas (opcional):



3. QUALIDADE E CICLO DE VIDA DA INFORMAÇÃO

As perguntas desta seção irão incidir sobre a gestão dos ativos de informação específicos na Organização, com vista a um acesso de longo prazo a informação de qualidade.

3.1. Gestão de Ativos

PERGUNTA: Até que ponto a Organização identifica, gere e monitoriza a sua informação?

1. Não há identificação da informação importante e do armazenamento da mesma. Informação importante ou estratégica não é identificada ou gerida.
2. O armazenamento de informação é informal. Os Colaboradores gerem a informação baseando-se na sua perceção e práticas.
3. Responsabilidades de propriedade da Informação e de armazenamento foram definidas e comunicadas, no entanto, ainda é praticada de forma inconsistente em toda a Organização. Há reconhecimento geral de que a informação podia ser melhor gerida.
4. A Organização está empenhada em garantir o armazenamento da informação. Os Colaboradores compreendem as suas responsabilidades de registar e manter a informação através de seu ciclo de vida.
5. Um modelo de armazenamento de informação foi transposto para a Organização em conformidade com as normas. Informação importante é gerida durante todo o seu ciclo de vida. Os Colaboradores com funções de Gestão de Informação trabalham ativamente com os utilizadores da informação para melhorar a utilização e a partilha.

Desconhecido / Precisa de mais informação

Não aplicável à Organização

Notas (opcional):

3.2. Políticas e Procedimentos

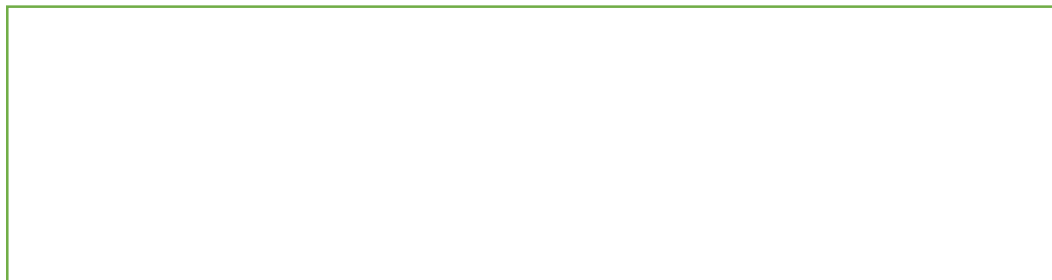
PERGUNTA: A Organização tem desenvolvido e implementado políticas de Gestão da Informação que fazem referência às Normas? Essas políticas são apoiadas por procedimentos documentados?

1. Não foram adotadas normas ou políticas relacionadas com a Gestão de Informação. As equipas de negócio definem e aplicam os seus próprios procedimentos.
2. Algumas normas estão a ser aplicados de forma ad-hoc. Não existe nenhuma Política de Gestão de Informação, mas alguns reconhecem que é necessário. Existem alguns procedimentos padrão a serem aplicados em toda a Organização.
3. Normas para a Gestão da Informação estão a ser incorporadas nas práticas de negócios. Uma Política de Gestão da Informação tem sido desenvolvida e a maioria dos Colaboradores estão cientes e seguem a política, mas violações a esta provavelmente ainda estão a acontecer.
4. Os Colaboradores seguem procedimentos de Gestão de Informação que está alinhada com a política da Organização. Políticas e procedimentos são adequados para o negócio da Organização e são revistos periodicamente para melhoria.
5. A Organização adotou normas que se refletem nas políticas e processos de negócio. As políticas são ativamente comunicadas e disponíveis para todos os Colaboradores, e são frequentemente revistas e atualizadas para assegurar a relevância e eficácia. A aplicação de políticas tem sido avaliada para confirmar que cumprem adequadamente as necessidades e requisitos de Gestão da Informação da Organização.

Desconhecido / Precisa de mais informação

Não aplicável na Organização

Notas (opcional):



3.3. Satisfazer as necessidades de negócio

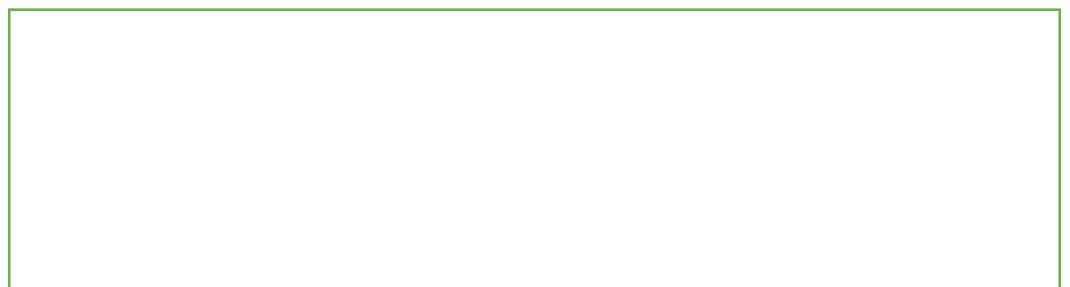
PERGUNTA: A informação está a atender as necessidades da empresa e dos seus Colaboradores em termos de importância estratégica, qualidade e acesso?

1. A informação disponível na Organização não é confiável e é incompleta. Há pouca compreensão das necessidades de informação do negócio e de como atingi-los.
2. Reconhece-se que a qualidade da informação é desigual em toda a Organização. Pode-se notar que os sistemas de informação não estão a cumprir a necessidade existente. A questão foi levantada ao nível da gestão.
3. A Gestão tomou medidas no sentido de reconhecer e abranger os princípios de qualidade da informação. Uma análise das necessidades de informação tem sido conduzida.
4. Informação sobre a Organização é considerada como de alta qualidade. Processos de melhoria estão no local para resolver questões de qualidade de informação. A Organização demonstra a conformidade com os padrões de qualidade da informação.
5. A informação sobre a Organização é reconhecida como autêntica e confiável por todos os utilizadores. A Organização tem implementado um programa de qualidade de informação dinâmico.

Desconhecido / precisa de mais informação

Não aplicável na Organização

Notas (opcional):



3.4. Acesso e Pesquisa

PERGUNTA: Quão fácil é para os Colaboradores encontrar a informação que procuram? Uma informação é capaz de ser encontrada quando ela é necessária?

1. Os Colaboradores gastam tempo excessivo à procura de informação eletrónica e em papel, usando uma variedade de métodos. A informação é armazenada de forma não-estruturada e com pouca ou nenhuma meta-informação associada.
2. Existem algumas diretrizes internas para o armazenamento e recuperação de informação, mas estas são aplicadas de forma irregular. Meta-informação básica pode ser aplicada a sistemas de informação para facilitar a localização, mas sabe-se que há uma grande quantidade de informação "invisível" na Organização, e que uma grande quantidade de informação desnecessária está a ser armazenada.
3. O acesso à informação é feito através de um único portal utilizando um sistema de meta-informação ou classificação. Os Colaboradores estão razoavelmente confiantes de que podem encontrar a informação que procuram.
4. Um repositório específico e / ou aplicativos de pesquisa foram desenvolvidos e são utilizados pelos Colaboradores. A informação é recolhida e armazenada com o propósito de ser acedida e localizada pelos utilizadores. Existe meta-informação suficiente para identificar e localizar a informação corretamente. O acesso controlado aos documentos foi definido e implementado.
5. Facilidade de armazenamento, classificação e recuperação da informação é uma operação central da Organização. Acesso à informação e partilha é facilitado e promovido ativamente. Procedimentos operacionais como a aplicação de meta-informação para o acesso à informação, armazenamento e recuperação têm sido implementados. A Organização está a trabalhar para a construção de um diretório de informação comum e outros mecanismos para facilitar a interorganização e descoberta de informação.

Desconhecido / Precisa de mais informação

Não aplicável à Organização

Notas (opcional):

3.5. Uso e reutilização da Informação

PERGUNTA: Quão utilizável é/será a informação que está a ser produzida pela Organização, tanto agora como no futuro?

1. A informação é frequentemente repetida/duplicada em diferentes áreas da Organização, sem aplicação de meta-informação. Há pouca troca de informação entre as áreas de negócio ou com outros grupos de interesse.
2. Têm ocorrido algumas tentativas de racionalizar a utilização da informação da Organização, mas as equipas são individuais e protetoras da sua própria informação. A informação criada é, em grande parte, de uso único e com pouca consideração para acesso futuro.
3. Foram introduzidas normas na Organização para facilitar a recolha, descrição e organização da informação e para evitar a duplicação da mesma. A partilha de informação na Organização é cada vez maior e a necessidade de proteger a informação para uso futuro é reconhecido.
4. O uso atual e futuro da informação é considerado quando a informação está a ser recolhida e desenvolvida. A informação é partilhada e reutilizada em toda a Organização e com partes interessadas externas, conforme apropriado.
5. A informação é recolhida, desenvolvida e armazenada com a partilha, colaboração e interoperabilidade em mente. O uso e a partilha da informação são facilitados e promovidos ativamente. Os Colaboradores procuram reutilizar e atualizar a informação existente em vez de criar uma nova. A Organização aplica níveis de acesso apropriados à informação e quando aplicável é disponibilizada para o público.

Desconhecido / Precisa de mais informação

Não aplicável na Organização

Notas (opcional):

4. SISTEMAS E PROCESSOS DE NEGÓCIO

As perguntas desta secção são sobre os sistemas e processos (tanto eletrónicos como manuais), que apoiam as práticas de Gestão de Informação na Organização.

4.1 . Melhoria de processos

PERGUNTA: Os processos de negócios foram alinhados com os requisitos de gestão de informação para garantir a qualidade da informação? A Organização identificou os pontos de integração de informação e eliminou processos duplicados?

1. Os processos de negócios em geral, não tomam em consideração a gestão de informação. Há evidências de sobreposição e / ou duplicação de processos e informação entre áreas.
2. Há uma consciência de que a Gestão da Informação pode / deve ser incorporada nos processos empresariais. A Organização está a fazer um esforço para perceber onde os processos de negócios podem ser redesenhados para melhorar a eficiência e reduzir a duplicação de informação.
3. Algumas práticas de Gestão de Informação foram incorporadas para melhorar as práticas de negócio existentes. Alguns processos duplicados foram eliminados e há melhor integração de processos e fluxo de informação.
4. Um esforço significativo tem sido posto em processos de reengenharia para eliminar a duplicação de informação e melhorar o fluxo de informação. Há visibilidade sobre os detalhes do processo e os proprietários desses processos estão abertos à mudança. Questões relativas a processos relacionados com a qualidade da informação são dirigidas aos Colaboradores apropriados.
5. Atividades de melhoria contínua são realizadas regularmente para garantir que os processos de negócio são otimizados para a qualidade, fluxo e partilha da informação. Processo de colaboração entre as equipas é alto e reflete melhores práticas da Organização.

Desconhecido / Precisa de mais informação

Não aplicável na Organização

Notas (opcional):

4.2. Sistemas e ferramentas de negócio

PERGUNTA: Será que a tecnologia disponível no apoio à Organização permite o fornecimento de uma estratégia de gestão de informação?

1. Não existe um sistema comum com fortes capacidades de Gestão de Informação. Existem vários sistemas, exigindo diferentes logins, que podem armazenar a mesma informação dentro da Organização. Ferramentas de Gestão de Informação, se existir, são selecionadas, e operadas pela área de Administração de Sistemas. Tem varias sistemas é o grande problema
2. A Organização está a tentar implementar a Gestão da Informação em sistemas de negócios que visam a concessão de uma melhor Gestão da Informação. Os esforços para encontrar tecnologias e ferramentas apropriadas foram iniciados, envolvendo especialistas de TI e de Gestão da Informação.
3. Ferramentas e sistemas de Gestão de Informação estão focados na informação crítica de negócios. Houve uma tentativa de combinar ou integrar sistemas de informação em todas as áreas.
4. TI e Gestão de Informação não são considerados como disciplinas separadas. Normas e práticas de Gestão de Informação foram implementados com sucesso em toda a Organização para criar um ambiente de informação consistente e confiável.
5. Sistemas de informação compatíveis e personalizados para as necessidades da Organização são totalmente operacionais e desempenham um papel crítico na gestão do ciclo de vida da informação. Os sistemas são geridos de forma eficaz durante o seu ciclo de vida, desde a aquisição até à desativação, para garantir a sua integridade e confiabilidade.

Desconhecido / Necessita de mais informação

Não aplicável à Organização

Notas (opcional):

4.3. Segurança da Informação

PERGUNTA: Qual é o estado da segurança da informação na Organização? Existe um sistema de Gestão de Segurança da Informação que trata do conjunto de preocupações de segurança da informação?

1. Não há uma Gestão da Segurança da Informação e falhas não-intencionais de segurança provavelmente estão a acontecer.
2. Foram feitos alguns esforços para proteger a informação, mas estas ainda são geridas ao nível de áreas independentes e abertos a um risco significativo.
3. A Organização está consciente das exigências do Sistema de Gestão de Segurança da Informação e está a trabalhar em medidas para atender às necessidades de execução.
4. A Organização está a implementar ativamente os requisitos do Sistema de Gestão de Segurança da Informação e a acompanhar a execução através da Autoavaliação do Relatório de Conformidade.
5. O Sistema de Gestão de Segurança da Informação está totalmente implementado, de acordo com os requisitos das normas ISO 27001. Não está aplicado a toda a empresa

Desconhecido / Precisa de obter mais informação

Não aplicável na Organização

Notas (opcional):

Anexo 5 - Poster da dissertação apresentado nas XIII Jornadas de Ciência da Informação em Maio de 2015

REPOSITÓRIO DIGITAL SEGURO

UM MODELO DE REQUISITOS PARA UM PROVEDOR DE SERVIÇOS DE CERTIFICAÇÃO

Dissertação em ambiente empresarial



Ângela Sofia de Sousa Santos

Orientação: Maria Manuela Pinto

CONTEXTUALIZAÇÃO

Campo científico: Ciência da Informação (CI)

Área de estudos: Gestão da Informação (GI)

Contexto: Prestador de produtos e serviços de certificação (MULTICERT)

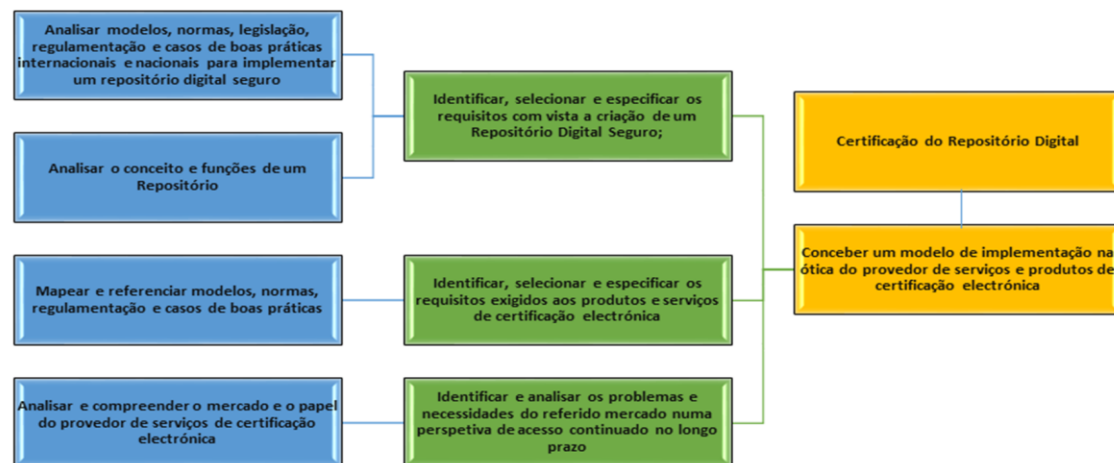
Objetivo geral: contribuir para a estruturação de um repositório digital seguro através de um diagnóstico organizacional, tecnológico e informacional e consequente elaboração de um *Documento de Especificação de Requisitos*

PROBLEMA/NECESSIDADE

A MULTICERT está particularmente sensível à temática da segurança da informação e, crescentemente, à necessidade de criar um Repositório Digital Seguro / Confiável e que atenda aos requisitos de Preservação da Informação no longo prazo. Neste contexto define-se a questão orientadora:

Como pode um fornecedor de produtos e serviços de certificação eletrónica contribuir para a segurança e a preservação da informação numa perspectiva de acesso continuado no longo prazo?

OBJETIVOS



REFERÊNCIAS

Planeamento

- PLANETS / OAIS
- PLATO, SCAPE
- Projeto APARSEN

Auditoria

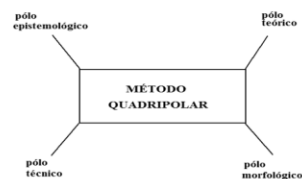
- DRAMBORA

Certificação

- ISO 15363:2012
- European Framework for Audit and Certification of Digital Repositories
- Data Seal of Approval e WDS
- Projeto PORTICO

MÉTODO e METODOLOGIAS

O Método Quadripolar orienta a delimitação e análise do problema e o desenvolvimento de contributos para a sua resolução



- Recolha e revisão de literatura com base nas metodologias de recolha e análise de dados
- Identificação e análise de casos similares
- Análise do contexto organizacional, tecnológico e informacional
- Observação direta e participante do funcionamento da Organização
- Realização de entrevistas exploratórias (colaboradores e parceiros)
- Levantamento, análise e especificação de requisitos

Metodologia de Investigação—Ação
Engenharia de Requisitos

RESULTADOS ESPERADOS

Diagnóstico e Avaliação da Maturidade da Gestão de Informação na MULTICERT

Documento de Requisitos para a criação do Repositório Digital Seguro/Confiável

Bases para a definição da Estratégia e Políticas de Gestão da Informação na MULTICERT

CONCEBER UM MODELO DE REQUISITOS NA ÓTICA DO PROVEDOR DE SERVIÇOS E PRODUTOS DE CERTIFICAÇÃO ELECTRÓNICA