M 2014

U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

A PRESERVAÇÃO DA INFORMAÇÃO:

UM CONTRIBUTO PARA A IMPLEMENTAÇÃO DE UM ARQUIVO DIGITAL CERTIFICÁVEL NO MUNICÍPIO DO PORTO

HUGO AZEVEDO OLIVEIRA

DISSERTAÇÃO DE MESTRADO APRESENTADA
À FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO EM
CIÊNCIA DA INFORMAÇÃO

Hugo Azevedo Oliveira

A Preservação da Informação: um contributo para a implementação de um Arquivo Digital Certificável no Município do Porto

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

Faculdade de Engenharia e Faculdade de Letras

Universidade do Porto

Julho de 2014

A Preservação da Informação: um contributo para a implementação de um Arquivo Digital Certificável no Município do Porto

Hugo Azevedo Oliveira

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

Membros do Júri

Professor Doutor António Lucas Soares

Faculdade de Engenharia - Universidade do Porto

Professor Doutor Carlos Guardado da Silva

Faculdade de Letras - Universidade de Lisboa

Dra. Maria Manuela Pinto

Faculdade de Letras - Universidade do Porto

Agradecimentos

Na elaboração deste trabalho foram vários os que contribuíram para que fosse possível atingir o fim desta dissertação.

Em primeiro gostaria de agradecer toda a disponibilidade e apoio prestados por ambos os meus orientadores. À Professora Doutora Maria Fernanda Martins por todo o seu interesse, pelo apoio e orientação neste projeto. À Dra. Manuela Pinto um agradecimento especial por toda a dedicação, paciência e, sobretudo, pelo incentivo e amizade manifestados ao longo de todo este percurso.

Ao Dr. João Paulo Lopes pela oportunidade de poder desenvolver este projeto no Arquivo Geral, bem como pelo todo o seu interesse e disponibilidade que demonstrou ao longo de todo este projeto.

Aos meus colegas do Arquivo Geral, com especial atenção à Dra. Marta Brandão e Dra. Marta Costa, pela colaboração, pela partilha de conhecimento e apoio durante o tempo a que me dediquei a este projeto. Em particular, também à Elisa, Emília, Hugo e José António.

Aos meus amigos e colegas de mestrado pelo seu companheirismo, pela partilha dos momentos de felicidade e incerteza ao longo do projeto, que se demonstraram importantes para o alcançar deste marco.

À minha família por todo o apoio e incentivo e pela contribuição para a minha formação, quer a nível pessoal quer profissional, sempre com esperança e convicção de que terminaria este projeto com sucesso.

Por último, um agradecimento muito especial à Ana Sofia, pela sua compreensão, força, carinho e todo o seu constante apoio que se tornou sem dúvida essencial para a concretização do Mestrado em Ciência da Informação (MCI).

"Na adversidade, uns desistem, enquanto outros batem records"

Ayrton Senna

Resumo

É indiscutível a importância que as TIC possuem na Era da Informação, constituindo-se como suporte na atualização e transformação da Administração Pública. A disseminação dos "sistemas de informação", a rápida evolução tecnológica e a quase total dependência da tecnologia, por parte de organizações e pessoas na sua atividade quotidiana, leva a que a temática da *Preservação da informação* se encontre numa posição cimeira nos dias atuais.

Sente-se, assim, a necessidade de repensar as tradicionais abordagens e discutem-se possíveis soluções mas, num momento em que a informação em meio digital, isto é, recebida, produzida e acumulada pela organização ou instituição, resultado de processos de digitalização ou nado-digital, assume cada vez maior importância, é um imperativo agir de forma fundamentada, assumir compromissos claros e avançar para a sua concretização. Este "desafio" vai, portanto, para além da *tecnologia*, envolvendo a *organização*, os seus *atores* e *processos*, bem como a *informação* produzida, recebida e armazenada, aplicando em relação direta diferentes perspetivas disciplinares mas onde se destaca o papel a desempenhar pela *Gestão da Informação,* a nível teórico e aplicado, e um novo posicionamento que coloca a Preservação da informação como sua variável, identificando-se claramente como objeto de estudo e de trabalho o fenómeno e processo infocomunicacional.

Este projeto de dissertação na área científica da Ciência da Informação (CI) e no campo de estudos da Gestão da Informação (GI), teve como contexto o universo das *Autarquias Locais* que necessitam, não unicamente de dar resposta a estas questões, mas, igualmente, de responder às políticas nacionais e internacionais que, cada vez mais, ditam um novo quadro de modernização administrativa crescentemente sustentado na utilização e mediação das TIC.

O estudo a desenvolver centrou-se na vertente da *Preservação da Informação*, no âmbito da *implementação e certificação do Arquivo Digital da Câmara Municipal do Porto,* enquadrado, em termos gerais, na *Política de Gestão da Informação e da Gestão das Tecnologias da Informação*, e, mais especificamente, na *Política de Preservação e Segurança da Informação*, tendo em vista a identificação e desenvolvimento de uma estrutura informacional de suporte à especificação, desenvolvimento e implementação das políticas, estratégias e planos relativos à preservação da informação em meio digital e à especificação de requisitos para o repositório digital confiável, enquadradas por uma proposta base de Política, Estratégia e Plano de Preservação da Informação da Câmara Municipal do Porto, na sua componente digital.

Desta forma, partindo do foco no meio digital, aborda-se a problemática da 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.

O contributo produzido fica patente na proposta de uma 2ª versão *do Modelo de Preservação e Segurança da Informação* (MP&SInf) que passa a incluir as bases do *Modelo Estratégico de Preservação da Informação,* complementando e articulando com o trabalho desenvolvido por Sousa (2013) no âmbito da Segurança da Informação. Detalharam-se, assim os elementos-base da componente digital, no âmbito da Gestão da Informação, a *Estrutura de "Serviços"* a prestar no âmbito da Gestão da Informação, o *Macroprocesso do 'Serviço de Gestão da Preservação' - Informação Digital* (que complementará o que existe na CMP para a Preservação de suportes tradicionais, por exemplo: pergaminho, papel e espécies fotográficas), a *Estrutura de Políticas e de Planos de Preservação e Segurança da Informação* e a estrutura e Documentos Base já criados para a respetiva especificação (os DSE), bem como o *Documento de Especificação de Requisitos* que suportará a certificação do Repositório Digital Confiável da CMP. Abordaram-se, ainda, dois casos práticos de produção informacional considerados prioritários no contexto da CMP, um em termos de especificação a desenvolver e outro que já resulta da adoção da estratégia de preservação de normalização de formatos a ingerir no repositório digital: 1) a recebida via email; 2) a adoção do formato PDF.

Palavras-chave: Ciência da Informação, Gestão da Informação, Preservação da Informação, Modelo de Preservação, Arquivo Digital, Certificação de Repositório, Produção Informacional via Email, Formato PDF, Autarquia Local, Câmara Municipal do Porto.

Abstract

It is undeniably the importance that ICT have in the Information Era, constituting as support in upgrading and transformation of the Public Administration. The dissemination of "information systems", rapid technological change and the almost total dependence on technology, by organizations and individuals in their daily activity, leads to the issue of preservation of information in a leading position today.

We feel therefore the necessity of rethink traditional approaches and discusses possible solutions but at a time when the digital information, ie, received, produced and accumulated by the organization or institution result of digitization processes or born-digital, assumes increasing importance, it is imperative to act in a reasoned manner, assume clear commitments and move towards its implementation.

This "challenge", therefore, goes beyond technology, involving the organization, its stakeholders and processes, as well as information produced, received and stored, applying in direct relationship different disciplinary perspectives but where it stands out the role to play by Information Management in theoretical and applied level, and a new positioning that puts the preservation of information as its variable, clearly identifying himself as an object of study and work and the phenomenon infocomunicacional process.

This dissertation project in the scientific area of information science and in the study field of Information Management, had as context the universe of Local Government that need not only to respond to these issues, but also to respond to national policies and international that more and more dictate a new framework for administrative modernization increasingly supported in the use and mediation of ICT.

The study to develop focused on the dimension of Preservation of Information, within the implementation and certification of the Digital Archive of the Municipality of Porto, framed in general terms, in the Information Management Policy (GI) and the Management of Information Technology (IT), and, more specifically, in the Information Preservation and Security Policy, in order to identifying and developing a informational structure supporting the specification, development and implementation of policies, strategies and plans applied to digital information preservation and the trusted digital repository requirements specification, framed by a base proposal for Policy, Strategy and Plan of Preservation of Information of Porto City Council, in its digital component.

This way, started from the focus on digital media, is addressed the problem of preservation of information on an integrated systems perspective and as a key function in the management

of organizational information, ie, without ignoring alignment of objectives, developing policies and cross-cutting strategies and compliance with good practices and assuming the preservation and information security and necessarily the technology that supports it, throughout their life cycle and management and organizational context in which it occurs.

The contribution made is clear in the proposal of a 2nd version of the Model for Preservation and Information Security (MP&SInf) which now includes the foundations of the Strategic Model for Preservation of Information, complementing and linking with the work developed by Sousa (2013) within the framework of Security information. We detailed, the fundamentals of digital component within the Information Management, the Structure of "services" to be provided under the Management of Information, the Macroprocess of the 'Service Management Preservation' - Digital Information (which will complement what exists in the CMP for the Preservation of traditional media, for example: parchment, paper and photographic species), the Structure of Policy of Preservation and Information Security and the structure and Documents Base already created for its specification (SDRs) and the Requirement Specification Document which shall bear the certification of Trustworthy Digital Repository of CMP. It also was approached two practical cases of informational production considered priorities in the context of CMP, one in terms of specification to develop and another already resulting from the adoption of conservation strategy standardization of formats to ingest the digital repository: 1) Received via email; 2) the adoption of the PDF format.

Keywords: Information Science, Information Management, Preservation of Information, Model of Preservation, Digital Archive, Certification of Repository, Informational Production by email, PDF format, Municipality, Porto City Hall.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AIP	Archival Information Package
AL	Administração Local
AMA	Agencia para a Modernização Administrativa
AP	Administração Pública
CI	Ciência da Informação
CIA	Conselho Internacional de Arquivo
CMP	Câmara Municipal do Porto
CPPD	Comité de Planeamento de Preservação Digital
CRL	Center for Research Libraries
CPSI	Comissão de Preservação e Segurança da Informação
DGLAB	Direção-Geral do Livro, dos Arquivos e das Bibliotecas
DMAG	Divisão Municipal de Arquivo Geral
DMAH	Divisão Municipal de Arquivo Histórico
DMSI	Divisão Municipal de Sistemas de Informação
DIP	Dissemination Information Package
DSE	Documentos de Suporte à Especificação
EAD	Encoded Archival Description
FEDORA	Flexible Extensible Digital Object Repository Architecture
GI	Gestão da Informação
MEF	Macroestrutura Funcional do Estado
MIP	Metainformação para a InteroPerabilidade
MP&SInf	Modelo de Preservação e Segurança da Informação
NARA	Nacional Archives and Records Administration
OAIS	Open Archival Information System

SAMA	Sistema de Apoios à Modernização Administrativa
SGQ	Sistema de Gestão da Qualidade
SGSPI	Sistema de Gestão de Segurança e Preservação da Informação
SI	Sistema de Informação
SIAP	Sistema [Integral] de Informação Ativa e Permanente
SIO	Sistema de Informação Organizacional
SIP	Submission Information Package
STI	Sistema Tecnológico de Informação
TI	Tecnologia de Informação
TIC	Tecnologias de Informação e Comunicação
TNA	The National Archives
TRAC	Trustworthy Repositories Audit & Certification
UCD	Unidade Central de Digitalização

Sumário

Introdução

1. Motivação e Objetivos

A área da Preservação da Informação em meio digital tem vindo a ser cada vez mais discutida e constitui-se como um alicerce fundamental para garantir o acesso continuado à informação no longo prazo.

À Preservação da Informação associam-se temáticas que focam a segurança da informação e a prevenção de falhas e riscos apontando todas elas para a importância da definição de políticas e estratégias, bem como de elaboração de planos que orientarão a ação operacional e que pressupõem o envolvimento do todo organizacional e a compreensão do que é necessário fazer por parte de todos os elementos da organização no sentido de orientar os esforços desenvolvidos e a desenvolver para estas temáticas, tornando-as uma efetiva prioridade e alertando os agentes intervenientes para o facto de que as suas ações contribuem (ou não) para um sistema de informação e uma organização mais credível e segura.

É neste contexto que a Câmara Municipal do Porto (CMP) tem vindo a atuar, garantindo uma continuidade de projetos no âmbito dos quais acabou por surgir a oportunidade de abordar a temática da Preservação da Informação num Município como objeto da presente dissertação.

O projeto delineado teve como principal objetivo contribuir para a certificação do repositório digital da CMP, enquadrado, em termos gerais, na *Política de Gestão da Informação e das Tecnologias da Informação*, e, mais especificamente, na *Política de Preservação e Segurança da Informação*, identificando e desenvolvendo a estrutura documental de suporte à *Preservação da Informação digital* e o *Documento de Especificação de Requisitos* para o repositório digital confiável, enquadrado por uma proposta base de *Estratégia, Políticas e Plano de Preservação da Informação* da Câmara Municipal do Porto, na sua componente digital.

Este objetivo decorre da proposta elaborada no projeto de dissertação desenvolvido por Sousa (2013) e enquadra-se no modelo de *Segurança e Preservação da Informação na CMP* aí contemplado.

Constituíram, pois, objetivos específicos do projeto:

- Situar o processo de modernização administrativa em curso na CMP face aos mais recentes desenvolvimentos teóricos, políticos, técnicos e normativos no âmbito da Gestão e Preservação da Informação em meio digital;

- Sistematizar os casos de boas práticas em termos de definição de estratégia, políticas e planos de preservação da informação em meio digital aplicáveis a municípios (nacionais e internacionais);
- Elaborar a estrutura documental de suporte à definição e desenvolvimento da *Estratégia*, *Políticas* e *Plano de Preservação da Informação Digital* da CMP.
- Apoiar o desenvolvimento *do Documento de Especificação de Requisitos* com vista à criação do Repositório Digital Certificável da CMP, que terá como principal documento orientador a norma ISO 16363:2012 – *Space Data and Information Transfer Systems: Audit and Certification of Trustworthy Digital Repositories*;
- Apoiar o desenvolvimento do Anexo relativo à *Segurança e Gestão de Riscos* (Série ISO 27000 Information Security Management Systems (ISMS) e ISO 31000:2009 - Risk management – Principles and guidelines), a agregar à especificação do Plano de Segurança da Informação e ao programa de auditorias internas e externas;

Apresenta-se de seguida a árvore de objetivos que sintetiza os objetivos fixados.

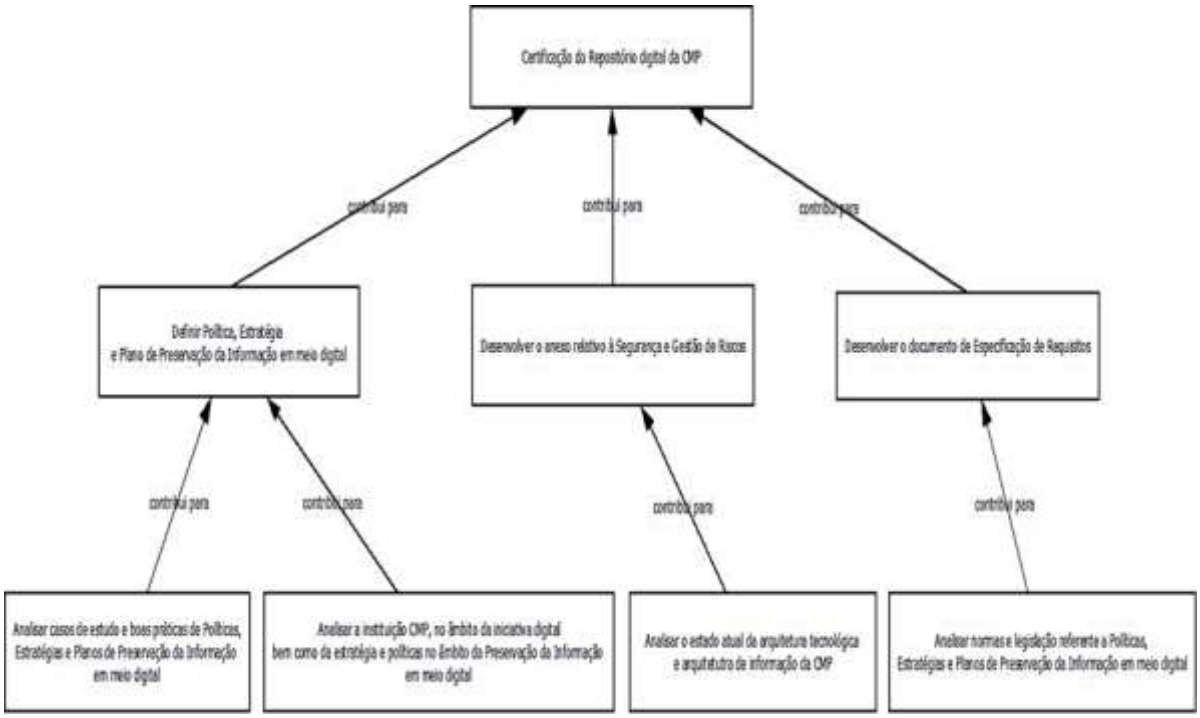


Ilustração 1 - Árvore de Objetivos

Face aos objetivos a que a CMP se propôs, relativamente à implementação de um Arquivo Digital Certificável com base na norma ISO 16363:2012 e especificamente direcionada à certificação de um repositório de informação digital, os primeiros

desenvolvimentos do projeto de dissertação evidenciaram a necessidade de focar o trabalho a realizar a montante e no contexto do referido repositório, tornando-se a análise da *estrutura documental de suporte* à *Preservação da Informação* um imperativo necessário para que aquele venha a ser uma realidade a médio prazo.

2. Problema de Investigação

O projeto a desenvolver visa estudar e responder a algumas das necessidades/problemas elencados para a 3ª fase da *Iniciativa de Modernização Administrativa* que vem sendo desenvolvida pelo Município do Porto, em alinhamento com as políticas nacionais e europeias aplicáveis à Administração Pública.

Uma iniciativa inscrita no *Sistema de Apoios à Modernização Administrativa* (SAMA), do Programa Operacional Fatores de Competitividade – COMPETE que visa apoiar a inovação e a qualidade dos serviços prestados ao cidadão e demais agentes, no seu relacionamento com o Município, bem como deste com os diversos níveis da estrutura da Administração Pública portuguesa em que se insere.

Nesse sentido, a candidatura do Município do Porto, recentemente aprovada, valorizou, sobretudo, a necessidade de garantir o processamento, a disponibilização, o acesso e o uso de informação de qualidade, pelo que o trabalho a desenvolver neste projeto situa-se no âmbito da definição da *Estratégia e Políticas de Gestão da Informação*, direcionando-se especificamente à *Preservação e Segurança da Informação*, com especial enfoque no meio digital e na operacionalização do *Arquivo Digital Certificado da CMP*, em estruturação.

Cientificamente visa-se contribuir para a demonstração aplicada da indissociabilidade de duas áreas afins, Ciência da Informação e Engenharia Informática, no âmbito específico do campo de estudos da Gestão da Informação (GI) na medida em que a Preservação da Informação é, nesta dissertação, assumida como variável da GI, encontrando-se presente ao longo de todo o ciclo de vida e gestão da informação e sendo essencial para a estruturação do Sistema de Informação Organizacional (SIO) da CMP.

A Administração Local, na qual se insere a CMP, para além dos desafios ao nível da inovação e da excelência nos serviços que presta, confronta-se com a premente "obrigação" de o fazer num contexto de redução de recursos (físicos, financeiros, etc.) e de pressão em termos da necessidade do uso intensivo da tecnologia.

Para além do desenvolvimento tecnológico, colocam-se cada vez mais questões de preservação e segurança da informação, sobretudo da existente em meio digital (com

documentos produzidos e recebidos digitalmente e outros digitalizados).

A Gestão da Informação, e particularmente a preservação da informação em meio digital, apresenta-se, pois, como uma preocupação a que a CMP procura dar resposta, tal como desde há muito o faz com os suportes tradicionais através da atuação dos serviços que integram o Arquivo Municipal da CMP em estreita articulação com os Serviços de informática do Município. O principal intuito consiste em prestar melhores serviços e assegurar procedimentos administrativos céleres e corretos apostando na gestão de um sistema de informação hibrido e cada vez mais dependente das plataformas tecnológicas.

Este é o contexto em que se insere o presente projeto de dissertação, direcionando-se especificamente à estruturação do Arquivo Digital da CMP a submeter a certificação, envolvendo esta a estrutura de gestão, as infraestruturas, o armazenamento, gestão e disponibilização da informação de acordo com os requisitos que garantam a confidencialidade, autenticidade, fidedignidade, integridade e inteligibilidade, isto é, provendo à gestão, preservação e segurança da informação no longo termo e o acesso continuado à mesma.

Nesse sentido, este projeto surge como o desenvolvimento natural de um anterior projeto que teve como principal objetivo a elaboração de uma proposta de *Modelo de Segurança e Preservação da Informação* aplicável às autarquias locais, através da conjugação das áreas da segurança e da preservação da informação, no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto (Sousa, 2013).

Como podemos verificar no modelo proposto por Sousa (2013) constata-se a importância e a inter-relação entre as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI que supervisiona a Comissão de Segurança e Preservação, colocando na sua base a cooperação entre a gestão dos sistemas tecnológicos de informação e a gestão da informação, uma visão holística e integrada dos planos a desenvolver, assim como a perspetivação quer em termos físicos (infraestruturas/suporte material), quer em termos lógicos.

Neste alinhamento as Políticas de Preservação apresentam-se com duas componentes – suportes tradicionais e meio digital – assumindo-se de forma cada vez mais efetiva a Preservação como variável da Gestão da Informação.

Se a componente ligada aos suportes tradicionais tem sido objeto de um intenso trabalho ao longo das últimas décadas, a preservação da informação em meio digital está a dar os primeiros passos, cabendo ao presente projeto de dissertação contribuir para o

desenvolvimento da estrutura documental de suporte à *Estratégia* e *Política de Preservação da Informação* e para a elaboração do *Plano de Preservação da Informação Digital* e, em última instância, para a criação de um repositório digital certificável.

A questão orientadora centra-se em aferir:

- Quais as estratégias, políticas, planos, procedimentos e requisitos a estabelecer tendo em vista a criação de um Repositório Digital Confiável, que garanta os atributos de autenticidade, integridade, inteligibilidade e de preservação da informação no longo prazo?

3. Abordagem teórica e metodológica

A abordagem a desenvolver no âmbito desta dissertação em Ciência da Informação, insere-se na área de estudos da Gestão da Informação (GI), assumindo a Preservação da Informação como uma variável da GI, direcionando-se concretamente à preservação da informação em meio digital, num contexto de certificação do repositório digital da CMP.

Como referência de investigação suportamo-nos no paradigma pós-custodial científico-informacional, recorrendo à Teoria Sistémica como ferramenta interpretativa e explicativa e tendo como referência metodológica o Método Quadripolar, proposto em 1974 por P. De Bruyne e outros autores para ser o instrumento operativo de uma dinâmica de investigação instauradora de um novo paradigma nas Ciências Humanas e Sociais e que foi adotado e sugerido como dispositivo metodológico global para a Ciência da Informação (Silva; Ribeiro, 2002).

O Método Quadripolar enquadrou e orientou tanto a dinâmica de estudo/pesquisa realizada como o trabalho que dela decorreu, com uma constante interação dos seus 4 pólos (pólo epistemológico, pólo teórico, pólo técnico e pólo morfológico) como se especifica de seguida.

No pólo epistemológico opera-se a permanente elaboração do objeto científico e a definição dos limites da problemática de investigação, neste caso em termos da definição do problema/necessidade e identificação dos paradigmas e dos critérios de cientificidade que orientam todo o processo. O problema apresentado situa, assim, este projeto na área de estudos da Gestão da Informação, no âmbito específico da preservação da informação em meio digital, perspetivado sob o novo *paradigma pós custodial e científico-informacional* que também tem orientado a própria atuação em termos de gestão da informação na CMP nos últimos anos.

No pólo teórico, centra-se a racionalidade do sujeito que conhece e aborda o objeto, assim como a postulação de leis, a formulação de hipóteses, teorias e conceitos operatórios e resultante confirmação do "contexto teórico" elaborado. Tomando como referência, o paradigma cientifico-informacional e os conceitos que o mesmo implica, partimos da abordagem da necessidade e problema e formulamos a questão já enunciada:

- Quais as estratégias, políticas, planos, procedimentos e requisitos a estabelecer tendo em vista a criação de um Repositório Digital Confiável, que garanta os atributos de autenticidade, integridade, inteligibilidade e de preservação da informação no longo prazo?

No pólo técnico, consuma-se, por via instrumental, o contacto com a realidade objetivada, tendo em vista a resolução do problema, sendo aqui que se desenvolvem operações fundamentais como a observação de casos e de variáveis, a avaliação retrospetiva e prospetiva ou a experimentação, ajustada ao campo de estudo de fenómenos humanos e sociais, tendo em vista a confirmação ou refutação das leis postuladas, das teorias elaboradas e dos conceitos operatórios formulados. Sendo este projeto de caráter prático, o principal enfoque neste pólo será inevitavelmente qualitativo. Pelas características do desafio e a transversalidade que envolve será desenvolvida a metodologia da investigação-ação dada a forma interativa como se desenvolve e permite a produção de saberes ao longo de todo o processo e a todo o grupo participativo (Coutinho, 2007). São duas vertentes que se jogam: a da investigação e a da ação procurando atingir resultados, quer no sentido de melhorar a compreensão sobre um determinado tema, quer na obtenção de resultados através da prática.

Como o próprio nome sugere, esta metodologia engloba duas vertentes, a da investigação e a da ação tendo como principal enfoque, a procura de obtenção de resultados, quer no sentido de melhorar a compreensão sobre um determinado tema, quer no alcançar de resultados através da prática.

Na opinião de Coutinho (2007), a Investigação-Ação tem um objetivo diferenciador em relação a outras metodologias que se prende com o facto de esta ser uma "produção teórica de saberes", onde é dada "grande importância à reformulação das práticas, embora as conclusões das investigações sejam necessárias para questionar a ação e lhe conferir sentido", tendo como finalidade "a solução de problemas".

Desta forma, podemos afirmar que esta investigação se centra num contexto da vida real, no campo de ação de uma organização.

Neste projeto as principais operações que integram este pólo são:

- Recolha de bibliografia em fontes diversificadas (bases de 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 de modelos teóricos e operacionais, nomeadamente o modelo SI-AP – Sistema [Integral] de Informação - Ativa e Permanente e os modelos normativos ISO 16363, ISO 27000 e ISO 31000;
- Identificação e análise de casos similares ao projeto em curso;
- Análise do contexto organizacional;
- Observação direta e participante do funcionamento da organização;
- Realização de entrevistas exploratórias (aos colaboradores e parceiros), que se revelarão importantes para o desenvolvimento eficaz do projeto;
- Identificação e análise de modelos de formulários internos e externos e de documentação de referência usados em âmbitos similares.

Por fim, sendo a gestão da informação a área de estudos desta dissertação será aplicado o Modelo de operacionalização designado por **SIAP**, inspirado na Teoria Sistémica no contexto do novo paradigma cientifico-informacional. Trata-se de um modelo que visa a constituição de um sistema com memória, potenciador do acesso e com enfoque especial na organização. Envolve uma lógica contínua da gestão do ciclo de vida da informação e no equilíbrio dos vértices: organicidade, funcionalidade e memória.

Finalmente, no pólo morfológico formalizam-se os resultados da investigação levada a cabo, através da representação do objeto em estudo e da exposição de todo o processo de pesquisa e análise que permitiu a construção científica em torno dele. Desta forma, pretende-se que os resultados sejam apresentados através de:

- Proposta de modelos de documentos de suporte à Estratégia, Políticas e Plano de Preservação da Informação da CMP, componente digital;
- Base do documento de Especificação de Requisitos com vista à criação do Repositório Digital Certificável da CMP;

4. Estrutura da dissertação

O presente documento compreende uma Introdução, quatro Capítulos e Conclusões e desenvolvimentos futuros.

Na Introdução é definida a problemática da investigação, a sua contextualização, bem como a motivação que levou à concretização da presente investigação, incidindo na importância da preservação e do acesso continuado à informação, mais concretamente à informação em meio digital, no longo prazo. São também expostos os objetivos e os resultados esperados, assim como a abordagem teórica e metodológica seguida para a sua elaboração.

O Capítulo 1 – *Das práticas à abordagem teórica e conceptual* – encontra-se dividido em 3 subcapítulos: *A preservação e a conservação: um percurso*; *A preservação digital: conceitos, problemas e estratégias* e, ainda, *A preservação como variável da Gestão da Informação*.

No primeiro subcapítulo, aborda-se a problemática da Preservação e da Conservação em particular expondo o percurso percorrido até à atualidade, nos subitens são abordados tanto os conceitos como os modelos empíricos onde se percebe que este não é um percurso simples, ou até mesmo linear, embora seja um percurso que acompanha a evolução da sociedade humana devendo hoje a Preservação ser assumida numa perspetiva sistémica e integrada.

No segundo subcapítulo é abordado a temática da *Preservação em meio digital*, mais particularmente conceitos, problemas e estratégias inerentes à área da *Preservação da Informação*, direcionando-se concretamente à preservação da informação em meio digital.

No terceiro subcapítulo é apresentada a *Preservação da Informação como variável da Gestão da Informação* sendo que nos subitens é descrita toda a base teórica da gestão da informação bem como a perspetiva integradora que propõe a assunção da Preservação da Informação como variável da Gestão da Informação, dada a sua incontornável presença ao longo de todo o ciclo de vida e de gestão da informação.

No Capítulo 2 – *O desafio do meio digital* – são expostos todo o contexto normativo necessário para a realização desta dissertação assim como um conjunto de guias de boas práticas que serão tidas como exemplos a seguir pelo Município do Porto, no contexto de certificação do repositório digital da CMP. Neste capítulo é, ainda, efetuada uma contextualização no quadro da Administração Pública portuguesa e referenciados casos de

boas práticas identificados em Municípios, tanto de âmbito internacional como nacional.

O Capítulo 3 - *O percurso da preservação da informação em meio digital na CMP* – apresenta o percurso que esta instituição desenvolveu no domínio da preservação da informação em meio digital, nomeadamente as iniciativas e os projetos existentes, o documento orientador criado no âmbito da certificação do repositório digital e ainda a primeira versão do *Modelo de Preservação e Segurança da Informação* (MP&SInf), desenvolvida em 2013.

No Capítulo 4 - *Contributo para o Modelo Estratégico de Preservação da Informação* – é apresentado todo o trabalho realizado no âmbito desta dissertação para a construção de um *Modelo Estratégico de Preservação da Informação* no quadro do MP&SInf.

Neste capítulo são enunciados os resultados do projeto, nomeadamente os elementos-base da componente digital, no âmbito da Gestão da Informação, sendo exposta a *Estrutura de "Serviços"* a prestar no âmbito da Gestão da Informação, o *Macroprocesso do 'Serviço de Gestão da Preservação' - Informação Digital* (que complementará o que existe na CMP para a Preservação de suportes tradicionais, por exemplo: pergaminho, papel e espécies fotográficas), o *Modelo de Preservação e Segurança da Informação* v.2, desenvolvido com base na investigação de Sousa (2013), a *Estrutura de Políticas e de Planos de Preservação e Segurança da Informação* e a estrutura e especificação dos *Documentos Base* para a respetiva especificação (os DSE), bem como o *Documento de Especificação de Requisitos* que suportará a certificação do *Repositório Digital Confiável da CMP*.

Este capítulo termina com a abordagem, a título exemplificativo, de dois casos práticos de produção informacional considerados prioritários no contexto da CMP, um em termos de especificação a desenvolver e outro que já resulta da adoção da estratégia de preservação de *normalização de formatos a ingerir no repositório digital*: 1) a recebida via email; 2) a adoção do formato PDF.

Por fim, nas *Conclusões* e perspetivas de trabalho futuro, são apresentadas as conclusões 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 Arquivo Digital Certificado.

1. Das práticas à abordagem teórica e conceptual

Na sociedade em que vivemos, seja ela denominada de Sociedade de Informação, Sociedade em Rede, ou mesmo Sociedade do Conhecimento, é sem dúvida alguma indiscutível a importância e impacto que as Tecnologias de Informação e Comunicação (TIC) têm nos diversos aspetos do nosso quotidiano, nomeadamente ao nível da Governação e de uma Administração Pública tradicionalmente associada à burocracia e à resistência à mudança.

Hoje, esta importância e impacto não podem deixar de ser considerados no âmbito mais alargado do "desafio digital". Este resulta de um progressivo processo de consciencialização que ocorreu ao longo da última década e que vem colocando o foco das atenções na necessidade de assegurar a preservação e o acesso continuado à informação digital no longo prazo, garantindo, em permanência, atributos fundamentais para a ação humana como: a confidencialidade, a disponibilidade, a autenticidade, a integridade, a inteligibilidade e a usabilidade da informação.

1.1. A Preservação e a conservação: um percurso

Olhando em retrospetiva, constatamos que ao longo da história da Humanidade, a produção informacional, isto é, a materialização das ideias e os registos necessários à vida em sociedade, fez-se utilizando vários suportes físicos, a que, apesar de todas as adversidades, ainda hoje podemos aceder, ultrapassadas as barreiras que uma diferente forma de escrita ou língua nos poderiam colocar mas que não interferiam com uma relação física e direta com o "objeto" documento e o acesso ao "escrito" (Pinto, 2013).

As TIC tornam-se parte integrante do quotidiano de indivíduos e organizações, afetando profundamente rotinas de trabalho, formas de relacionamento, quer pessoal quer a nível social, a que não escapa a relação do produtor de informação que cria, recebe, acumula, usa e dissemina essa informação.

Segundo Pinto (2013) e para "[...] melhor compreender e enfrentar os novos desafios impõe-se, pois, analisar retrospetivamente os problemas suscitados e as práticas desenvolvidas no âmbito da conservação".

Após um largo período de constante evolução e de profundas alterações e ruturas dos vínculos estabelecidos entre produtores e informação produzida/acumulada, passando pela institucionalização da função através de entidades custodiadoras, atinge-se, uma dimensão de cientificidade que enquadra e orienta um renovado modo de operação.

Este não foi um processo pacífico caracterizando-se por cisões que se solidificam "durante a primeira metade do séc. XX e que, quando confrontadas com o desafio digital, não deixarão de ter consequências, influenciando os posicionamentos e, consequentemente, as linhas de investigação e a definição de estratégias…" (Pinto, 2013).

Para Pinto (2013) isto significa "uma dinâmica que é indissociável, e decorrente, da complexidade de um desafio digital que ultrapassa delimitações consensualmente aceites na realidade analógica, bem como da crescente consciência da incapacidade individual para lhe fazer face".

1.1.1. Conceitos

Desta forma, torna-se necessário e pertinente clarificar os conceitos base de "Preservação" e "Conservação" e aferir em que medida estão associados a determinados tipos de serviços de informação ou tipo de profissional, bem como perspetivá-los à luz da Ciência da Informação.

Estes termos, que estão profundamente relacionados, "refletem conceitos ligados a um "saber fazer" e a práticas empíricas progressivamente adequadas à operacionalização de técnicas de conservação muito próximas das Ciências Naturais, sendo, ainda, muito comum a utilização indistinta dos termos preservação e conservação, bem como a existência de dificuldades em definir onde acaba a preservação e começa a conservação e onde acaba esta e começa o restauro" (Pinto, 2009).

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. No que respeita à **Conservação**, é mencionado 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).

De acordo com o Novo Dicionário do Livro, a **Preservação** é definida em duas aceções: a primeira aceção é "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 a segunda "Medidas coletivas e individuais tomadas no que respeita à reparação, restauro, proteção e manutenção do património bibliográfico". No que concerne à **Conservação** são apresentadas sete aceções: "1) 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; 2) 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; 3) Proteção; 4) Campo do conhecimento respeitante à coordenação e planeamento da aplicação prática das técnicas de encadernação, restauro, química do papel e outro material tecnológico, assim como outros conhecimentos relativos à preservação dos fundos arquivísticos; 5) Preservação; 6) Processo inicial de restauro; 7) Nome dado ao conjunto de processos que visam a estabilização mecânica e química dos materiais constituintes do documento gráfico" (Faria e Pericão, 1999 *apud* Pinto, 2009).

No ponto de vista da CI a **Preservação** é "intrínseca à função de Gestão, seja a nível institucional, seja a nível intermédio, 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" (Pinto, 2009). No que à **Conservação** diz respeito, esta toma contornos de cariz mais preventivo, onde são aplicadas técnicas e medidas, desenvolvendo "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).

1.1.2. Modelos Empíricos

Com a necessidade de registar a informação num suporte material, verifica-se, a necessidade de também a organizar, instalar e armazenar adequadamente, zelando pelos acervos por forma a garantir o acesso aos mesmos em diferentes períodos e, eventualmente, em lugares distintos. A relevância da proteção dos documentos – maioritariamente artefactos escritos [manuscritos] – foi-se afirmando ao longo do tempo como um âmbito de maior valor para os seus produtores e disseminadores.

De acordo com Pinto (2013) "Com a *Revolução da Tipografia/Imprensa*, não ocorrendo propriamente uma alteração do conjunto de signos utilizados e mantendo-se a situação do registro da informação diretamente num suporte material separado do sujeito, a

escrita passa da fase manuscrita para a fase impressa (essencialmente do "papel impresso") através da invenção da imprensa e da tipografia por Gutenberg em meados do século XV".

Desta forma o "modelo empírico" da proteção do "artefacto escrito" mantém-se em torno do "artefacto", sendo agora manuscrito e impresso.

Após o período da Revolução Francesa, emerge a associação da memória registada/memória escrita ao conceito operatório de "Património Documental", fruto das influências do romantismo, nacionalismo, historicismo e de reação ao industrialismo, especificando o "artefacto", manuscrito e impresso, como "artefacto cultural" que, associado à emergência do paradigma custodial e tecnicista, inscrevem no "modelo empírico" da proteção do artefacto escrito o pendor patrimonial, custodial e técnico, que caracterizará, até aos anos 70/80 do séc. XX, o emergente "modelo empírico" da conservação do "artefacto cultural escrito" (Pinto, 2013).

Na situação do pós 2ª Guerra Mundial e face ao progresso científico e técnico, numa atuação conjunta da UNESCO e das organizações de âmbito profissional como a IFLA e o CIA, são reconhecidos oficialmente os problemas mundiais ao nível da "Preservação e Conservação" (P&C). Segue, assim, "uma nova etapa na qual se passa do enfoque na "conservação" para o enfoque na P&C, aliando a efetivação prática dos dois conceitos, isto é, associar a definição estratégica à ação operacional, e enunciando o novo "modelo", ainda empírico, da P&C do "artefacto cultural escrito" (Pinto, 2013).

O "modelo" em que nos situamos nos dias de hoje é de um posicionamento em termos de "Preservação Sistémica" proposto por Pinto (2008, 2009, 2013), uma forma de perspetivação ainda em construção e que se sustenta numa visão holística e sistémica que assume a **Preservação como variável da Gestão da Informação**, assumindo de forma integrada o Sistema de Informação Organizacional (SIO), nomeadamente ultrapassando separações como digital *vs* "analógico" (tradicional), e o subjacente ciclo de vida e gestão da informação.

Modelos	Período
Proteção do "artefacto escrito"	Da antiguidade ao séc. XVIII
Conservação do "artefacto cultural escrito"	Séc. XVIII – anos 70 séc. XX
P&C do "artefacto cultural escrito"	Anos 70 séc. XX - início séc. XXI
Preservação Sistêmica	**Em construção na atualidade**

Ilustração 2 - Evolução dos modelos empíricos ao modelo teórico da preservação (Pinto, 2013)

De acordo com Pinto (2013), este é um percurso que não se mostra como simples, ou até mesmo linear, sendo que será ainda incorporada a complexidade intrínseca à afirmação da intervenção tecnológica, com consequências diretas no processo infocomunicacional.

Um percurso que acompanha a evolução da sociedade humana e que, em termos de Preservação da Informação, indica a relevante necessidade da assunção da complexa realidade indissociável da Informação e do "meio" digital em que é produzida, transmitida, armazenada e usada e no qual terá que ser preservada.

1.2. A Preservação em meio digital: conceitos, problemas e estratégias

A temática da designada "Preservação Digital" surge durante a década de 90 do séc. XX mas só na primeira década do século XXI adquire a relevância que o "desafio digital" exigia mas que tinha ainda que ultrapassar o nível "individual", "casuístico" e "específico" das abordagens entretanto efetuadas.

Bearman (2007) confrontado com a questão "Preservar o quê", na área da Herança Cultural, aponta a existência de quatro problemas essenciais na emergente área da Preservação Digital:

- As instituições individuais tentam preservar de acordo com os seus próprios critérios e área específica;
- Bibliotecas, arquivos, museus e cientistas da computação, não concordam sobre o que efetivamente estão a tentar preservar (conteúdo, contexto, forma ou função?);
- Para a herança cultural sobreviver, cada um necessitará de preservar todas as vistas do objeto;
- Às instituições individuais faltam conhecimento e competências para preservar a herança digital.

Por sua vez, Pinto (2010) traça um roteiro da Preservação na Era da Informação representando-o no PRESERVMAP, 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 perspetivada sistemicamente), refletindo o aparecimento das preocupações com a *Preservação Digital* a par da tradicional área da *Preservação e Conservação* (P&C) e a proposta de confluência que considera indispensável.

Ferreira (2011), centrado na preservação digital, refere que esta deixa de estar focada

em ações imediatas, como a preservação dos suportes, para se concentrar em ações a longo prazo e em infraestruturas técnicas e sociais que assegurem a perenidade dos documentos digitais.

Para compreender estas posições é fundamental perceber as abordagens que se vão desenvolvendo, nomeadamente as definições centradas na preservação em meio digital que emerge sob o conceito de "Preservação Digital" e que Pinto, numa perspetiva sistémica e de gestão integrada da informação referencia, em sentido especifico, sob a expressão "**Preservação em meio digital**", ou "Preservação da Informação Digital", sob o conceito geral de "**Preservação da Informação**".

Não se pode esquecer como referência o ano de 2003 e a adoção da *Carta para a Preservação do Património Digital* da UNESCO, na qual são identificados os recursos únicos fruto do saber ou da expressão dos seres humanos, compreendendo recursos de carácter cultural, educativo, científico ou administrativo e informação técnica, jurídica, médica e de outro tipo, que são gerados diretamente em formato digital ou a partir da conversão de material analógico já existente.

A UNESCO visa a proteção do Património, memória da humanidade, mas apela à mobilização de esforços em torno da "preservação digital" e chama a atenção para os **quatro "níveis" do "objeto digital",** e não só para a componente física (suporte material). Reforça-se, assim, a ideia de que a preservação em meio digital só se efetivará se organizações e indivíduos assumirem as suas responsabilidades neste âmbito, alertando para a importância da existência de um *programa de preservação digital*, e definindo-a como:

> "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 conceitual 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" (UNESCO, 2003).

Por sua vez o Conselho Internacional de Arquivos (CIA, 2005), dirigindo-se à comunidade arquivística, considera que o propósito da preservação digital será idêntico ao do analógico, no entanto, no caso do digital alguns aspetos das tarefas de preservação assumiriam uma maior importância e urgência mantendo como razões da preservação de documentos (records):

- O seu valor probatório (para demonstrar que ações foram ou não realizadas e que

decisões foram ou não tomadas, e não apenas no sentido do processo legal formalmente constituído);

- E a reutilização dos próprios documentos ou da informação que eles contêm (para potenciar as facilidades de acesso mas também cumprir os requisitos legais).

Como requisitos básicos para atingir os objetivos de preservação os documentos (records) deveriam ser: autênticos, completos, acessíveis e inteligíveis, processáveis e potencialmente reutilizáveis.

Em função desses objetivos, não se pretende preservar "*the behaviour and appearance of old computer software and hardware as a museum might want to do*" mas, mesmo que a opção tomada implique a alteração da aparência "*which still preserves its principal characteristics, its evidential value and the information within it can be considered adequate for our purpose*" (ICA, 2005 *apud* Pinto, 2013).

O CIA apresenta a ideia de "preservação a longo termo", incluindo a noção de preservação "permanente", a aplicação ao incorporado nos arquivos nacionais, a preservação por períodos determinados que ultrapassem o tempo de vida do *software* e do *hardware* (por exemplo condicionantes legais de 75 a 100 anos), a preservação por períodos de tempo indefinidos, mas não infinitos, que podem exceder os 5 anos.

No domínio das bibliotecas a ALA (*American Library Association*) refere "*Digital preservation combines policies, strategies and actions to ensure access to reformatted and born digital content regardless of the challenges of media failure and technological change. The goal of digital preservation is the accurate rendering of authenticated content over time* (ALA, 2007).

Para Ferreira (2006) a "preservação digital consiste na capacidade de garantir que a informação digital permanece acessível, interpretável e autêntica na presença de uma plataforma tecnológica diferente daquela que fora inicialmente utilizada no momento da sua criação".

A nível normativo a ISO/TR 18492:2005 incide no termo "preservação a longo termo que define como:

> "period of time that electronic document-based information is maintained as accessible and authentic evidence [...] This period of time can range between a few years to hundreds of years, depending upon the needs and requirements of the organization. For some organizations, this period of time would be determined by regulatory compliance, legal requirements and business needs. For other organizations, such as

archival repositories holding public records, the period of time required to retain electronic document-based information is usually thought to be hundreds of years" (ISO 18492, 2005).

A informação nado-digital, ou seja, produzida, recebida, armazenada e acedida exclusivamente em meio digital, tem que ser mantida no meio digital, apesar deste ser crescentemente assumido como frágil e volátil, possuindo ciclos de obsolescência extremamente rápidos o que adensa os problemas em torno da preservação da informação em todo o seu ciclo de vida (Sousa, 2013).

Sousa (2013) refere que a preservação da informação em meio digital "é um requisito e condição vital para qualquer serviço, dado que se tem assistido ao crescimento exponencial da informação em formato digital e, consequentemente, à necessidade de garantir o seu armazenamento e acesso, assegurando a acessibilidade, integridade, autenticidade, preservação a longo prazo e inteligibilidade".

De facto, e após análise das muitas das definições encontradas para o termo de preservação digital (expressão mais corrente existente na bibliografia, sendo nossa opção o uso do termo "preservação da informação em meio digital"), podemos perceber que todas têm em comum o facto de enfatizarem o armazenamento e a acessibilidade, a necessidade de garantir os atributos considerados essenciais dos documentos/objetos digitais, o facto de serem indispensáveis plataformas tecnológicas distintas daquelas que são utilizadas aquando da criação do documento original e a complexidade que envolve mas que ainda não estará a ser bem compreendida.

A dificuldade fundamental da preservação da informação em meio digital advém da natureza dos próprios "objetos" que são para preservar. Diferentemente dos formatos tradicionais, os "objetos" digitais são acessíveis somente através de combinações específicas de componentes de *hardware* e *software*. Até há bem pouco tempo atrás, a atenção dos profissionais da informação concentrava-se, apenas, na longevidade do suporte físico onde a informação era armazenada, mas com o aumento exponencial das tecnologias, esse posicionamento nos dias correntes deixa de ser suficiente. Mesmo nas melhores condições de armazenamento, o meio digital pode ter o seu ciclo de vida descontinuado pela falta ou inadequação de qualquer um dos demais componentes (Thomaz e Soares, 2004).

De acordo com Lusenet (2001, *apud* Thomaz e Soares, 2004), para compreender o conjunto de problemas associados à preservação da informação em meio digital é preciso, principalmente e antes de mais nada, consciencializarmo-nos que:

- "Os meios digitais são suportes transitórios que prestam sua função somente por um

período limitado de tempo e que a transferência para novos meios é absolutamente necessário;

- O *software* e o *hardware* tornam-se obsoletos em questão de anos, ao invés de décadas, e que embora as versões sucessivas de programas possam ser compatíveis, os fabricantes de *software* normalmente não garantem a compatibilidade por um longo período de tempo;
- O *software* pago é problemático não apenas porque é protegido e o código fonte não está disponível mas, também, porque normalmente está documentado de forma inadequada tornando a conversão de dados muito mais complexa" (Lusenet, 2001, apud Thomaz e Soares, 2004).

No que diz respeito ao futuro estes são alguns dos fatores que afetam o nível de risco da preservação da informação no longo termo e o acesso continuado à mesma:

- Os suportes no qual é armazenada a informação - uma vez que são instáveis e com a possibilidade de se deteriorarem dentro de alguns anos ou décadas;
- Produção e registo de informação que requer combinações específicas de *hardware* e *software* - que no decorrer dos anos se tornam obsoletos, o que tornará impossível o acesso à mesma;
- Os formatos de ficheiro que evoluem ao longo do tempo – inviabilizando a garantia de interoperabilidade com os *software*s atuais;
- Os acidentes que possam ocorrer - como catástrofes naturais, incêndios, inundações, ou até "ataques" informáticos e vírus que podem danificar ou mesmo destruírem os conteúdos armazenados;
- As consequências da segurança ao nível tecnológico (barreiras ao acesso), nomeadamente, a proteção por senha, criptografia e outros dipositivos de segurança que poderão impedir o acesso contínuo para além das permissões para o qual foram projetados;
- A falta de um modelo eficaz, que potencie a recuperação da informação, devendo ser considerada a constante necessidade de identificação e descrição dos conteúdos digitais.

São, pois, inúmeros os problemas e desafios a enfrentar e que não passam apenas por medidas do foro informático/tecnológico para que, segundo Bearman (2007 *apud* Pinto, 2010):

> "the fundamental challenge we face is to move our efforts from the individual repository level to the systemic level. Our habit of focusing selection and preservation in individual institutions is a consequence of the characteristics of physical heritage. But this approach fails when applied to the digital heritage. I believe that most of the solutions we have developed to date and envisioned as future solutions to problems of preserving the digital heritage will not succeed because they attempt to solve a systemic problem with fixes applied institutionally" Bearman (2007 *apud* Pinto, 2010).

1.3. A Preservação da Informação como variável da Gestão da Informação

O ritmo a que a informação em meio digital é produzida obriga a não negligenciar o facto de a mutabilidade e a vulnerabilidade da informação em formato digital colocarem dificuldades nunca antes sentidas.

O que se pretende preservar envolve "qualquer informação que possa ser gerada em, ou convertida para uma sequência de dígitos binários, armazenada e recuperada sob controlo de um computador e que é tratada como uma unidade do ponto de vista da informação. Uma unidade de sentido (estruturada ou não) cuja produção, armazenamento e uso envolvem necessariamente a codificação de código humano para código binário (e vice-versa), o que a torna dependente do sistema tecnológico intermediário a partir do qual o processo de codificação/descodificação se opera" (Pinto, 2010).

Atualmente, o desafio que se coloca é precisamente o da gestão da informação em meio digital (Pinto, 2007a), onde a obsolescência tecnológica, visível a vários níveis (*hardware*, *software*, suportes de armazenamento, formatos, etc.) é um entre vários fatores a considerar.

De acordo com Pinto (2010), este problema suscita duas questões: a necessidade de garantir a inteligibilidade e o acesso continuado à informação, independentemente das mutações tecnológicas; a indissociável necessidade da inequívoca identificação do contexto de produção dessa informação e de intervenções subsequentes.

A unidade informacional exige que a preservação em meio digital assente numa pluridimensionalidade que integra: a **dimensão física**, a **dimensão lógica**, a **dimensão conceptual/intelectual** e a **dimensão essencial** (Pinto, 2009).

A **dimensão física** reporta aquando do registo da informação em diversos suportes materiais - magnéticos (cassetes VHS, cassetes de música, etc.), óticos (CD-ROM's, DVD's, etc.) – convocando a **dimensão lógica**, dada a utilização de diversificadíssimos formatos (inteligíveis para a "máquina"), envolvendo, assim, a utilização de aplicações de *hardware* e

software através das quais seja possível aceder e ler/descodificar a informação (Pinto, 2009).

A **dimensão conceptual ou intelectual** reporta-se ao momento em que "o código adquire um significado para o ser humano, o que não acontece na dimensão lógica ou física" (Pinto, 2009).

Por fim, a **dimensão essencial** garante a perceção dos diferentes contextos de produção informacional, abarcando a salvaguarda de metainformação técnica, administrativa, descritiva e/ou estrutural, garantindo desta forma "a capacidade de a unidade informacional ser autodemonstrável, mantendo ligados a si, os elementos contextualizadores da sua produção e ciclo de vida, sob o ponto de vista ambiental – interno e externo, informacional, orgânico, funcional e tecnológico" (Pinto, 2009).

"…Quando falamos em Preservação, que assumimos como variável da GI, entramos no âmbito da definição da estratégia (seja a nível institucional, seja a nível intermédio) devendo ser pensada no longo prazo e em termos de políticas, planos e programas, recursos e estrutura orgânica/funcional e tecnológica que os suporte…" (Pinto, 2013).

Desta forma, é implícito o efetivo alinhamento da estratégia da Gestão da Informação (incluindo os requisitos da função Preservação) com a estratégia global da instituição e ainda com os contextos e ambiente externo em que esta está inserida.

Trata-se, pois, de uma abordagem que, face aos desafios da gestão de sistemas de informação inteiramente digitais ou híbridos, assume a preservação da informação como variável da gestão da informação, mantendo o enfoque no fenómeno e processo infocomunicacional, sustentada na teoria sistémica e corporizada no modelo interativo previsto no SI-AP.

Dada a constante evolução tecnológica, que afeta todas as dimensões, torna-se necessário garantir não uma mas várias estratégias de preservação a longo prazo. A interligação de todas as dimensões torna-se na garantia básica para a existência de informação de qualidade e inteligível, não sendo possível deixar de considerar a gestão integrada e interdisciplinar de todo o ciclo de vida da informação, conscientes de ciclos de obsolescência cada vez mais rápidos e que suscitam riscos e custos de preservação cada vez mais elevados (Pinto, 2010).

Torna-se necessário atuar ao nível da cultura, políticas, estratégias e planos que nas organizações assumam e integrem a preservação de informação, sob o risco da informação ser definitivamente perdida.

Pinto (2010) considera que "não deveremos, por isso, separar a preservação digital da

preservação analógica, sustentando distinções superficialmente criadas em função do suporte, mas assumir a complexidade do desafio, a diversidade de atores, bem como a multiplicidade de "produtos informacionais" e procurar colmatar a tendência para a existência de abordagens particulares da informação e dos sistemas de informação (por parte de arquivistas, bibliotecários, documentalistas ou mesmo de conservadores de museus), com as consequentes quebra e subvalorização de relações infocomunicacionais e do(s) contexto(s) em que ocorrem e a não potenciação do sistema de informação e da sua gestão" (Pinto, 2010).

1.3.1. A Gestão da Informação

A temática em análise torna fundamental a identificação e definição de alguns conceitos como é o caso dos conceitos operatórios estruturantes de "informação", "sistema de informação", "sistema tecnológico de informação" e "gestão de informação", a par de conceitos específicos como o de "preservação da informação", "política de preservação", "plano de preservação" e "repositório digital".

No que respeita ao conceito de "Informação", na sociedade contemporânea a informação possui um caráter estratégico na medida em que é fundamental para o regular funcionamento das atividades desenvolvidas pelas organizações, sendo um recurso fundamental para a tomada de decisão e um valioso ativo organizacional.

O conceito base de que partimos para esta dissertação é o de "informação" definido como sendo *o conjunto estruturado de representações mentais e emocionais codificadas (signos e símbolos) e modeladas com/pela interacção 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, 2006).

No novo "meio digital" a informação é produzida e registada através da interposição tecnológica (a nível físico e lógico) e envolve conjuntos de signos inteligíveis pela "máquina" e pelo Homem (código binário e código humano) (Pinto, 2013). A informação é, assim, passível de registo em diferentes formatos e suportes materiais. Contudo, esse registo não segue a linearidade do manuscrito ou do impresso, assumindo o meio tecnológico (*hardware* e *software*) em que este ocorre uma relevância determinante.

A materialização da ação humana complexifica-se com a mediação tecnológica. À gestão do documento – informação registada num suporte - terá que se suceder uma gestão que atendendo a todo o seu ciclo de vida (que passa principalmente pelos processos básicos de produção/criação, organização, utilização, preservação armazenamento/transferência/ destruição …) contemple as várias dimensões referenciadas e que se configuram ao nível das

unidades informacionais: a física, a lógica, a conceptual e a essencial.

Assim, a Gestão da Informação (GI), constituindo numa perspetiva CI um dos seus campos de estudo, tem na sua origem um percurso evolutivo que se tem desenvolvido em crescendo e que se inicia no âmbito da Documentação, despertando progressivamente o interesse da comunidade académica e empresarial, sobretudo a partir da década de 1980 com a disseminação do uso de computadores, desde logo ao nível empresarial, impondo-se como algo fundamental para o eficiente e eficaz funcionamento das organizações cada vez mais dependentes do recurso/ativo "informação".

Wilson (2003) define a GI como "a aplicação dos princípios de gestão para a aquisição, organização, controlo, disseminação e uso de informação relevante para o funcionamento eficaz das organizações de todos os tipos."

Choo (2003) define-a como a gestão de processos para adquirir, criar, organizar, distribuir e utilizar informação exigindo a adoção e adesão aos princípios orientadores que incluem ativos de informação. A informação deve, portanto, ser disponibilizada e partilhada, sendo que a informação relevante para a organização, a preservar, deve ser gerida e mantida o mais eficazmente possível. O "[...] objetivo principal da Gestão de Informação 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" (Choo, 2003).

Segundo Gouveia (2004), a gestão da informação "agrupa os esforços organizacionais relacionados com o valor, o custo, a qualidade, a origem, a segurança, a propriedade, a distribuição, a fiabilidade, a adequação e a pertinência da informação como suporte da missão e objetivos de uma organização".

Nesta dissertação, assume-se o estudo da gestão da informação como campo de estudos da Ciência da Informação, indissociável da Organização e Representação da Informação e do Comportamento Informacional, dada a necessidade do enfoque científico na informação, fenómeno e processo, em todas as fases do seu ciclo de vida.

O conceito de Gestão da Informação encontra-se, assim, 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).

A GI tem no seu objeto científico – a informação - um recurso e ativo tido como de extrema importância para qualquer organização dado que reflete a atividade organizacional,

sendo a materialização/evidência dessa atividade, memória organizacional e imprescindível recurso de gestão.

Numa perspetiva sistémica, associado ao conceito de informação encontra-se o de "Sistema de Informação" (SI), reflexo da complexidade e natureza das organizações.

Segundo Luís Borges Gouveia (2000), o SI é assumido numa perspetiva tecnológica constituindo uma "[...] unidade de operação que engloba todos os subsistemas de computadores existentes na empresa para os mais diversos fins, e também as funções que, de alguma forma, se relacionam com o tratamento de informação (...) O sistema de informação abarca todo o tipo de sistemas de manipulação de informação, incluindo manuais, relatórios, fichas e outra documentação".

Já para 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" que distingue de Sistema Tecnológico de Informação (STI).

Beynon-Davies (2002) utiliza um termo aparentemente semelhante, o de Sistema de Tecnologia de Informação (STI) definindo-o como "um sistema técnico [...] uma coleção organizada de *hardware*, *software*, dados e tecnologia de comunicações projetado para suportar os aspetos de algum sistema de informação", assumindo o sistema de informação na aceção de sistema informático que Silva coloca sob a designação de STI (Pinto, 2010).

De acordo com Pinto (2010), alinhando com a proposta de Silva (2006), o STI "é assumido como a plataforma tecnológica - meio físico/lógico de suporte à produção, transmissão, armazenamento e acesso à informação que constitui o SI propriamente dito" acrescendo que independentemente de se tratar de um SI digital, híbrido ou analógico será este, que identifica a missão/necessidades da organização que o produz, acumula e usa e que norteia a função de gestão e os profissionais da informação por ela responsáveis.

Assim, para prover à produção, acumulação, uso e preservação do SI é imprescindível conhecer, compreender e representar o contexto organizacional para depois conhecer, compreender, organizar e representar o próprio sistema de informação e estar apto para o gerir, disponibilizar e preservar ao longo do tempo (Pinto, 2009).

Colocando o foco na informação e no processo infocomunicacional, Pinto (2010) propõe uma mudança que aproxima, por força do impacto das Tecnologias da Informação (TI), a Gestão da Informação de uma função tradicional – a Preservação e a Conservação – que, na última década assiste à afirmação da "Preservação Digital" corporizando-se a

tendência que tende a separar "analógico" e "digital", propondo a sua efetiva interatuação sustentada na abordagem da Preservação como variável da GI.

1.3.2. A Preservação da Informação: uma perspetiva integradora

Situando-nos na Era da Informação e no novo paradigma, podemos verificar que a área científica da CI compreende três campos de estudo fundamentais: o da Produção/Gestão da informação, o da Organização e Representação (instrumentos de pesquisa e metainformação) e o do Comportamento Informacional (necessidades, práticas de acesso e uso da informação nos mais diversos contextos), as quais se prolongam nos ramos disciplinares de aplicação teórico-prática como a arquivística e a biblioteconomia (Silva et al. 1999).

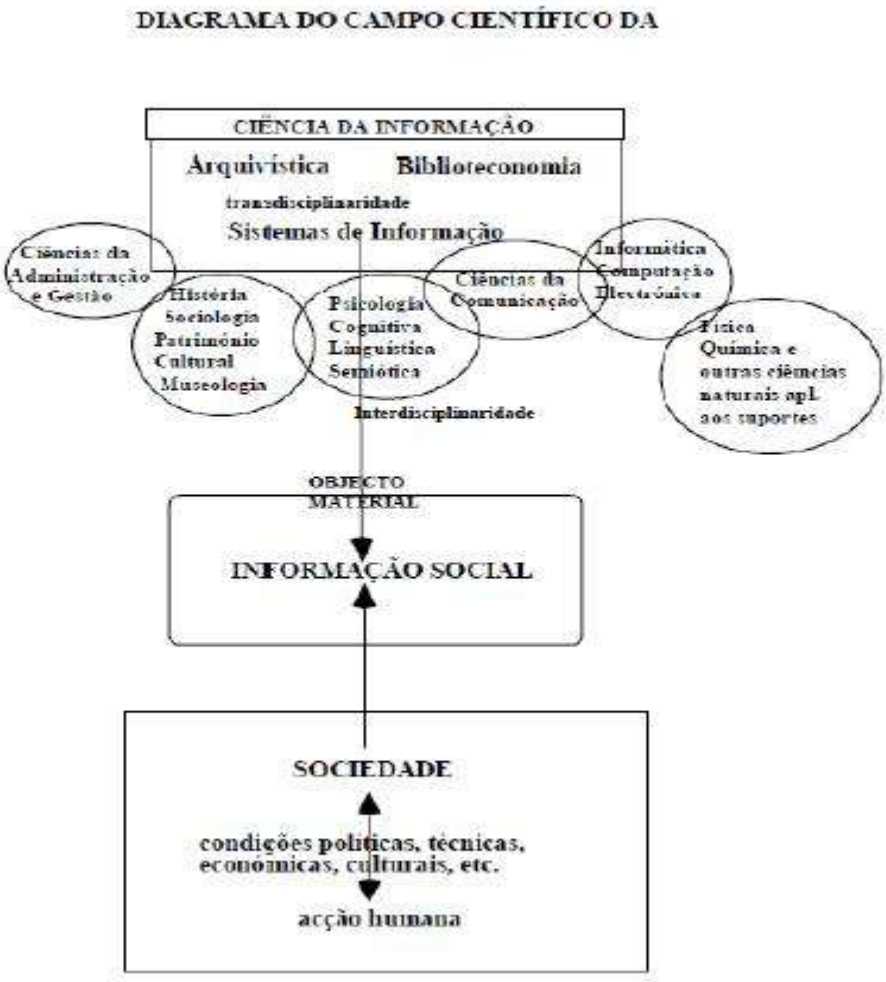


Ilustração 3 - Campo de estudos da CI (Silva, et al., 1999)

A gestão da informação, ao ser assumida como uma das áreas de estudo não prescinde do seu natural cruzamento ou interação com as outras áreas identificadas. Por um lado a área da produção tem uma relação direta com a organicidade (toda a informação é orgânica) e com o seu contexto organizacional, por outro, a Gestão da Informação assenta no ciclo de

operações e atos que vão, numa Organização/Empresa, da produção ao uso para tomada de decisões inteligentes.

Ora, numa abordagem transversal e holística e sendo a CI uma ciência social que investiga tudo o que se relacione com o fenómeno infocomunicacional (origem, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e uso da informação), tornam-se fundamentais as áreas específicas de investigação em CI: a produção de informação em qualquer contexto, as formas e estratégias funcionais de organização da informação pelos seus produtores e as complexas questões relacionadas com o fluxo e o uso da informação na busca/uso da informação necessária, comportamento informacional.

Partindo de uma Gestão da Informação cada vez mais integradora e direcionada à gestão de todas as fases do ciclo de vida da informação, Pinto (2010) propõe, assim, a assunção da Preservação da Informação como variável da gestão da informação dada a sua incontornável presença ao longo de todo o ciclo de vida e de gestão da informação, sobretudo quando está em causa a preservação da informação em meio digital que, por força da existência dominante de sistemas híbridos, em que suportes tradicionais e meio digital coabitam, tem que ser pensada e operacionalizada em função de ambos, convocando, uma vez mais, a perspetiva sistémica.

O ciclo de vida de qualquer unidade de informação (simples ou composta) é essencial para a sua preservação. A Preservação, variável da GI, é iniciada desde logo na conceção e implementação da plataforma tecnológica na qual será concebida, organizada, armazenada e disseminada a informação, nomeadamente no *software* utilizado, nos formatos adotados, na recolha, na fase e momento próprio, da metainformação administrativa, técnica, estrutural, descritiva ou de preservação que possibilite a sua futura referenciação e o desencadear das diferentes estratégias de preservação que agirão sobre as distintas dimensões, seja a bidimensionalidade do documento analógico, seja a pluridimensionalidade do "objeto" digital (Pinto, 2013).

Assim, a Gestão da Informação deverá considerar a informação na sua globalidade e complexidade apelando a uma preservação sistémica aos vários níveis e entre os vários níveis, a saber: nível da unidade informacional (informação e metainformação); nível do SI (seja digital, analógico ou híbrido); nível do STI (toda a arquitetura computacional), ao nível da organização (estrutura, processos, pessoas, SI e STI; contexto interno e externo); nível interorganizacional; nível nacional; ao nível global [...] a preservação começa 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 atempada da metainformação administrativa, técnica, estrutural, descritiva ou de preservação que permita a sua futura referenciação e o despoletar das diferentes estratégias de preservação que agirão sobre as diferentes dimensões, seja a bidimensionalidade do documento analógico, seja a pluridimensionalidade do "objeto" digital" (Pinto, 2009:350).

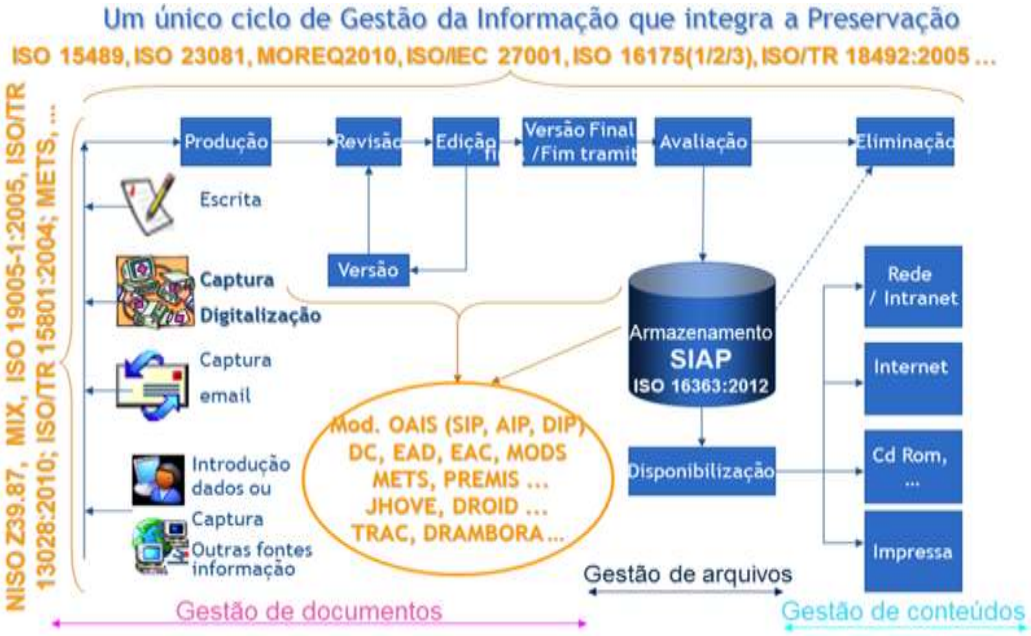


Ilustração 4 - Um único ciclo de gestão que integra a preservação (Pinto, 2014)

Como se constata na ilustração acima, desenvolve-se um **complexo processo integrado de gestão** que convoca conhecimento teórico, instrumentos, ferramentas e técnicas de operacionalização que estarão presentes ao longo de todo o ciclo de vida e gestão da informação, abarcando momentos que, ainda hoje, são frequentemente assumidos de forma segmentada e sem articulação entre si.

Desta forma, considera-se que o principal objetivo da preservação em meio digital, passa por assegurar que a informação contida no sistema de informação organizacional permaneça acessível, íntegra e autêntica ao longo do tempo, apelando assim a uma preservação sistémica a vários níveis e que atua nas diferentes fases do ciclo de vida e nas distintas dimensões da unidade de informação, seja a bidimensionalidade do documento analógico, seja a pluridimensionalidade da unidade de informação.

Desta forma, segundo Sousa (2013) podemos considerar a preservação em meio digital como um requisito e condição vital para qualquer serviço ou organização.

Uma posição que abordamos na perspetiva da Gestão da informação e do novo paradigma pós-custodial, científico e informacional, mas que supõe a reformulação de papéis

tradicionais, presentes em inúmeros serviços da Administração Pública, nomeadamente local, como é o caso do arquivista que Balcky (2011) referencia como custodiador de documentos ao serviço da investigação, mas que terá de se assumir como um **gestor e estruturador da informação**. Não basta organizar para disponibilizar, é fundamental conhecer a instituição enquanto entidade participante de um ambiente social com contexto, produtor de diversos tipos de informação e cujo fluxo determina os tipos de utilizadores que usam e necessitam daquela informação produzida.

2. O desafio do meio digital

2.1. Contexto normativo

O uso e o desenvolvimento de normas e modelos confiáveis têm feito parte das preocupações de profissionais da informação e da própria "indústria" da Informação, nomeadamente ao nível da mais recente área da preservação em meio digital com impacto, por exemplo, ao nível da organização e recuperação da informação e da interoperabilidade entre os diversos sistemas.

Convém atentar, no entanto, que no âmbito da Preservação a questão da normalização se pode colocar a dois níveis: a da normalização de formatos e o enquadramento normativo em geral.

A normalização de formatos é uma das várias estratégias a adotar ao nível da preservação em meio digital e a *Digital Preservation Coalition* aponta-lhe vantagens nomeadamente:

- Formatos padronizados são suscetíveis de apresentar menos problemas na migração de um formato para outro;
- Um número relativamente pequeno de formatos padrão será muito mais fácil de gerir, tanto a curto como longo prazo;
- Um amplo consenso sobre as normas irá facilitar e simplificar a colaboração em arquivo digital entre as instituições e setores (DPC, 2008:59);
- Contudo, não deixa de referenciar fatores que inibem o uso de normas como uma estratégia de preservação digital;
- O ritmo da mudança é tão rápida que as normas que tenham atingido o estágio de ser formalmente aprovado, inevitavelmente, ficam para trás podendo até ser substituídas;
- As pressões competitivas entre fornecedores favorece o desenvolvimento de extensões proprietárias para, ou implementações de normas, o que pode diluir as vantagens da consistência e interoperabilidade para a preservação;
- As próprias normas adaptam e alteram novos ambientes tecnológicos, conduzindo a uma série de variações do padrão original, que pode ou não ser compatível a longo prazo, mesmo se eles são compatíveis no curto prazo;

- As normas podem ser um recurso intensivo para implementar;
- Num ambiente mutável e altamente distribuído, é impossível as normas serem completamente prescritivas (DPC, 2008:59).

Os fatores enumerados acima significam que estas normas terão de ser vistas como parte de um conjunto de estratégias de preservação, não constituindo a própria estratégia, sendo que a necessidade de uma abordagem mais fluída tem levado ao aumento dos esforços para estabelecer as melhores práticas.

Esta é apenas uma referência geral na medida em que, não se direcionando esta dissertação de forma específica às estratégias de preservação e, de forma particular, à normalização de formatos, o foco principal a este nível centra-se na normalização em geral, abarcando aspetos diversificados e que interferem direta ou indiretamente com a preservação da informação no longo termo e o acesso continuado à mesma.

No panorama internacional foram surgindo normas, referências, projetos e especificações em que algumas instituições, sobretudo da Europa, Austrália e América do Norte têm desempenhado um papel de destaque na divulgação de procedimentos e boas práticas no que concerne à preservação em meio digital (Sousa, 2013).

Assim, um dos principais motivos para as organizações se regerem pelas normas, prende-se com o facto de estas serem modelos de referência e instrumento de padronização, sobretudo a nível operacional. Ao adotarmos estes padrões, estamos em consonância com metodologias e referenciais desenvolvidos, testados, estabelecidos e reconhecidos internacionalmente.

Num caso do quotidiano como é o da certificação (empresas, produtos, serviços, etc.) esta é um elemento-chave para que as organizações, públicas ou privadas, obtenham reconhecimento, ao apresentarem conformidade com os requisitos de uma determinada norma com impacto nacional e/ou internacional.

Vieira e Borbinha (2011) a propósito do estado da arte da "**Gestão de Documentos de Arquivo**[1]", apresentam como instrumentos normativos principais os referenciados no quadro abaixo:

[1] Definindo "Gestão de documentos e arquivo" como o "Campo da gestão responsável por um controlo eficiente e sistemático da produção, recepção, manutenção, utilização e destino dos documentos de arquivo, incluindo os processos para constituir e manter prova e informação sobre actividades e transacções" (ISO 15489-1 [NP 4438] apud Vieira e Borbinha, 2011), sendo "documento de arquivo" definido como o documento "[...] produzido, recebido e mantido a título probatório e informativo por uma organização ou pessoa, no cumprimento das suas obrigações legais ou condução das suas actividades" (ISO 15489-1 [NP 4438] apud Vieira e Borbinha, 2011).

Acrónimo - Nome	Entidade Responsável	Descrição
ISAD(G) - General International Standard Archival Description	ICA	Regras gerais de descrição arquivística que podem ser aplicadas independentemente do formato, de maneira a assegurarem a criação de descrições consistentes, apropriadas e auto-explicativas.
ISAAR(CPF) – International Archival Authority Record for Corporate Bodies, Persons and Families	ICA	Orientações para a preparação de registos de autoridade arquivística que proporcionam descrição das entidades (pessoas colectivas, pessoas singulares e famílias) associadas à produção e gestão de arquivos.
EAD – Encoded Archival Description	Library of Congress (EUA)	Elementos e atributos que permitem descrever colecções de arquivos e as suas estruturas num formato possível de ser lido por uma máquina.
EAC (CPF) – Encoded Archival Context – Corporate Bodies, Persons and Families	EAC Working Group	Elementos e atributos que permitem descrever informação sobre os criadores de material arquivístico assim como as circunstâncias em que esses materiais foram criados e usados.
NP4438/ISO15489 – Informação e Documentação – Gestão de Documentos de Arquivo	Instituto Português da Qualidade /ISO	Define como uma organização pode sistematicamente e efectivamente melhorar a sua gestão de documentos de arquivos. O objectivo da norma é facilitar o processo de criar recomendações, procedimentos e sistemas que suportem a gestão de documentos de arquivo em todos os seus formatos.
ISO16175 – Information and Documentation – Principles and Functional Requirements for Records in Electronic Office Environments	ISO	Conjunto de requisitos para SGDA. Os requisitos definidos na norma têm como objectivo definir os processos e requisitos para identificar e gerir documentos de arquivo em SGDA.
ISO26122 – Information and Documentation – Work Process Analysis for Records	ISO	Recomendações para a criação, captura e controlo de documentos de arquivo. Inclui a descrição de uma análise funcional (decomposição de funções em processos), e uma análise sequencial (investigação dos fluxos de transacções de negócio).
ISO/DIS 30300/30301 – Management Systems for Records	ISO	A norma 30300 define o vocabulário e conceitos principais enquanto a 30301 define os requisitos para sistemas de gestão de documentos de arquivo
Metodologia DIRKS	NAA (Austrália)	Metodologia de oito etapas desenhada para ajudar as organizações a melhorar a sua gestão de informação e documentos de arquivo. É uma abordagem estruturada e rigorosa desenhada para assegurar que a gestão de informação de uma organização é baseada nas necessidades de negócio da mesma.

Ilustração 5 - Gestão de Documentos de Arquivo (Vieira e Borbinha, 2011)

Um ponto de partida comum com o que elaborámos para o presente projeto de dissertação mas que, face aos objetivos redefinidos e fixados, teve que ser concebido de uma forma mais direcionada, na sequência do proposto por Pinto (2009, 2011, 2013), com o contributo do elenco já apresentado por Sousa (2013):

- **ISO 15489-1** - Information and documentation – Records Management Part 1: General [versão portuguesa NP 4438-1:2005] e Part 2: Guidelines [versão portuguesa NP 4438-2:2005];
- **ISO/TS 23081-1:2004** - Information and documentation – Records management processes - Metadata for records;
- **ISO 14721:2003** - Space data and information transfer systems. Open archival information system (OAIS);
- **ISO/TR 15801:2004** – Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability;
- **ISO 16363:2012** – Space data and information transfer systems – Audit and

certification of trustworthy digital repositories;

- **ISO/TR 18492:2005** - Long-term preservation of electronic document-based information;
- **ISO/TR 13028:2010** - Information and documentation: Implementation guidelines for digitization of records;
- **ISO/IEC 27001:2005** - Information technology. Security techniques. Information security management systems. Requirements;
- **MoReq2010** - Modular Requirements for Records Systems.

Neste enunciado de normas tem particular importância a norma ISO/TR 18492:2005, apesar de ser muito genérica, e, sobretudo, a ISO 16363:2012 que define um Guia de práticas recomendadas para fundamentar um processo de certificação e de auditoria para avaliar a confiabilidade de um repositório digital, no âmbito da preservação em meio digital, evidenciando a problemática em estudo neste projeto de dissertação e confirmando a inseparabilidade do tema da preservação em meio digital da existência de repositórios digitais confiáveis desenvolvidos com base em estratégias e políticas previamente estudadas, concebidas, aprovadas e implementadas.

Segundo esta norma, um repositório digital necessita de uma constante monitorização, planeamento, manutenção, bem como de uma estratégia de implementação para levar a cabo a sua missão, a preservação em meio digital.

Um repositório digital confiável não deve deixar de parte a implementação de ações e de uma estratégia consciente, e entender os riscos e ameaças a que os sistemas estão sujeitos. A norma faz ainda uma ressalva quanto ao estado de confiança que o repositório alcança, pois não se trata de uma realização única, dado que pressupõe auditorias regulares para que se possa averiguar a continuada conformidade (ISO 16363:2012).

Como observado anteriormente, os esforços no sentido de uma consolidação das políticas, estratégias, processos e procedimentos necessários para uma eficaz preservação, segurança e acesso continuado à informação, continuam a ser vastos, sendo as normas um aspeto a considerar, entre outros, sendo de sublinhar os pressupostos e modelo teórico-metodológico que permitirão o seu efetivo enquadramento e implementação.

A preservação da informação em meio digital é um requisito e condição vital para qualquer serviço, dado que se tem assistido ao crescimento exponencial da informação em formato digital e, consequentemente, à necessidade de prover ao seu armazenamento e acesso, garantindo acessibilidade, autenticidade, fidedignidade, integridade e inteligibilidade,

sem esquecer, no entanto, que não pode deixar de ser pensada em função da estratégia, políticas e plano geral de Preservação da Informação, no contexto da estratégia, política e plano de Gestão da Informação na Organização.

2.2. Guias de boas práticas

São várias as instituições e organizações identificadas na revisão da literatura, nomeadamente as propostas mais recentes da ISO, grupo de trabalho TC/46, da *Digital Preservation Coalition* (DPC), da *British Library*, dos *Archives New Zealand*, da *National Library of New Zealand*, dos *National Archives of Australia*, entre outras possíveis[2].

Como referimos muitas das normas resultam de boas práticas de âmbito nacional que são reconhecidas internacionalmente consagrando-se depois como instrumentos normativos como os produzidos pela ISO.

Na última década é visível o aumento dos esforços para definir toda uma gama de boas práticas, em particular na criação dos "recursos digitais", uma intervenção numa fase do ciclo de vida da informação que irá ajudar significativamente os esforços de preservação futura da informação digital.

Estes Guias, invariavelmente incluem, mas não estão limitados ao uso de normas devidamente apropriadas.

Os elementos comuns de boas práticas na criação incluem:

- O uso de formatos de dados abertos;
- O Fornecimento de metainformação em conformidade com os padrões emergentes e documentação destinada a facilitar o uso futuro e a gestão de recursos;

[2] Cf. ISO TC 46/SC 11/WG 7 - DIGITAL RECORDS PRESERVATION - Where to Start Guide, 2010; DPC - Preservation Management of Digital Materials: The Handbook"; SKINNER, Katherine; SCHULTZ, Matt (2010). A Guide to Distributed Digital Preservation. Atlanta: Educopia Institute. ISBN: 978-0-9826653-0-5. Consultado em 10 dez. 2013, Disponível em http://open.bu.edu/xmlui/bitstream/handle/2144/1351/GDDP_Educopia.pdf?sequence=1>; ARCHIVES NEW ZEALAND; NATIONAL LIBRARY OF NEW ZEALAND (2011). Digital Preservation Strategy. Consultado em 4 jan. 2014, Disponível em http://archives.govt.nz/sites/default/files/Digital_Preservation_Strategy.pdf>; NATIONAL ARCHIVES OF AUSTRALIA (2009) - Digital Preservation Policy: Preserving Archival Digital Records Transferred from Commonwealth Agencies. Consultado em 14 out. 2013, Disponível em http://www.naa.gov.au/about-us/organisation/accountability/operations-and-preservation/digital-preservation-policy.aspx; THE NATIONAL ARCHIVES, a). Digital Preservation Policy. Consultado em 24 out. 2013, Disponível em http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-preservation-policy.htm>; THE NATIONAL ARCHIVES, b). Digital Preservation Strategy. Consultado em 27 outubro 2013, Disponível em http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-preservation-strategy.htm>; THE NATIONAL ARCHIVES, c). Guidance. Consultado em 28 out. 2013, Disponível em http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm>; THE NATIONAL ARCHIVES, d). Digital Archiving.
Consultado em 29 out. 2013, Disponível em http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-archiving.htm>

- A atribuição de nomes permanentes aos recursos digitais *online*;
- Aplicação de modelos conceptuais e de especificação de requisitos;

No documento publicado pela *Digital Records Preservation* (2010), é referido o porquê de nos devermos preocupar com a preservação de registos digitais, o tipo de ações que devem ser tomadas para que a sua preservação seja eficaz e eficiente, culminando com a explicação de como se deve implementar um plano de preservação para a informação em meio digital.

Já a *Digital Preservation Coalition* (DPC) com a elaboração do seu manual fornece um guia internacional de autoridade e prática para o tema da *gestão dos recursos digitais* ao longo do tempo e os problemas na manutenção de acesso aos mesmos. Este manual aborda a preservação em meio digital onde são referidas questões sobre as alterações na tecnologia, os custos, as estratégias a seguir e assuntos legais, como os direitos de autor.

Os *Archives New Zealand* e a *National Library of New Zealand* identificaram a preservação de conteúdos digitais como uma área de interesse comum e a necessidade de novos métodos de gestão e cuidados para melhor servir a referida preservação. Para tal desenvolveram em conjunto um documento onde definem uma *Estratégia de Preservação Digital* para o património documental digital e arquivos públicos da Nova Zelândia, que afirma o compromisso de ambas as organizações para garantir que o conteúdo digital no seu atendimento é gerido e preservado de uma forma que reflete seu *status* como um ativo da Nova Zelândia (*Archives New Zealand; National Library of New Zealand*, 2011).

Num outro caso, a *British Library* e os *National Archives of Australia*, adotaram o modelo de referência OAIS ou tiveram o modelo em conta nas especificações dos seus sistemas. Este último no seu documento com a *Política de Preservação Digital*, aborda temas como os desafios para a preservação em meio digital de registos, as abordagens e os princípios da preservação em meio digital e ainda as características essenciais dos registos digitais a serem preservados (*National Archives of Australia*, 2009).

Os *National Archives of Australia* (2009) são responsáveis pela preservação dos "*records*" (registos) da Commonwealth que constituem os respetivos recursos de arquivo. Estes incluem registos nado-digitais e a preservação digital de cópias de originais de documentos analógicos. Este Arquivo só aceita a informação de entidades governamentais que tenham sido avaliados e selecionados[3] para a retenção permanente. Em circunstâncias excecionais, os Arquivos Nacionais da Austrália, aceitam informação cujo valor não foi identificado, por exemplo que está em risco ou que é considerada um recurso significativo.

[3] Com base em instrumentos de decisão sobre a manutenção, destruição ou transferência de um *record*.

Desta forma, o principal objetivo de se estabelecer uma política de preservação digital neste arquivo é preservar qualquer tipo de registo em meio digital que seja criado em qualquer plataforma de computação, criado usando qualquer tipo de aplicação, entregue em qualquer tipo de meio digital, de qualquer entidade da Commonwealth, proporcionando a pesquisa e o seu acesso, não só à atual como também às futuras gerações.

De acordo com a DPC "*There is still some distance to go before best practice in all aspects of digital preservation can be definitively articulated and in such a rapidly changing environment it may never be categorically established*" (DPC, 2008:60).

2.3. Pensar, planear e gerir a Preservação

Na perspetiva da Ciência da Informação, e apoiados num modelo de GI que engloba a preservação sistémica, sistemática e ativa, o conceito de "Preservação" implica dois planos interrelacionados:

- [...] a **componente estratégica e de gestão**, que convoca a preservação - gestão da preservação - envolvendo a adoção de políticas e medidas de gestão para a preservação (de âmbito público e/ou privado), através de instrumentos legais e normativos, organismos regulamentadores e fiscalizadores, bem como regulamentação, normas de funcionamento interno e planos das Instituições/Organizações, cuja elaboração e aplicação obedeceu e obedecerá aos ditames da "intencionalidade orgânica de preservar para usar face a necessidades e imperativos orgânico-funcionais vários" (Silva, 2006);
- a **componente operaciona**l que, como exposto, convoca a conservação e a aplicação dos procedimentos, medidas e técnicas e o desenvolvimento de ações de proteção da informação/documento, que, cada vez mais, se desenvolverão em pleno contexto de produção do S.I. e cujo início será indissociável da própria conceção e utilização do S.T.I." (Pinto, 2009, 2011).

Neste projeto de dissertação, estará particularmente em foco a **componente estratégica e de gestão** na medida em que se direciona à produção de contributos para o delinear das Políticas, Estratégias e do próprio Plano de Preservação da Informação em meio digital, constituindo este, a par do Plano relativo à informação em suportes "analógicos", um dos componentes das Políticas, Estratégias e Plano de Preservação da Informação na CMP, decorrendo este das Políticas de Segurança e Preservação da Informação da CMP. Uma abordagem orientada, pois, para o meio digital.

a) Políticas e Estratégias de Preservação

O quadro normativo (ISO 27001:2005), que aborda os requisitos para um **Sistema de Gestão de Segurança da Informação** (SGSI), aponta como principais atributos da informação: a **Confidencialidade** (que pode ser entendida como a garantia de que a informação se encontra acessível apenas a pessoas com permissão/autorização); a **Integridade** (a proteção da exatidão da informação e prevenção contra a sua modificação não autorizada); a **Disponibilidade** (a garantia de que as pessoas com permissão/autorização têm acesso à informação).

Não obstante, existem outros atributos igualmente reconhecidos, dada a sua importância, nomeadamente: a **autenticidade**, a **responsabilidade**, o **não-repúdio** e a **confiabilidade.**

De modo a assegurar estes atributos, é necessário que se definam e implementem **Políticas de Preservação** adequadas que englobem todo o ciclo de vida da informação (conceção, produção, armazenamento, manutenção, avaliação/seleção e acesso aos recursos digitais). Estas políticas são parte integrante da **Política de Gestão da Informação** tendo esta que ser assumida nas **Políticas e Estratégias da Organização** e aceite por todos os responsáveis da mesma.

Já para Ferreira (2006), que se centra no "arquivo", a definição de uma *Política de Preservação* envolve, geralmente, todas as facetas de um arquivo e implica:

- A criação de políticas de avaliação e seleção de materiais;
- A identificação de esquemas de metainformação apropriados (metainformação 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 (Ferreira, 2006).

Na perspetiva dos *The National Archives* (UK) uma Política de Preservação Digital deve:

- Atribuir a responsabilidade e gestão da política a um membro sénior dentro da organização (ou seja, um diretor ou chefe de serviço);
- Indicar 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 registos (*records*[4]), a proteção de dados, a segurança da informação e a política de preservação para os analógicos;
- Apoiar a estratégia de preservação digital (The National Archives a).

Acresce, ainda, a definição de **Estratégia de Preservação Digital.** Esta deve incluir:

- Um mecanismo formal de aceitação de registos (*records)* incluindo uma norma aceite para formatos de ficheiro e níveis de descrição para os registos;
- Um processo seguro para a transferência de registos para armazenamento, garantindo uma gestão adequada (incluindo verificações de integridade);
- Mapear processos para capturar a metainformação descritiva numa base de dados pesquisável ligada aos registos, permitindo a estes permanecer localizáveis;
- Um mecanismo formal para fornecer aos utilizadores o conteúdo dos registos preservados no formato mais apropriado para o mesmo;
- Um rigoroso sistema de monitorização das atividades de preservação que possa produzir dados de auditoria utilizáveis;
- A extensão em que cada processo é utilizado vai depender do tamanho e da extensão da coleção (The National Archives, b).

Por seu lado a *British Library*, através do seu *Preservation Advisory Center* apresenta como definição:

> *"A preservation policy is an essential component of a collections management framework, regardless of the size of the collection or organisation. It sets out an organisation's approach to preservation, addressing the questions of what needs to be preserved, why, for what purpose, and for how long. The policy clarifies the responsibilities of all concerned, staff, volunteers and users alike. It enables organisations to set and validate priorities, and to review long-standing practices. Preservation strategies, work plans, procedures and processes should all follow from a preservation policy*" (British Library, 2013)

Acrescem, ainda, o que se consideram ser os pontos fortes de uma política de preservação e que se criam quando a política:

- *clarify the relationship between the organization's mission and preservation activity*
- *clarify the scope of preservation activity by identifying the collections to be*

[4] "*Information created, received, and maintained as evidence and informations by an organization or person, in pursuance of legal obligations or in the transaction of business*". (ISO 15489-1, 2001).

preserved, their significance and the desired retention period

- *act as a focal point for collaborative working across organizations and in some cases between organizations*
- *clarify relationships with other aspects of collections management such as collections acquisition, access and security*
- *provide a statement of accountability against which performance can be monitored*
- *demonstrate the organization's long-term commitment to its collections to funders and users, internal and external*
- *act as a communication tool, internally and externally*
- *provide a basis for the development of preservation strategy and preservation Programmes.*
- *provide a basis for establishing priorities and justifying investment*
- *demonstrate responsible stewardship for the benefit of current and future users*
- *explain to users why certain actions are taken and others are not"* (British Library, 2013).

Na perspetiva do repositório e segundo a norma ISO 16363:2012 – *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*, podemos definir *Política de Preservação* como sendo:

- uma declaração escrita, autorizada pela administração do repositório, que descreve a conduta a ser tomada pelo repositório para a preservação de objetos registados no mesmo, definição que quando aplicada a uma entidade como a CMP terá que ser perspetivada num âmbito mais alargado, como proposto por Sousa (2013).

É, também, referido na norma que a *Política de Preservação* terá que ser consistente com o *Plano Estratégico de Preservação*.

b) Plano de Preservação

De acordo com Becker e Rauber (2011), um **Plano de Preservação** define uma série de ações de preservação a ser tomada por uma instituição responsável, devido a um risco identificado para um determinado conjunto de objetos digitais. 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 de preservação, as estratégias de preservação e avaliadas a decisão resultante de uma estratégia, incluindo a fundamentação da decisão.

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

- Identificação;
- Estado e *Triggers;*
- Descrição do ambiente institucional;
- Descrição do acervo;
- Requisitos para a preservação;
- Evidência de decisão para uma estratégia de preservação;
- Custos;
- Funções e responsabilidades;
- Plano de Ação de Preservação.

Na perspetiva do repositório, o **Plano Estratégico de Preservação Digital** é definido pela ISO 16363:2012 como:

- Uma declaração por escrito, autorizada pela administração do repositório, que afirma as metas e objetivos para alcançar essa parte da missão do repositório preocupada com a preservação. Estes planos estratégicos podem incluir planos a longo e curto prazo.
- A missão do **planeamento de preservação** consiste em assegurar o acesso futuro a informação autêntica envolvendo um conjunto específico de objetos digitais e comunidades alvo, definindo as ações necessárias para a sua preservação (ISO 16363, 2012).

Na seguinte tabela pode-se observar os diferentes estados de desenvolvimento de um Plano e as possiveis situações que despoletam as necessidades e determinam as ações de Preservação.

Tabela 1 - Alertas, *Triggers* e Eventos (Adapt. de Becker, et al., 2009)

Alerta	Desencadeado pela entidade funcional OAIS	Evento (Exemplos)
Nova coleção / acervo	Administração Monitorizar a comunidade designada	Acordo para uma nova coleção Novo tipo de objeto em utilização Submissões frequentes de formatos inesperados
Perfil de coleção alterada	Monitorizar a comunidade designada	Utilização de uma nova versão de um formato de objeto na comunidade designada Submissão frequente de formatos inesperados ou

Alerta	Desencadeado pela entidade funcional OAIS	Evento (Exemplos)
	Gestão de configuração do sistema (em Administração)	novas versões de um formato de objeto, ou objetos com novas funcionalidades / características. A Coleção cresce mais rápido do que o inicialmente previsto e especificado no plano de preservação existente
Mudança Ambiental	Monitorizar a Tecnologia Monitorizar a comunidade designada	Alteração nos resultados da avaliação dos objetivos de um plano de preservação existente, por exemplo, alterações de preços ou avaliação de risco alterada; Novas estratégias de preservação disponíveis por exemplo, novas versões de ferramentas e serviços; Iminente obsolescência da tecnologia utilizada, por exemplo, quando um formato de destino usado num plano de preservação baseado em migração está a tornar-se obsoleto. Mudança de *software* disponível nos locais dos utilizadores (por exemplo, indicado por relatórios sobre problemas com DIP's)
Mudança de Objetivos	Monitorizar a Tecnologia Monitorizar a comunidade designada Gestão de configuração do sistema (em Administração)	Novas normas que devem ser adotadas. Mudança na plataforma computacional ou nas tecnologias de comunicação utilizadas. Mudança na comunidade designada de consumidores ou comunidade produtora Mudança de políticas institucionais
Revisão periódica	Desenvolver Design de pacotes e planos de migração	Criados numa base agendada definida na política institucional ou no plano de preservação

De acordo com os autores Barbedo et al. (2010), em estudo realizado no âmbito das funções da então Direção-Geral de Arquivos (DGARQ), "o desenvolvimento de um plano de preservação digital e a seleção das estratégias apropriadas deve ser o resultado de um esforço de **colaboração entre as unidades orgânicas** referentes ao **arquivo** (gestão

documental) e à **informática** (tecnologias da informação), com a participação de todas as unidades orgânicas afetadas pelo processo ou que produzam informação eletrónica".

Segundo Barbedo et al. (2010) um *Plano de Preservação Digital* é um documento estratégico que contém políticas e procedimentos orientados para a constituição de uma estrutura técnica e organizacional que permita preservar de forma continuada documentos de arquivo eletrónicos (DAE) através de ações realizadas sobre os objetos digitais (OD) que os compõem, isto é, um plano visa garantir que a informação seja preservada de forma legível e acessível, mantendo simultaneamente as suas propriedades de autenticidade e integridade durante tanto tempo quanto a organização dela necessitar.

O *Plano de Preservação Digital* permitirá identificar quais as funcionalidades que devem ser implementadas e a forma de as implementar, para manter a integridade e usabilidade dos documentos de arquivo eletrónicos ao longo do tempo (Barbedo et al., 2010).

Ilustração 6 - Hierarquia da Política e Estratégia da Organização ao Plano Preservação Digital

Um *Plano de Preservação* deve traduzir uma *Política de Preservação*, especificar o tratamento do acervo/coleção num dado contexto institucional, deve estar preparado para a ocorrência de mudanças na tecnologia, no ambiente organizacional, nos requisitos do

utilizador, para alterações das ferramentas necessárias e para as mudanças da estratégia de preservação. O plano de preservação deve por fim conter uma ação concreta, pode ser uma definição de *workflow*, que detalhe as ações e o ambiente técnico que enquadra o desenvolvimento do processo de planeamento. O Plano de Preservação deve fornecer o contexto, ou seja, o *Plano de Ação de Preservação*.

No âmbito das entidades ligadas à Administração Central do Estado destacamos as propostas de Plano da atual Direção-Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB-PT), dos *National Archives of Austrália* (NAA-AU), dos *The National Archives* (TNA-UK), bem como instituições ligadas à investigação e serviços de informação como o *Council on Library and Information Resources*, (CLIR-US), a *Library of Congress* (LC-US) e a *British Library* (BL-UK), para além de entidades ligadas aos Municípios que se analisarão adiante.

Para garantir que o conteúdo digital permanece acessível e autêntico para os futuros utilizadores, o plano a ser criado tem de levar em conta as restrições legais e técnicas, tais como o espaço de armazenamento, infraestrutura e entrega, problemas de direitos de autor, os custos, as necessidades dos utilizadores e características do objeto. Também não é possível deixar de referir que a preservação em meio digital implica custos significativos que devem ser analisados e previstos pela organização através do reforço orçamental, considerado adequado à situação diagnosticada aquando da elaboração do Plano de Preservação em meio Digital.

Com a investigação que se desenvolveu em torno desta temática surgiram ferramentas que apoiam algumas das tarefas e processos, nomeadamente ao nível do *Processo de Planeamento da Preservação* com a ferramenta **PLATO**.

Esta ferramenta visa apoiar a tomada de decisão no âmbito da implementação de um processo de planeamento de preservação e integra serviços para a caracterização do conteúdo, ações de preservação e comparação automática de objetos numa arquitetura orientada a serviços para, assim, fornecer o máximo de apoio para o planeamento de preservação.

Estas funcionalidades permitem a tomada de decisões baseadas em evidências confiáveis, conforme requerido *pela Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC), atual norma **ISO 16363:2012**, que orienta operacionalmente este projeto.

O *Processo de Planeamento de Preservação* PLATO inclui quatro etapas distintas, cada uma com uma variedade de subetapas: “Definir Requisitos”, “Avaliar alternativas”, “Analisar os Resultados” e “Construir um Plano de Preservação”.

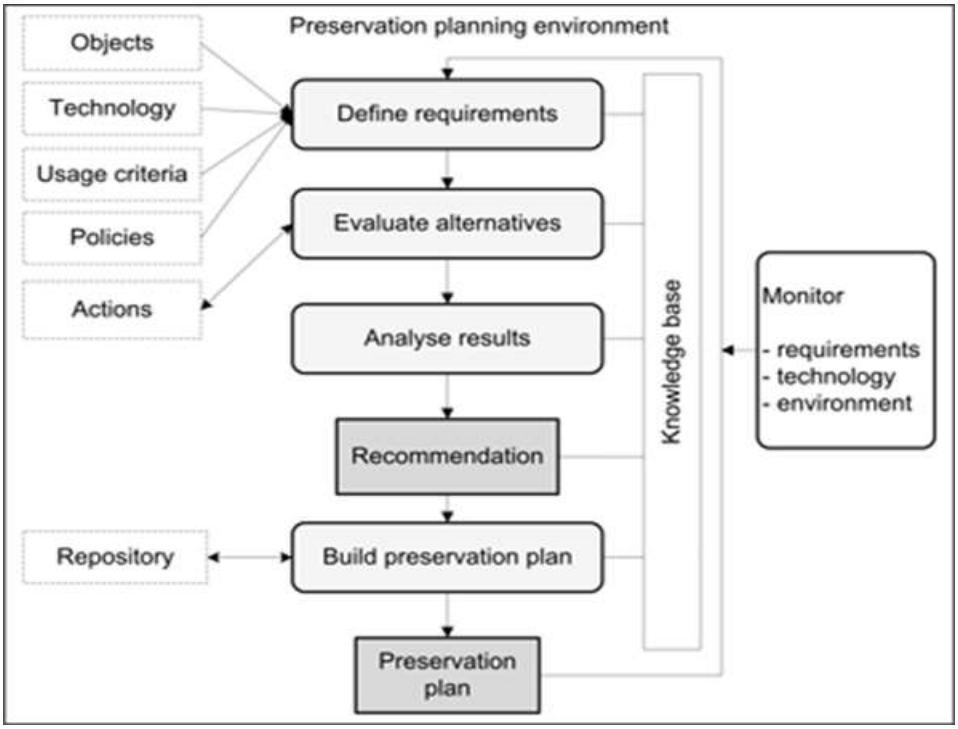


Ilustração 7 - Contexto do Planeamento da Preservação (PLATO) (Becker, et al., 2009)

Esta ferramenta, que na sequência deste projeto, será analisada e testada, permite especificar uma série de etapas ou ações (*Plano de Ação de Preservação*), juntamente com as *responsabilidades*, as *regras* e *requisitos* a aplicar a um determinado conjunto de ativos de informação.

Desta forma, um *Plano de Preservação* deve conter uma identificação, um *estado* que deve incluir a razão para a elaboração do plano. Caso tenha sido aprovado deve conter a informação de quando e por quem teve a *aprovação,* e ainda deve incluir a ligação a outros *planos relacionados*. O plano deve ainda conter uma *descrição do ambiente institucional*, uma *descrição da coleção* ("objetos digitais"), o *objetivo e requisitos* e a *evidência de decisão* para uma ação de *preservação específica*.

O planeamento adequado deve levar em consideração todos os fatores relevantes, incluindo:

- Políticas de preservação institucionais que fornecem restrições e drivers para o planeamento de preservação operacional.
- A obrigação legal da instituição.
- Requisitos institucionais, por exemplo cobrir o acesso a coleções e segurança.
- Constrangimentos institucionais, como o pessoal limitado ou recurso financeiro, ou limitações técnicas.

Após a conclusão do processo de planeamento, esta ferramenta produz um plano de preservação que contém:

- Informação contextual, incluindo a razão para a criação do plano, o contexto institucional e uma descrição da coleção.
- Evidências descrevendo as estratégias de preservação avaliadas e dando a razão para a decisão de escolher uma estratégia particular.
- Uma série de passos ou ações, chamado de Plano de Ação de Preservação.
- Funções, responsabilidades, regras e condições para a execução da coleta.
- Um Plano de Preservação executável que pode ser implantado.

A chave para um processo de planeamento mais simples e mais eficiente é a capacidade de importar as informações relevantes de outras fontes para apoiar ou automatizar o processo de tomada de decisão. Por exemplo:

- Uma ativação da Visão fornece o planeador com as informações necessárias para começar o planeamento (por exemplo, as políticas de controlo e definir o conteúdo em questão).
- O Modelo de política contém informações descrevendo o contexto institucional que pode ser aplicado no primeiro passo de planeamento.
- Políticas de controlo descrevem os requisitos sobre os objetos, que são usadas para derivar critérios de decisão.
- Um perfil de conteúdo XML pode ser carregado que completa a página do Plato "definir amostras".

Como podemos observar, a ilustração 8 exibe o *workflow* do processo de planeamento e mostra também os passos concretos dentro dos 4 principais fluxos de trabalho de alto nível que passamos a especificar:

- **Definir requisitos**: A primeira fase do fluxo de trabalho estabelece as pedras angulares do esforço de planeamento. Ela começa com a recolha e a documentar os fatores de influência e restrições sobre as possíveis ações e procedimentos. Em seguida, descreve o conjunto de objetos sob consideração e, finalmente, define o conjunto completo de requisitos a serem levados em conta;
- **Avaliar alternativas**: A segunda fase do fluxo de trabalho do planeamento baseia-se na experimentação controlada. Avalia as ações potenciais de forma quantitativa, aplicando-lhes o conteúdo da amostra previamente definido e analisando os

resultados com relação aos requisitos especificados na árvore de objetivos. Este processo de avaliação empírica resulta numa base de evidências que sustenta as decisões a serem tomadas nas fases sucessivas**;**

- **Análise de Resultados:** Na terceira fase, são analisados os resultados da experiência, agregados e consolidados em três etapas: transformar os valores medidos, definir os fatores de importância e analisar os resultados;
- **Construir Plano de Preservação:** Na quarta e última fase deste workflow de planeamento, é criado um plano de preservação, com base na decisão para uma ação de preservação. Este especifica uma série de etapas ou ações concretas, juntamente com responsabilidades organizacionais, regras e condições para a execução da ação de preservação na coleção.

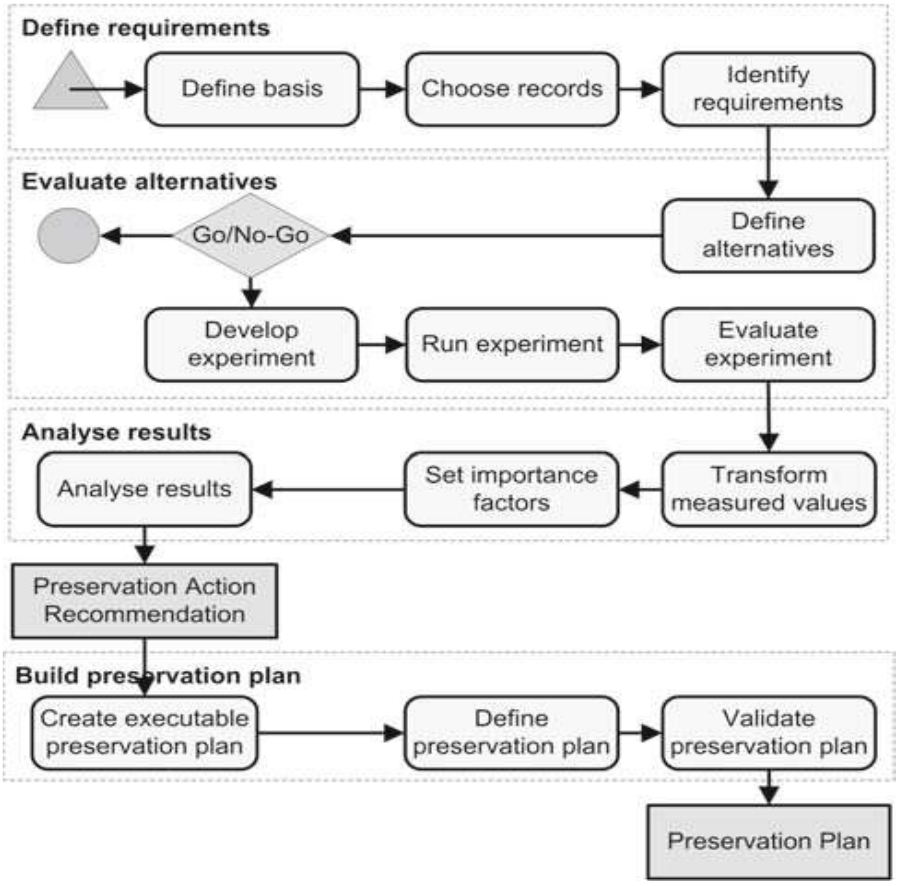


Ilustração 8 - *Workflow* do processo de planeamento (Becker, et al., 2009)

É também importante referir que para a construção de um Plano de Preservação da informação, existem determinados fatores que devem ser considerados aquando da sua elaboração. Como podemos constatar pela ilustração 9, identificam-se fatores como a tecnologia, normas e políticas e as próprias características dos objetos digitais, sendo

requisitos essenciais para a Preservação destes objetos.

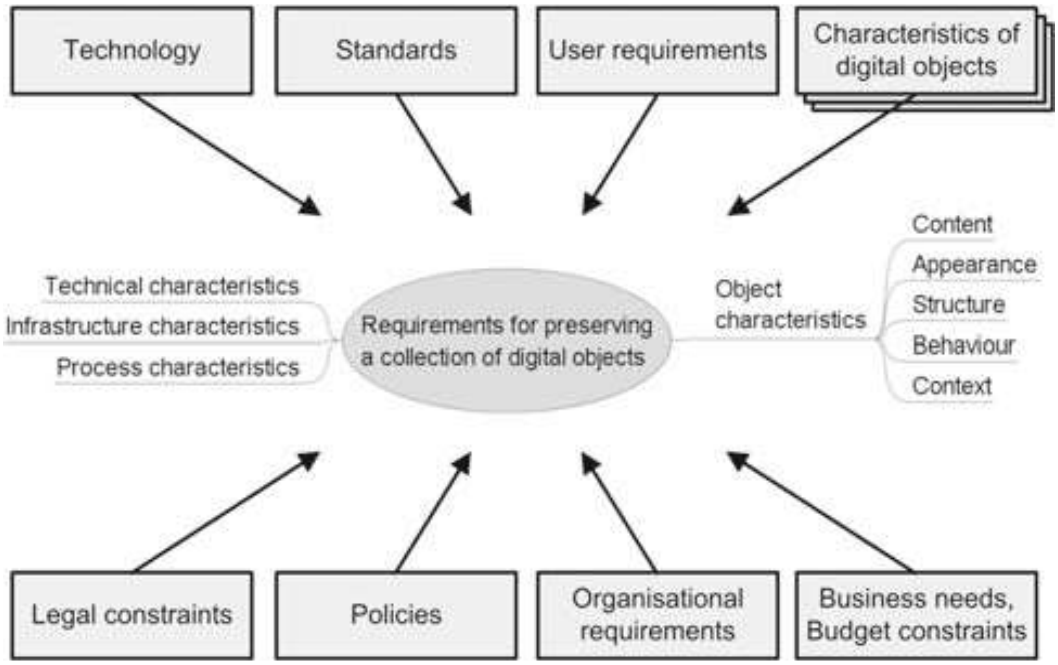


Ilustração 9 - Fatores de Influência (Becker, et al., 2009)

O resultado final é um plano de preservação completamente especificado, validado e aprovado formalmente, definindo etapas e responsabilidades concretas para manter um certo conjunto de objetos vivos. O plano inclui a base de evidência completa de tomada de decisão e em conformidade com a definição do plano.

2.4. O Contexto da Administração Pública Portuguesa

O uso das Tecnologias de Informação e Comunicação (TIC), e, consequentemente a produção de informação em meio digital, têm crescido de forma exponencial na Administração Pública (AP), a nível central e local, em Portugal.

O *Plano Global Estratégico de Racionalização e Redução de custos* nas TIC (PGERRTIC, 2013) constitui o principal documento orientador, a nível nacional, no âmbito da utilização das TIC na Administração Pública portuguesa e no apoio ao governo eletrónico.

Esta é uma iniciativa, a nível nacional, que visa a redução de custos com as TIC na Administração Pública (AP), sendo a Agência para a Modernização Administrativa (AMA) responsável pela gestão operacional do Plano, que se insere no âmbito das iniciativas ligadas

à modernização administrativa e do governo eletrónico.

O Plano é constituído por 25 medidas que compreendem domínios tão diversos como a interoperabilidade na AP, a partilha e uniformização de *software*, o *Cloud Computing*, a Administração Aberta ou a racionalização dos Centros de Dados e a Central Eletrónica do Estado. Estas medidas têm um carácter transversal e terão impacto em toda a Administração Pública, assentando sobre 5 eixos estratégicos de racionalização:

- Melhoria dos mecanismos de *Governance*;
- Redução de custos;
- Estímulo ao crescimento económico;
- Implementação de soluções TIC comuns;
- Utilização das TIC para potenciar a mudança e a modernização administrativa.

Neste último eixo estratégico, encontra-se a **Interoperabilidade** na AP, sendo que para tal, foi previamente desenvolvida e aprovada a **Macroestrutura Funcional do Estado** (MEF), a nível central e depois adaptada à Administração Local (AL), o que nos remete para a articulação deste Plano com a ação da DGLAB (antiga DGARQ), que coordena a política arquivística nacional e busca uma aproximação aos organismos produtores de informação no contexto da AP.

As iniciativas do Governo Eletrónico determinam que a AP deve basear, cada vez mais, a sua atividade no processo de negócio eletrónico no intuito de agilizar processos e assegurar um serviço mais rápido, completo e transparente para o cidadão. Neste cenário tornou-se claro o crescimento da produção de "objetos digitais", informação que as entidades públicas pretendem ter assegurado o seu valor evidencial e de autenticidade.

Neste sentido a DGLAB tem promovido o desenvolvimento de processos, ferramentas e recursos que possam dar resposta às necessidades de preservação dos "objetos digitais" produzidos na Administração Pública e cuja preservação continuada seja considerada como justificada. As vias de atuação da DGLAB são quatro:

- O desenvolvimento de um arquivo digital com capacidade de integrar, gerir e disseminar os objetos digitais produzidos na Administração Pública;
- A produção de documentos técnicos e normativos que auxiliem as instituições a compreender, gerir e desenvolver ferramentas que viabilizem a preservação dos seus objetos digitais, domínio onde foi publicado as "Recomendações para a produção de planos de preservação digital";

- A intervenção na qualificação de "Sistemas de Arquivos";
- A construção de comunidades em torno da preservação do património digital com vista à exploração de recursos comuns.

Entre os instrumentos produzidos encontra-se a MEF. Esta consiste na proposta de uma estrutura de informação que pretende representar a uniformidade e a utilização da mesma linguagem pelas diferentes entidades da AP, isto é, consiste na estrutura base a utilizar para a organização da informação produzida, recebida e acumulada, nomeadamente, por todas as autarquias, procurando facilitar, desta forma, a partilha e recuperação de informação.

Na prática, pretende-se a utilização de um instrumento único (através da atribuição de um código funcional a cada série/documento), utilizado por qualquer entidade pública. A estrutura decompõe-se em duas instâncias: a de primeiro nível representa as *funções*, e a de segundo nível representa as *subfunções* em que as primeiras podem ser decompostas (Sousa, 2013).

A este respeito, na apresentação do Projeto MEF, foi salientada a importância desta ferramenta que funcionará em articulação com uma outra, a **MIP – Metainformação para a InteroPerabilidade**. A MIP visa facilitar "a interoperabilidade semântica na Administração Pública" (Lourenço, et al., 2013). Em paralelo, pretende garantir a uniformidade entre as regras de metainformação utilizadas nos municípios.

A aplicação destas duas ferramentas procura potenciar um maior aproveitamento dos recursos individuais, através da:

- Dinamização da interoperabilidade na administração, aumentando a reutilização da informação em diferentes contextos funcionais e orgânicos;
- Desenvolvimento da perceção organizacional de diferentes significados da informação produzida pelos organismos da administração;
- Aumento de eficiência induzido pelo aproveitamento de informação produzida e comunicada, a par da mais rápida compreensão dessa mesma informação e consequente resposta operacional empreendida em função da mesma (Lourenço, et al., 2013).

Este é, pois, um contexto que, numa perspetiva estratégica e operacional, não poderá ser ignorado ao formular as políticas, estratégias e plano de preservação no âmbito de um Município que, apesar da sua autonomia, se tem que integrar nas regras do funcionamento da Administração do Estado.

2.5. Casos de referência em Municípios

Existindo a nível nacional referências que mencionaremos adiante, no âmbito dos Municípios esta é uma área emergente pelo que se apresentam alguns dos casos de boas práticas, no panorama internacional, que serão analisados e avaliada a sua utilização como referência para o Município do Porto:

- *Sheffield Archives* (Reino Unido);
- *London Metropolitan Archives* (Reino Unido);
- *City of Vancouver* (Canadá).

Um dos pontos que capta mais atenção nestes casos é a ainda visível distinção da abordagem e análise diferenciada, aos vários níveis, entre documentos "analógicos" (suportes tradicionais) e documentos digitais, envolvendo entidades distintas e com missões distintas, embora sejam todos convergentes em termos de objetivo "procurar garantir a preservação e o acesso a longo prazo" da informação pela qual são responsáveis.

Estes casos apresentam aspetos em comum, em termos de Políticas e posicionamento estratégico, que são preenchidos consoante as necessidades de cada caso, nomeadamente:

- **Declaração de Visão / Declaração da Política** - Serve para demonstrar o alcance da Política de Preservação Digital.
- **Fundamentação** – a forma como se irá preservar e gerir os objetos digitais.
- **Âmbito** - Qual a área de atuação da política, ou seja, aquilo que a política cobre.
- **Objetivos** – Finalidades da Política de Preservação Digital
- **Formatos de ficheiros de dados/ Formatos de preservação** – especificação dos formatos de preservação dos ficheiros.
- **Características dos objetos digitais** – enumeração dos atributos de propriedades dos objetos digitais.
- **Abordagem à preservação digital** – a abordagem efetuada relativamente aos objetos digitais, como os processos utilizados (migração, normalização, etc.).
- **Armazenamento digital** – definição do sistema tecnológico que irá permitir a preservação dos objetos digitais.
- **Responsabilidades** – Indica as responsabilidades e funções dos elementos da equipa, de forma a responder aos requisitos presentes na ISO 16363:2012.

- **Normas, orientações e organizações** – indicação dos padrões, normas, e referenciais que servem de base à política de preservação.
- **Cooperação/colaboração** – comprometimento com outros organismos na promoção de ferramentas de preservação digital; estabelecimento de parcerias (Sousa, 2013).

Desta forma, destacamos um projeto de âmbito internacional, que servirá como guia de boas práticas no âmbito de preservação da informação em meio digital em autarquias, o da cidade de Vancouver no Canadá que desenvolveu uma estratégia digital, em que a sua visão era melhorar as ligações digitais multidirecionais entre os cidadãos, funcionários, empresas e o próprio governo.

Para a realização desta estratégia, foram identificados por base 4 pilares:

- **Compromisso + Acesso** – Como a cidade e os seus constituintes se envolvem uns com os outros, através de prestação de serviços transacionais, colaboração e comunicação.
- **Infraestrutura e Ativos** - Concentra-se em infraestrutura e ativos (*software*, *hardware* e dados) digitais.
- **Economia** - Centrada na economia digital no que diz respeito ao apoio ao crescimento do setor digital e permitir que todas as empresas beneficiem de infraestrutura e serviços digitais.
- **Maturidade Organizacional Digital** - Este engloba governação digital, permitindo que os funcionários da cidade tenham ferramentas que promovam tanto a cultura digital como a inovação.

Em cada um destes pilares identificados pela cidade de Vancouver existem iniciativas que são medidas para levar a cabo a estratégia digital implementada pela cidade.

As principais iniciativas do pilar **Compromisso + Acesso** são: ativar os serviços municipais através de plataformas digitais, expandir o programa de dados aberto e promover a atividade digital através de comunicações e ferramentas de acionamento. A iniciativa referente à **Infraestrutura e Ativos** é expandir o acesso digital em toda a cidade. Quanto ao pilar da **Economia** são três as iniciativas: estabelecer um programa de incubação digital, criar um ambiente regulatório favorável que propicia a indústria digital e com a ajuda de parceiros da comunidade e da indústria, apoiar uma prova ágil do conceito do programa. Por fim, no que diz respeito à **Maturidade Organizacional Digital**, as iniciativas são estabelecer serviços de governação digitais e ainda, a implementação de uma estratégia de

força de trabalho móvel.

No caso da cidade de Londres, os *London Metropolitan Archives* em conjunto com a *Guildhall Library Manuscripts* criaram um documento que especifica como os funcionários destas duas instituições, que existem para "coletar registos do rico passado histórico de Londres e de encontrar e coletar registos da vibrante e diversificada presente Londres, que são selecionados, catalogados, armazenados e permanentemente preservados para o uso e benefício das gerações presentes e futuras", deverão preservar e gerir os seus arquivos digitais.

Este documento, a *Política de Preservação Digital*, aborda vários tópicos, desde o armazenamento digital onde se fala da base quer tecnológica quer física de como preservar os documentos, os formatos de ficheiro que deverão ser utilizados, bem como as responsabilidades que deve haver ao nível das pessoas à frente deste projeto.

No que diz respeito aos *Sheffield Archives,* igualmente como os *London Metropolitan Archives* e a *Guildhall Library Manuscripts* elaboraram um documento sobre a *Política de Preservação Digital* no qual está descrito entre outros, a sua coleção de objetos digitais, a consequente avaliação, seleção e aquisição dos mesmos, questões relacionadas com o armazenamento, manutenção e o acesso a estes objetos, estabelecendo no final um comprometimento com outros organismos na promoção de ferramentas de preservação digital, nomeadamente com os *The National Archives* UK (TNA), Digital Preservation Coalition (DPC) e a *British Library* (BL).

Um contexto de atuação muito similar ao traçado pelo Município do Porto e no qual procuraremos identificar as políticas e estratégias delineadas em termos de preservação da informação digital, acrescendo-lhe os contributos colhidos com as experiências já consolidadas destes casos de referência.

3. O percurso da preservação da informação em meio digital na CMP

3.1. Iniciativas e projetos

As expectativas e exigências crescentes dos cidadãos face aos serviços públicos, aliadas ao desenvolvimento das tecnologias da informação, desafiam a administração pública a reorientar a oferta ao cidadão/empresa para a inovação dos serviços prestados, atendendo à sua eficiência e qualidade, assegurando a organização e a disponibilização de informação inteligente.

No seguimento da forte aposta feita, nos últimos anos, pela Câmara Municipal do Porto na melhoria da interação entre a autarquia e o cidadão/empresa, nomeadamente através da melhoria dos serviços prestados, importa agora dar continuidade ao processo, capacitando assim o cidadão, assumindo simultaneamente, opções inovadoras. Estas passam por tomar o território e a sua comunidade como elementos primordiais que fazem um esforço consciente para usar a tecnologia da informação, de modo a transformar a vida e o trabalho de forma significativa e fundamental.

Neste contexto e na senda da candidatura ao *Sistema de Apoios à Modernização Administrativa* (SAMA), do Programa Operacional Fatores de Competitividade – COMPETE, a CMP pretende, com a implementação de novas medidas e projetos a que intitulou **cap@CIDADE: inovar para o cidadão,** melhorar os serviços prestados aos cidadãos e empresas que interagem com o Município do Porto.

Importa referir que o Programa Operacional Fatores de Competitividade – COMPETE, "destina-se ao financiamento de projetos no âmbito do alinhamento estratégico, designadamente:

- Modernização da Administração Pública, tendo em conta a racionalização e redução de custos das TIC;
- Aumento da eficiência na Administração Pública na vertente dos processos e da interação com os cidadãos e as empresas;
- Contribuir para a melhoria da competitividade da economia regional;
- Contribuir para a prossecução dos objetivos estratégicos de modernização da

Administração Pública referidos no aviso de concurso nº 1/SAMA/2012."[5]

Os objetivos da operação prendem-se com o facto de, há muito, se sentir maiores exigências nos serviços públicos em servir bem o cidadão e as organizações, a que não escapa o forte aliado que são as tecnologias de informação e que retratam um fator de inovação e competitividade por excelência.

Assim sendo, este projeto tem como objetivos fundamentais:

- Capacitar os cidadãos, a administração e demais agentes para que, com a sua atuação, que se pretende cada vez mais integrada e colaborativa, fomentem a competitividade e o desenvolvimento;
- Disponibilizar serviços ao cidadão/empresa assentes num conceito de administração aberta, publicando e agregando informação produzida pela CMP, potenciando os serviços *online*;
- Sustentar a atuação da CMP e a sua prestação de serviços, numa base tecnológica e informacional inovadora que privilegie a interoperabilidade e a disponibilização da informação e fomente o incremento do alinhamento tecnológico com a organização;
- Assegurar uma resposta mais célere, fiável e eficaz ao cidadão/empresa;
- Racionalizar os recursos e diminuir os custos públicos de contexto;
- Criar um contexto favorável à dinamização económica.

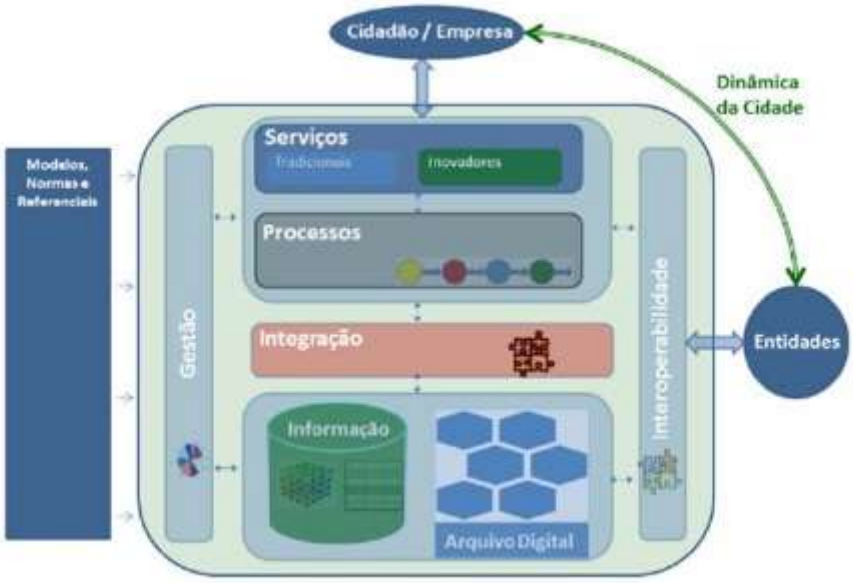


Ilustração 10 - Projeto cap@CIDADE: inovar para o cidadão

[5] Fonte: Proposta cap@CIDADE: inovar para o cidadão (documento interno)

A ilustração 10 demonstra o que se pretende atingir através deste projeto, isto é, uma estrutura integradora de serviços (tradicionais e inovadores) e processos que sirvam de suporte à tomada de decisão por parte da Gestão de Topo, aliado ao conceito de interoperabilidade, responsável pela disponibilização de informação válida ao cidadão/empresa.

A propósito da operação **cap@CIDADE: inovar para o cidadão:** "Será desenvolvido um conjunto de atividades que responderão ao trinómio: cidadão/empresa, inovação e racionalização, tendo como um dos principais objetivos sustentar a atuação do Município e a sua prestação de serviços, numa base tecnológica e informacional inovadora que privilegia a interoperabilidade e a disponibilização da informação"[6].

Do conjunto de atividades elencado no âmbito desta operação surge então a "Implementação do Arquivo Digital Certificável", nível em que este projeto de dissertação se enquadra, que é antecedido pela "Definição da arquitetura de informação", "Definição da arquitetura de sistemas tecnológicos" e da criação do "Modelo conceptual do Arquivo Digital Certificável".

Estas atividades têm como principais objetivos "uma efetiva racionalização de recursos, que passa pelo fomento da interoperabilidade interna e externa; a melhoria, controlo e monitorização da informação e a criação de um modelo passível de ser demonstrado e replicado noutras autarquias e/ou organismos."[7]

Em suma, a CMP com uma implementação bem-sucedida destas atividades constituintes do projeto **cap@CIDADE: inovar para o cidadão**, "caminha para a criação de uma verdadeira cidade inteligente e sustentável, resultante da capacidade das diferentes partes interessadas que integram a comunidade para promoverem a cooperação intelectual em processos de criação. Esta atuação integra a inovação como elemento essencial para corporizar a prestação de novos serviços e alavancar a capacitação do cidadão e o crescimento estruturado da cidade."[8]

3.2. O Documento Orientador

No âmbito do projeto "*Operacionalização Projeto cap@CIDADE – SAMA 2013/2015*" e tendo como ponto de partida a criação de um Arquivo Digital certificável para a Câmara Municipal do Porto, este documento orientador elaborado por uma equipa pluri e

[6] Fonte: Declaração CMP (documento interno)
[7] Fonte: Proposta cap@CIDADE: inovar para o cidadão (documento interno)
[8] Fonte: Declaração CMP (documento interno)

multidisciplinar teve como principal objetivo fornecer todo um conjunto de orientações necessárias para que, de certa forma, fosse possível a concretização deste projeto circunscrito ao desenvolvimento de uma arquitetura info-tecnológica coesa e rigorosa na organização.

Para tal, foi necessário em primeiro lugar esclarecer alguns conceitos importantes para uma melhor interpretação das temáticas a serem analisadas para o projeto. É consensual a todos os participantes, que o desenvolvimento de um projeto desta envergadura comporta um elevado nível de complexidade, pelo que se torna essencial a proatividade de várias áreas de conhecimento.

Este documento contém cinco capítulos principais, são eles:

- **Introdução** – Nesta parte do documento são então abordados e definidos alguns conceitos mais complexos de compreensão, os objetivos e impactos esperados, quer a nível organizacional quer do cidadão, do projeto, o plano metodológico bem como a sua perspetiva incremental.
- **Modelo Conceptual** – É selecionado o modelo conceptual para o repositório digital, analisa-se quer a arquitetura tecnologia quer informacional da CMP e também a própria arquitetura do repositório nomeadamente a parte de armazenamento.
- **"Estado da Arte" do município do Porto** – Como o próprio nome do capítulo indica, neste são apresentados os resultados da análise feita à arquitetura tecnológica, as políticas de gestão da informação, assim como as de segurança e preservação da informação. São também abordadas as preocupações legais do projeto, mais concretamente a questão da validade da assinatura digital.
- **Modelos de Operacionalização** – Neste capítulo são apresentados os vários planos consequentes deste projeto, nomeadamente, o plano de ação, plano estratégico e plano tático e operacional – projetos estruturantes.
- **Desafios Futuros** – Este último capítulo expõe o que será de esperar, isto é, desafios óbvios e pertinentes uma vez que nos movimentamos numa área ainda desconhecida e de caráter vanguardista

No decorrer desta dissertação, esta equipa multidisciplinar, do qual fazem parte colaboradores da DMSI, da DMAG e da DMAH reuniu várias vezes para discutir as diferentes temáticas em estudo, naturalmente, com enfoque na interligação da área informacional e tecnológica. No decurso desta atividade, foram sendo criadas pequenas equipas de trabalho,

às quais era afeta uma determinada área para estudo e análise. Posteriormente, eram discutidas as soluções encontradas e trilhado o caminho a seguir, naquele que é, ainda, uma árdua e complexa tarefa no que à preservação em meio digital diz respeito.

Encontram-se assim reunidos os principais intervenientes, que terão de implementar e reajustar os princípios enunciados neste trabalho por forma a garantir a plena adesão municipal à revolução informacional em curso.

3.3. O Modelo de Segurança e Preservação da Informação

Partindo do levantamento dos instrumentos normativos, modelos e guias de boas práticas existentes, foi proposto por Sousa (2013) um *Modelo de Segurança e Preservação da Informação* para o município do Porto.

Assim, numa primeira etapa, partindo para o levantamento da situação atual relativa à segurança da informação, procedeu-se a uma pesquisa dos instrumentos normativos, modelos e guias de boas práticas existentes e à sua análise e comparação com os controlos da ISO/IEC 27002. Os documentos encontrados (Procedimentos e instruções de trabalho, impressos, ordens de serviço, etc.) encontram-se disponíveis para consulta dos colaboradores na CMP através de aplicações da rede interna, no Portal do Colaborador ou no Portal da Qualidade (Sousa, 2013).

Foi também delineado como objetivo, a elaboração de um conjunto de políticas de suporte ao Sistema de Gestão de Segurança da Informação (SGSI) que são essenciais para a observação dos três princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

Estas políticas são fundamentais, uma vez que permitem:

- A análise e identificação dos riscos, e respetivas categorias, que aliadas a um conjunto de controlos potenciam a deteção de ameaças e riscos;
- O tratamento dos riscos, através dos mecanismos necessários na prevenção e correção das ameaças e vulnerabilidades detetadas.

Os principais documentos a serem elaborados para a implementação do SGSI passavam pela definição da *Comissão de Gestão de Segurança da Informação* (CGSI) e o Âmbito do *Sistema de Gestão de Segurança da Informação* (Sousa, 2013).

A *Comissão de Gestão de Segurança da Informação* (CGSI) fornece a direção e estratégia no âmbito da evolução da maturidade de TI/SI e do nível da segurança de

informação para a camada de gestão da organização. É essencial, na medida em que, a gestão dos SI e da própria informação revela-se crucial a nível estratégico (Sousa, 2013).

Foi igualmente produzido o documento que define o Âmbito do SGSI. Dada a complexidade a que está inerente um SGSI que englobe toda a organização, aplicou-se um âmbito mais reduzido, embora igualmente ambicioso – a aplicação ao Arquivo Digital da CMP.

O Arquivo Digital da CMP terá como objetivo manter e preservar informação Ativa e Permanente, gerida de forma integrada, independentemente do seu suporte. Este caracteriza-se pela presença de um **Sistema [Integral] de Informação Ativa e Permanente** (SIAP) que implica a existência de uma gestão contínua e integral do ciclo de vida da informação que, desta forma, acompanha a componente orgânica que a usa e/ou cria, sendo, simultaneamente, o reflexo da interatividade informacional da organização (Sousa, 2013).

Desta forma, surgem, as políticas mais detalhadas e que servem de suporte à Política de Segurança da Informação:

- Política de Classificação da Informação;
- Política de Gestão de Acessos;
- Política de Gestão de *Passwords*;
- Política de Utilização de Correio Eletrónico;
- Política de *Backups;*
- Política de Acesso à Internet;
- Política de Gestão de Operações;
- Política de Secretária Limpa Ecrã Limpo;
- Política de Segurança Física e Ambiental;
- Política de Segurança de Rede (Sousa, 2013).

Assim, o modelo de Segurança e de Preservação da Informação ganha esta representação em que ambas as Políticas de Segurança e Preservação da informação são alicerçadas pelas políticas e planos de GI e TI, bem como de uma comissão de GI e TI que monitoriza essas mesmas políticas e planos, que por sua vez supervisiona a Comissão de Segurança e Preservação, colocando na sua base a cooperação entre a gestão dos sistemas tecnológicos de informação e a gestão da informação, uma visão holística e integrada dos planos a desenvolver.

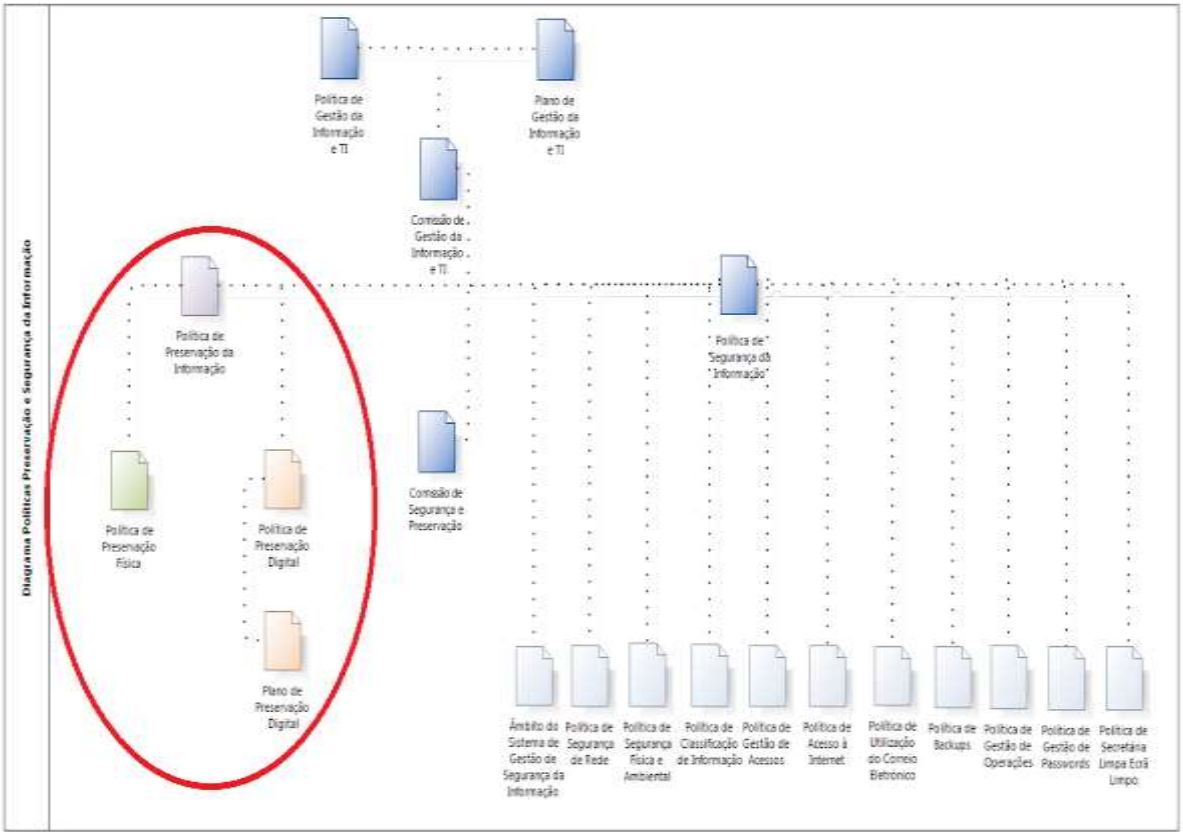


Ilustração 11 - Modelo de Preservação e Segurança da Informação (MP&SInf) V.1 (Sousa, 2013)

Desta forma, o conjunto delimitado na ilustração acima, traça o ponto de partida para esta dissertação, centrando-se esta no âmbito das *Políticas de Preservação da Informação* com especial enfoque no meio digital.

3.4. Do Arquivo Digital ao Repositório Digital Confiável

Foram várias as técnicas que o Homem utilizou ao longo da História para tratamento de informação sendo que a utilização de computadores foi apenas um passo na evolução daqueles meios. Um dos fatores que se tornou decisivo para a adoção das tecnologias para tratamento da informação foi o fenómeno ocorrido a partir da segunda metade dos anos 40 do séc. XX, que ficou conhecido por «explosão documental», com impacto significativo em variados aspetos da vida dos arquivos (Balcky, 2011).

A constatação de que cada vez mais se produz informação em meio digital, suscetível de ser guardada em suportes cada vez mais diversificados e capazes de armazenar quantidades fenomenais de dados, levou à criação de arquivos digitais capazes de armazenar e preservar

toda essa informação.

No entanto, não é consensual a definição de Arquivo digital ou mesmo de Repositório Digital.

A própria UNESCO acentua o impacto de uma situação ambígua quando ao definir programa de preservação ressalta a necessidade de usar o termo *digital materials* dado que "*more commonly used terms such as* ***digital archive*** *and* ***digital repository*** *have been avoided because of their potential ambiguities: archive has different meanings for the records management community and the ICT community, whereas both archive and repository may imply a single storage site – not an appropriate implication where very distributed arrangements may be in place*" (Pinto, 2010).

A normativa ISO/TR 18492:2005 define "arquivo eletrónico" (*Electronic archiving*) como "*storage of electronic information in an independent physical or logical space where the information is protected from loss, alteration and deterioration (NOTE The information may be used as reliable evidence in the future if it has been protected in this manner).*"

Esta aborda o termo repositório de armazenamento (*storage repository*), que distingue de outras definições de cariz técnico "[…] *repository organization or entity charged with the storage and maintenance of authentic electronic document-based information (NOTE It is recognized that this definition is different from technical definitions of "storage repositories").*

Para Balcky (2011) um "repositório digital" terá essencialmente uma estrutura lógica, sujeita ao contexto tecnológico em permanente mudança, em oposição ao arquivo tradicional, com formatos analógicos e suportes cuja estabilidade poderá durar séculos.

Segundo esta autora, um repositório digital "[…] é uma estrutura que compreende tecnologia, recursos humanos e informação de natureza digital – objetos digitais -, isto é, com um conteúdo essencialmente numérico, cujo significado é garantido através de processos de codificação e descodificação e, um conjunto de políticas para incorporar, gerir e acessibilizar, numa perspetiva continuada, objetos digitais de natureza arquivística" (Balcky, 2011). Consequentemente, a sua estabilidade e continuidade têm que ser asseguradas de forma a garantir as suas propriedades básicas – **integridade**, **fidedignidade**, **autenticidade** e **utilização** – ao longo do tempo.

No início do projeto da criação do arquivo digital certificável da CMP, surgiu uma dúvida não em torno do arquivo *versus* repositório mas entre *arquivo eletrónico* (denominação de origem) ou arquivo digital (que se vinha impondo e com a qual começava a

concorrer a designação *repositório digital*). No início a opção incidiu no eletrónico e não digital, pois, na altura, o termo "digital" continha um pendor muito tecnológico ao contrário da designação "eletrónico" que se configurava mais sistémica e por isso mais abrangente. Porém, consultada bibliografia especializada e estudados alguns projetos e modelos de referência internacionais, nomeadamente o OAIS Reference Model e o TRAC (*Trustworthy Repositories Audit & Certification: Criteria and Checklist*), compreendeu-se que o mais adequado seria usar o termo "Arquivo Digital". O termo "eletrónico" poderia suscitar ambiguidade, pois, do ponto de vista tecnológico, existe uma diferença entre os termos "eletrónico" e "digital" e nem tudo o que é eletrónico é digital (por ex. leitor de cassete vídeo ou música, etc.). Por outro lado, torna-se evidente a crescente utilização de expressões como "documento digital ou eletrónico" o que chama a atenção para o facto de que um documento digital é, na verdade, uma variante de documento eletrónico, mas codificado em dígitos binários implicando a utilização de um computador/sistema computacional, isto é, suporte, para ser reproduzido.

Entretanto emerge o termo "repositório digital" onde o conteúdo, ativos digitais, são armazenados e podem ser pesquisados e recuperados para uso posterior. Um repositório suporta mecanismos para importação, exportação, identificação, armazenamento e recuperação de ativos digitais. Colocar o conteúdo digital num repositório permite que a instituição consiga, geri-lo e preservá-lo, e, portanto, tirar o máximo dele.

De acordo com a TRAC, o termo repositório digital é "often used interchangeably. OAIS uses archive when referring to an organization that intends to preserve information for access and use by a designated community(ies). *Trusted Digital Repositories: Attributes and Responsibilities* prefers the term digital repository. Digital archives and digital repositories should not be confused with either *digital libraries*, which collect and provide access to digital information, but may not commit to its long-term preservation, or data archives, which do commit to long-term preservation but limit their collections to statistical datasets."

Na sua origem encontramos o repositório institucional ligado a duas tendências:

- A da necessidade de interoperabilidade e a sua ligação à *Open Archives Initiative* (OAI) e ao seu *Open Archives Initiative Protocol for Metadata Harvesting* (OAI-PMH), que resultam das iniciativas internacionais em torno do *Open Access Movement,* no âmbito da informação científica e técnica;
- A emergência das bibliotecas digitais centradas na coleta, armazenamento, classificação, catalogação, preservação e disponibilização de conteúdos digitais.

De forma simples é identificado como um arquivo *online* direcionado à recolha,

preservação e difusão de informação digital resultante da produção intelectual de uma instituição, particularmente uma universidade ou instituição de investigação.

Lynch define a sua visão de um "*repositório institucional*" como "... um conjunto de serviços que a organização oferece aos membros da sua comunidade para a gestão e disseminação de materiais digitais criados pela instituição e membros da sua comunidade. É essencialmente um compromisso organizacional com a administração destes materiais digitais, incluindo a preservação a longo prazo se for o caso, bem como a organização e acesso ou distribuição" (Lynch, 2003, apud Wheatley, 2004).

Já Strathmann (2008) referencia os mais recentes "*repositórios digitais certificados*" que surgem como resposta à problemática da criação exponencial de conteúdos digitais e de não haver nada ou algo que pudesse garantir a **integridade**, a **autenticidade** e a **acessibilidade** dessa informação no longo prazo.

De acordo com Strathmann (2008), existe a premissa subjacente aos requisitos fundamentais para os repositórios de todos os tipos e tamanhos segundo a qual estes e as respetivas atividades de preservação devem ser dimensionados para as necessidades e os meios da comunidade alvo.

A criação de *repositórios de preservação* configura-se como algo complexo face à inexistência de soluções ou estratégias únicas, o que conduz à necessidade de uma conjugação de esforços que tem como marcos principais os seguintes documentos e iniciativas:

- 2002 - *Trusted Repositories Attributes & Responsibilities*;
- 2002 - *Reference Model for an Open Archival Information System* (desenvolvido pela NASA e norma ISO 14721 em 2003);
- 2005 - RLG/NARA (*National Archives and Records Administration) Draft Audit Check-list for Repository Certification* (entra em discussão pública);
- 2006-2007 - CRL and DCC *Pilot Repository Audits*;
- dez 2006 - *Catalogue of Criteria for Trusted Digital Repositories* (publicado pelo NESTOR);
- fev 2007 - *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) publicado pela DCC/DPE;
- mar 2007 - *Trustworthy Repositories Audit & Certification* (TRAC) *Criteria and Check-list*;

- 2012 - ISO 16363:2012 - *Space data and information transfer systems – Audit and certification of trustworthy digital repositories* (antigo TRAC).

Em 2003, o RLG e os NARA (US) criam uma *task-force* para abordar especificamente a certificação de repositórios digitais, tendo como objetivo desenvolver critérios para identificar os repositórios digitais capazes de armazenar e garantir o acesso à informação de forma confiável. O desafio consiste em definir critérios de certificação e delinear um processo para certificação aplicável a repositórios e arquivos digitais, sejam repositórios institucionais académicos e de bibliotecas nacionais, grandes arquivos de dados ou para prestação de serviços de arquivo a terceiros.

Entre 2005 e 2007 este trabalho envolveu grupos de trabalho na Europa, bem como nos Estados Unidos.

No âmbito internacional são, assim, formulados os dez princípios básicos a cumprir por *repositórios digitais*, resultado do trabalho de cooperação de várias entidades, nomeadamente a DCC (*Digital Curation Center*), a DPE (*Digital Preservation Europe*) e a CRL (*Center for Research Libraries*):

- Comprometer-se na contínua manutenção de objetos digitais para a comunidade / comunidades alvo;
- Demonstrar aptidão organizacional (incluindo financeira, pessoal, estrutura e processos) para cumprir o seu compromisso;
- Adquirir e manter os direitos contratuais e legais necessários e cumprir com as responsabilidades;
- Ter uma política eficaz e eficiente;
- Adquirir e ingerir objetos digitais com base em critérios estabelecidos e que correspondam aos seus compromissos e capacidades;
- Manter / garantir a integridade, a autenticidade e a usabilidade do objeto digital que detém ao longo do tempo;
- Criar e manter metainformação necessária sobre ações tomadas em objetos digitais durante a preservação, bem como sobre a produção, suporte de acesso e contexto de processos de uso antes da preservação;
- Preencher os requisitos de divulgação necessários;
- Possuir um programa estratégico para o planeamento e ações de preservação;

- Possuir uma infraestrutura técnica adequada para a manutenção contínua e segurança dos seus objetos digitais.

Segue-se, em 2007, o documento TRAC (*Trustworthy Repositories Audit & Certification*), uma versão revista e que complementa o documento anterior, apresentando como objetivos:

- Fornecer uma ferramenta que permita **auditar**, **avaliar**, e potencialmente **certificar** repositórios digitais;
- Estabelecer a **documentação necessária** para realizar uma auditoria;
- Desenhar o processo de certificação;
- Estabelecer metodologias apropriadas para determinar a robustez e a sustentabilidade de um repositório digital.

Este documento apresenta-se sob a forma de uma *checklist* contendo todos os requisitos que um repositório digital deve possuir para que possa ser confiável.

Esta iniciativa está na base da publicação, em 2012, da norma internacional ISO 16363 criada com o propósito de definir a prática recomendada para orientar um processo de certificação e auditoria para avaliar a confiabilidade dos repositórios digitais, tendo como âmbito toda o conjunto de repositórios digitais existentes.

Um repositório digital confiável não deve deixar de parte a implementação de ações e de uma estratégia consciente, e entender os riscos e ameaças a que os sistemas estão sujeitos. Este deve ser visto na sua totalidade, partindo da organização que o gere até à sua própria estrutura. É por isso fundamental que este tenha um conjunto de políticas e procedimentos bem definidos, que envolvam as temáticas da gestão dos objetos digitais, do seu armazenamento e preservação, até à infraestrutura tecnológica, segurança e gestão de acessos.

Um repositório digital confiável deverá considerar as ameaças e riscos no seio dos seus sistemas. Serão exigidos aos repositórios a constante monitorização, planeamento e manutenção, bem como ações conscientes e implementação da estratégia a fim de estes realizarem a sua missão, isto é, assegurar a preservação da informação digital a longo prazo.

O projeto PORTICO constituiu-se como *repositório digital confiável* em 2010, através de uma auditoria levada a cabo pelo *Center for Research Libraries* (CRL), tendo sido o primeiro repositório de preservação de informação em meio digital a ser certificado de acordo com os requisitos explícitos na então designada TRAC e, posteriormente, convertida

em ISO (16363:2012).

De acordo com esta normativa, existem três áreas principais a serem avaliadas, para que um repositório seja certificado:

- Infraestrutura organizacional;
- Gestão de objetos digitais;
- Infraestrutura e Gestão de Riscos de Segurança.

Do relatório de certificação do PORTICO efetuado pelo CRL, destacam-se alguns aspetos tecnológicos que devem ser tidos em conta aquando da implementação de um Arquivo Digital:

- A descrição de quaisquer mudanças significativas na arquitetura do sistema de repositório ou de configuração, *software* crítico, ou plataformas de *software*;
- Registo de riscos do *software* e *hardware*;
- Políticas-chave fundamentais em matéria de aquisição, gestão e disposição do conteúdo arquivado, arquivos relacionados e metainformação;
- Registos de eventos e mudanças significativas na natureza e condição do conteúdo digital, como os *logs* do servidor;
- Registos de eventos e mudanças significativas nas operações do repositório (Sousa, 2013).

Um repositório digital deve, por isso, mostrar evidências de que se encontra em conformidade com os critérios estabelecidos na ISO 16363:2012, por intermédio da documentação (planos, políticas, declarações, etc.) e da adequação da missão e objetivos do repositório às necessidades da *comunidade-alvo* (Sousa, 2013).

No caso da CMP o seu arquivo/repositório digital encontra-se numa nova fase de desenvolvimento com a vista à sua preparação para a certificação.

A plataforma tecnológica sobre a qual assenta o repositório da CMP é o *software* FEDORA (*Flexible Extensible Digital Object Repository Architecture*).

O FEDORA é uma estrutura conceptual que usa um conjunto de abstrações sobre informação digital para fornecer a base para *software* capaz de gerir informação em meio digital. Fornece a base para assegurar a durabilidade da informação a longo prazo e garantir a sua disponibilização para ser usada de formas diversificadas. É necessário perceber que a plataforma FEDORA fornece os alicerces sobre os quais se pode construir uma variedade de

esquemas de gestão de informação para diferentes casos de uso, e não uma solução completa para um caso de uso em específico.

Neste contexto, o *Fedora Software Repository* apresenta como características principais:

- Permite armazenar todos os tipos de conteúdo e respetiva metainformação;
- Permite gerir e manter conteúdos digitais de qualquer tipo;
- Permite gerir e manter metainformação sobre o conteúdo, em qualquer formato;
- Tem capacidade para milhões de objetos;
- Utiliza protocolos de acesso aos dados via Web APIs (REST / SOAP);
- Fornece pesquisa RDF (SPARQL);
- Utilitário de reconstrução (para recuperação de desastres e migração de dados);
- Todo o repositório pode ser reconstruído a partir do objeto digital e arquivos de conteúdo;
- *Content Model Architecture* (definir "tipos" de objetos a partir do seu conteúdo);
- Muitas opções de armazenamento (sistemas de banco de dados e arquivos);
- Mensagens JMS (permite envio de mensagens entre as várias aplicações e repositório);
- Administração GUI via web (baixo nível de edição de objetos);
- Provedores de Serviços OAI-PMH;
- Serviço de Pesquisa *GSearch* (texto completo);
- Múltiplos *front-ends* orientados a clientes.

Em suma, mesmo que algumas políticas de preservação sejam articuladas e geridas no FEDORA, a instituição ainda tem de formular essas políticas. Estas não se encontram predefinidas no FEDORA, ou seja, em vez de servir como uma solução de repositório *out-of-box*, o FEDORA é uma arquitetura de repositório no qual uma instituição pode construir um repositório de muitas maneiras diferentes.

Como resultado, a adequação do FEDORA como base de um “Sistema de Preservação” depende significativamente da sua implementação.

Desta forma, podemos afirmar que sem as pessoas, infraestrutura, políticas e

procedimentos adequados, nem mesmo a melhor plataforma de preservação pode garantir uma preservação eficaz e eficiente dos seus documentos.

4. Contributo para o *Modelo Estratégico de Preservação da Informação*

4.1. Estrutura Informacional de suporte ao *Serviço de Gestão da Preservação da Informação*

A necessidade de certificar o repositório digital por parte da CMP deu por sua vez, origem à necessidade da criação de um *Plano de Preservação da Informação*.

Assim sendo, e como ponto de partida, estabeleceu-se a necessidade de se criarem as bases para a construção deste Plano como sendo uma dos instrumentos de suporte à certificação do repositório digital da CMP, em conjunto com o *Plano de Segurança da Informação*.

Para a construção do Plano de Preservação da Informação em meio digital e consequentemente a implementação da certificação a nível do repositório digital, a primeira proposta foi tomar a decisão de criar toda a *estrutura de suporte à especificação*.

Neste sentido, foi necessário abordar os dois campos e perceber quais as carências a nível documental para se poder trabalhar no âmbito da Preservação da Informação, no sentido de poder contribuir para a construção de um Plano de Preservação e na área do repositório digital confiável (ilustração 16).

Partindo do levantamento dos instrumentos normativos, nomeadamente ISO 16363 e ISO 18492, modelos e guias de boas práticas existentes como os casos de Londres e Sheffield, foi elaborada uma estrutura documental de suporte, referidos como *Documentos de Suporte à Especificação* (DSE) que têm no seu intuito serem guias práticos, isto é, bases informacionais, os quais deverão ser consultados e seguidos para que se consiga desenvolver o *Modelo de Segurança e Preservação da Informação da CMP,* um contributo essencial para o processo de certificação do *repositório digital* (anexo 4).

Neste contexto foi elaborada toda uma estrutura de suporte informacional que servirá de base para o Plano de Preservação da Informação em meio digital da CMP, de entre os quais se destacam: *Plano de Preservação*; *Estratégia de Preservação*; *Política de Preservação*; *Identificação e Avaliação de Formatos*; *Identificação de Sistemas de Informação*; *Declaração de Missão*; *Acordo de Custódia*; P*lano de Contingência* e *Plano de Recuperação de desastres*.

Alguns documentos estabelecidos tiveram como base documentos internos da CMP, que se encontram disponíveis através de aplicações da rede interna, no *Portal do Colaborador* ou no *Portal da Qualidade* que foram assim utilizados e modelados para que se adequassem ao Plano de Preservação da informação em meio digital.

No cabeçalho de cada documento, encontra-se alguma informação, nomeadamente a data em que o documento foi elaborado, o número de revisões efetuado ao mesmo e também um código único, o qual foi criado de acordo com a tabela de controlo de documentos formulada no âmbito deste projeto, tendo como base os instrumentos normativos ISO/TR 18492:2005, e, sobretudo, a ISO 16363:2012 bem como os guias de boas práticas a nível internacional como os, *Sheffield Archives, London Metropolitan Archives,* NAA e os NARA (anexo 2).

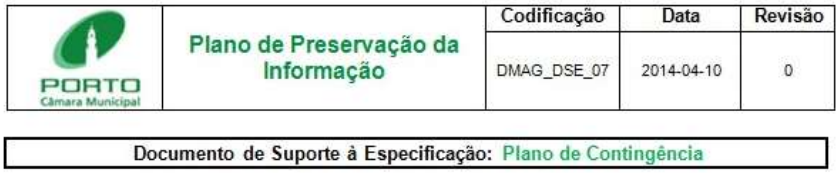


Ilustração 12 - Exemplo do cabeçalho de um documento de suporte à especificação

É igualmente importante referir que toda esta estrutura de suporte documental segue um formato padrão que consiste nos seguintes passos:

1. Objetivo;
2. Âmbito;
3. Responsabilidades;
4. Descrição;
5. Definições e Abreviaturas;
6. Anexos.

Como podemos verificar pela ilustração 13, encontram-se duas tabelas que servem basicamente como controlo do documento, ou seja, na primeira tabela está mencionada a pessoa responsável pela elaboração do documento, a pessoa que o verifica (chefia) e depois segue para aprovação para a direção municipal. Na tabela seguinte encontram-se as questões de revisão bem como das alterações que foram feitas no documento.

De seguida, no capítulo dos *Objetivos* é descrito qual o propósito do documento que está a ser elaborado, enquanto a questão do *Âmbito* serve para enquadrar, de uma forma holística, o documento em toda esta estrutura de suporte à elaboração do Plano de Preservação da informação.

	Responsável	Data	Assinatura
Elaborado por	Equipa da		
Verificado por	Chefe de Divisão		
Aprovado por	Diretor Municipal		

Revisão	Data da Aprovação	Descrição das Alterações
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Plano de contingência, para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

Qualquer cópia / impressão deste documento é considerada NÃO CONTROLADA, devendo ser confirmada a sua atualização. Página **1** de **4**
Não é permitida a entrega deste documento a terceiros e a circulação externa, sem autorização da CMP.

Ilustração 13 - Estrutura do Formulário DSE (1)

O ponto das responsabilidades consiste numa pequena tabela onde se encontram todos os intervenientes que contribuem para a criação daquele documento, incluindo as chefias para a sua validação. Na parte da descrição, encontra-se o desenvolvimento do próprio documento, ou seja, toda a base informacional suportada a nível normativo e nos guias de boas práticas, aqui considerados para este projeto (ilustração 14).

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Plano de Contingência

Propósito

Esta orientação interina fornece instruções para ações que serão tomadas no caso de o Governo não providenciar as dotações regulares ou uma resolução contínua, resultando numa interrupção do financiamento para as funções apropriadas do arquivo.

Resumo das atividades NARA em caso de lapso de verbas:

a) *No caso de um lapso de dotações, a instituição deverá suspender imediatamente todas as atividades apropriadas. Salvo conforme autorizado por este plano de contingência, nenhuma atividade que requerem a intervenção ou a presença no local de um Governo ou o contratante empregado ou de outra forma requer a obrigação de dotações anuais serão permitidas;*
b) *Todas as instalações de arquivo devem ser fechadas, nomeadamente aos funcionários, público em geral e ocupantes não-federais e será assegurado para a duração de um lapso de financiamento.*
c) *A maioria dos funcionários deve ser dispensada temporariamente. Exceto para os funcionários identificados como "exceção" no âmbito deste plano de contingência e funcionários pagos a partir de fontes diferentes de uma dotação anual;*
d) *Alguns empregados podem ser chamados ao serviço em casos de emergência. Em caso de uma emergência que ocorre durante um lapso de dotações anuais, os funcionários que foram inicialmente designados como "não-isentos" podem ser temporariamente chamados da licença para executar funções de emergência.*
e) *A maioria dos contratos deve ser suspensa. Contratos isentos (como contratos de serviços públicos e de serviços de telecomunicações) vão manter o nível "mínimo" de contrato de serviço necessário para proteger a vida e a propriedade.*
f) *Listagens de emergência serão mantidas vigentes. As organizações deverão rever periodicamente estas listas de emergência, para garantir que as mesmas são atuais.*

Ilustração 14 - Estrutura do Formulário DSE (2)

No que diz respeito às definições e abreviaturas servem para dar a conhecer algum termo utilizado na parte da descrição que para facilitar a leitura foi abreviado, por exemplo. Nos anexos encontram-se algumas tabelas e imagens que servem de apoio ao que foi escrito como base informacional no ponto da descrição (ilustração 15).

É de seguida apresentado, um quadro geral para responder a um lapso temporário de dotações. Apesar de "temporário" é definido como 30 dias consecutivos ou menos para ações adversas de funcionários, nesta parte, significa apenas o período relativamente curto, muitas vezes apenas alguns dias ou menos, normalmente exigidos para o Congresso fornecer fundos. Se um lapso for alargado ou uma atividade for finalizada, serão emitidas instruções adicionais.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Ilustração 15 - Estrutura do Formulário DSE (3)

Após a descrição geral de toda esta estrutura documental de suporte, criada para apoiar a elaboração do Plano de Preservação, passamos agora a especificar/descrever cada um dos documentos criados para o efeito.

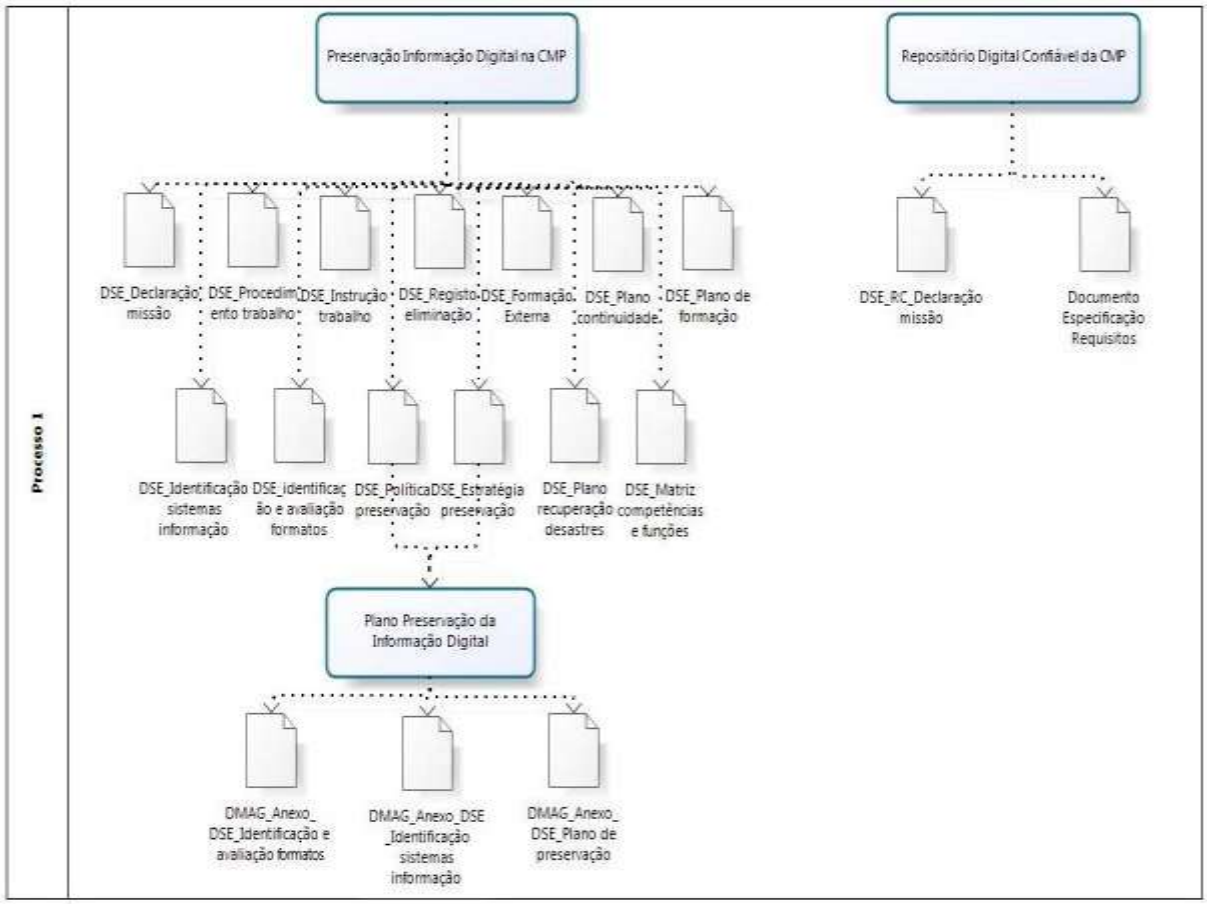


Ilustração 16 - Estrutura de Documentos de Suporte à Especificação (DSE)

O documento criado relativo ao **Plano de Preservação** tem como principal objetivo servir de guia para a definição de uma estrutura base para a construção do Plano de Preservação da informação [em meio] digital da CMP. Este documento contém assim as principais diretrizes a serem seguidas para a elaboração de um Plano de Preservação da informação. Foram ainda elaborados como suporte ao conteúdo informacional deste documento, quatro anexos sobre: As várias e possíveis estratégias de preservação, os procedimentos de preparação de documentos para armazenamento e preservação, uma *checklist* de Avaliação das digitalizações e uma tabela onde estão patentes a variedade de registos digitais que podem ser gerados por diferentes organizações no seu dia-a-dia.

O documento da **Estratégia de Preservação** tem como objetivo principal fornecer as bases para a definição de uma estratégia de preservação da informação a longo termo, para a elaboração do Plano de Preservação da informação em meio digital da CMP.

Quanto ao documento da **Política de Preservação**, este tem como intenção servir de guia para a definição de uma Política de preservação da informação em meio digital, para a

elaboração do Plano de Preservação da informação em meio digital da CMP, fornecendo os tópicos base a abordar para a elaboração deste documento.

No que diz respeito ao documento da **Declaração de Missão**, este tem como principal objetivo servir de guia para a definição de uma Declaração de Missão, para a elaboração do Plano de Preservação da informação em meio digital da CMP. Este documento contém exemplos de outras declarações de missões nomeadamente dos Arquivos Metropolitanos de Londres e dos TNA.

O documento alusivo à **Identificação de Sistemas de Informação** tem como finalidade servir de guia para a definição de um Diagnóstico dos sistemas tecnológicos e informacionais, para a elaboração do Plano de Preservação da informação digital da CMP. Este documento deu origem a um anexo onde consta uma folha de recolha/ levantamento de dados para análise e diagnóstico dos sistemas de informação existentes na organização, bem como uma grelha bastante detalhada para a caracterização dos sistemas de informação onde se abordam vários fatores a ter em conta nessa mesma caracterização como: interoperabilidade do sistema, crescimento do sistema e segurança do sistema.

O documento da **Identificação e Avaliação de Formatos** tem como propósito como o nome indica, fornecer um guia onde se encontrem expostos alguns exemplos de como se deve orientar e avaliar as opções existentes para os formatos de ficheiros e plataformas de armazenamento para uma Preservação da informação em meio digital, para a elaboração do Plano de Preservação da informação em meio digital da CMP. Este documento deu origem à criação de um anexo, que contém uma tabela com o critério a ter em conta no momento da avaliação do formato bem como a descrição desse mesmo critério.

No documento referente ao **Plano de Contingência** é exposto um caso para servir de guia para a definição de um Plano de contingência, para a elaboração do Plano de Preservação da informação digital da CMP. Este fornece instruções para ações que serão tomadas no caso de o Governo não fornecer o financiamento regular ou uma resolução contínua, resultando numa interrupção do financiamento para as funções apropriadas do arquivo.

Já o documento relativo ao **Plano de Continuidade** serve de guia para a definição de um Plano de continuidade, para a elaboração do Plano de Preservação da informação em meio digital da CMP, baseado em seis princípios da Continuidade Digital que irá ajudar as organizações a alcançar benefícios de negócios, incluindo a eficiência e minimização de riscos.

No que diz respeito ao documento sobre o **Plano de Recuperação de desastres** tem como principal objetivo servir de guia para a definição de Plano de Recuperação de

desastres, para a elaboração do Plano de Preservação de informação em meio digital da CMP. Este plano é destinado a comunicar os procedimentos de preparação de desastres, continuidade e recuperação do arquivo de dados para o pessoal, os depositantes, utilizadores e financiadores, bem como facilitar a promulgação da preparação de desastres no arquivo e para garantir o acesso contínuo aos bens e serviços digitais prestados pelo arquivo, com o mínimo de interrupção.

Relativamente ao documento sobre **Acordo de Custódia**, este documento tem como principal objetivo servir de guia para a definição de um Acordo de custódia, para a elaboração do Plano de Preservação da informação digital da CMP. Este documento foi produzido tendo por base um documento interno da CMP disponível no Portal da Qualidade.

O documento referente ao **Registo de Eliminação**, tem como responsabilidade servir de 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 CMP. Este documento foi elaborado tendo por base um documento interno da CMP disponível no Portal da Qualidade.

Foi igualmente abordada a **Política de *Backups***, que tem como principal objetivo servir de guia para o estabelecimento desta política, que por sua vez, define o conjunto de procedimentos a levar a cabo para se salvaguardar os Sistemas de Informação da CMP através da realização de *backups*, para o Plano de Preservação da informação digital da CMP. Este documento foi produzido tendo por base um documento interno da CMP disponível no Portal da Qualidade.

O documento **Ata de Reunião** tem como principal objetivo servir de guia para a definição de uma Ata de reunião, para a elaboração do Plano de Preservação da informação digital da CMP. Este documento foi elaborado tendo por base um documento interno da CMP disponível no Portal da Qualidade.

No documento relativo à **Matriz de competências e funções**, encontra-se uma grelha que serve de guia para a definição de uma estrutura nuclear com as competências e funções dos colaboradores que serve posteriormente para uma avaliação do seu desempenho na organização, para a elaboração do Plano de Preservação da informação em meio digital da CMP. Este documento foi elaborado tendo por base um documento interno da CMP disponível no Portal da Qualidade.

Quanto ao documento do **Plano de Formação**, tem como propósito servir de guia para a definição de um Plano de Formação, para a elaboração do Plano de Preservação da informação em meio digital da CMP. Este documento foi elaborado tendo por base um

documento interno da CMP disponível no Portal da Qualidade.

Os documentos relativos à **Instrução de Trabalho** e **Procedimento de Trabalho,** têm como responsabilidade servir de guia para a definição de uma instrução e de um procedimento de trabalho, para a elaboração do Plano de Preservação da informação em meio digital da CMP. Estes documentos foram elaborados tendo por base documentos internos da CMP disponíveis no Portal da Qualidade.

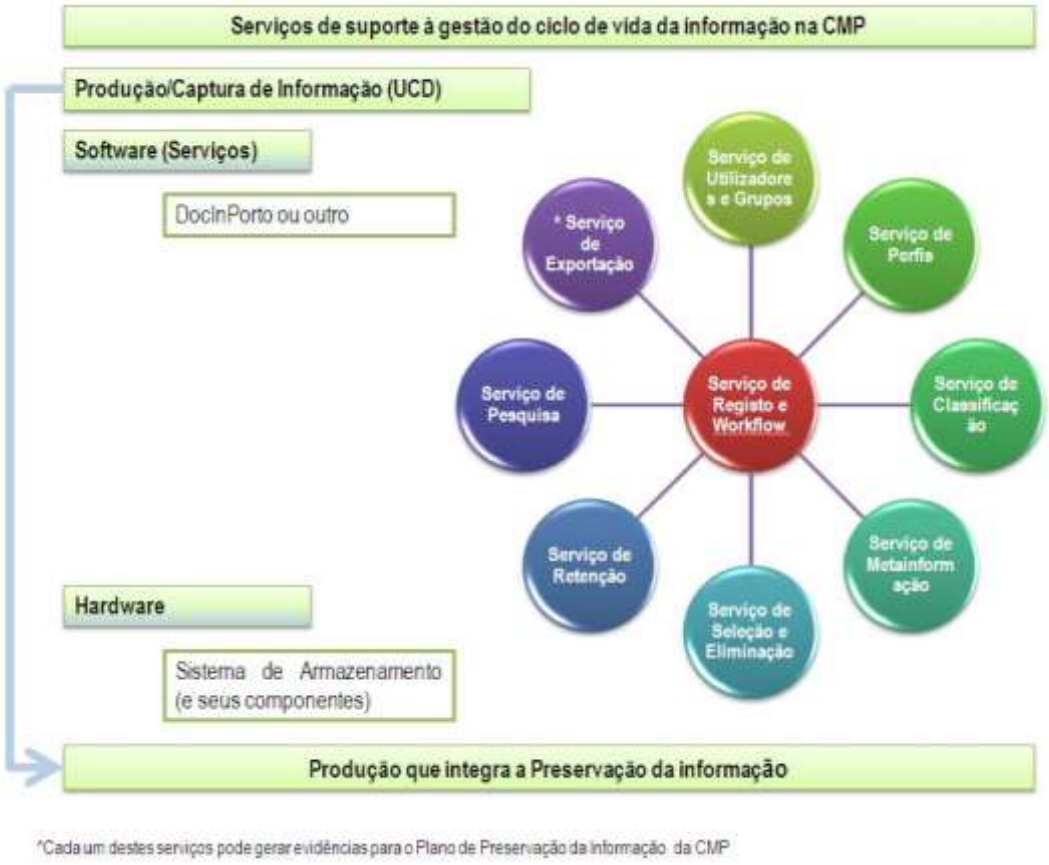


Ilustração 17 - Estrutura base de "Serviços" a abarcar pelo "Serviço de Gestão da Preservação" na CMP

A imagem supra dá uma visão geral da estrutura base de "Serviços" e orientará o trabalho a desenvolver nas diversas vertentes (fase do ciclo de vida, *hardware*, *software* e serviços, em linha com o proposto pelo MoReq2010), estando sob a incidência do presente projeto o **Serviço de Gestão da Preservação** que abarcará toda essa estrutura e que consiste num conjunto de funcionalidades que permitirão a implementação das políticas necessárias à Preservação da informação.

Assim, a ilustração que se segue vem na sequência da anterior, pois ilustra em alto nível o *Serviço de Gestão da Preservação da Informação Digital na CMP*, onde apoiados no modelo OAIS podemos especificar os passos principais do processo: entrada/ingestão (SIP),

processamento/gestão (AIP) e disseminação da informação (DIP) no repositório digital.

Assim, e após identificados os Pacotes de Informação, estes podem ser classificados em três tipos:

- *Submission Information Package* – **SIP**, será o pacote enviado do processo de entrada/ingestão de informação para o Repositório;
- *Archival Information Package* – **AIP**, será o pacote de informação efetivamente armazenado dentro do Repositório;
- *Dissemination Information Package* – **DIP**, será o pacote transferido do Repositório para um utilizador em resposta a uma solicitação.

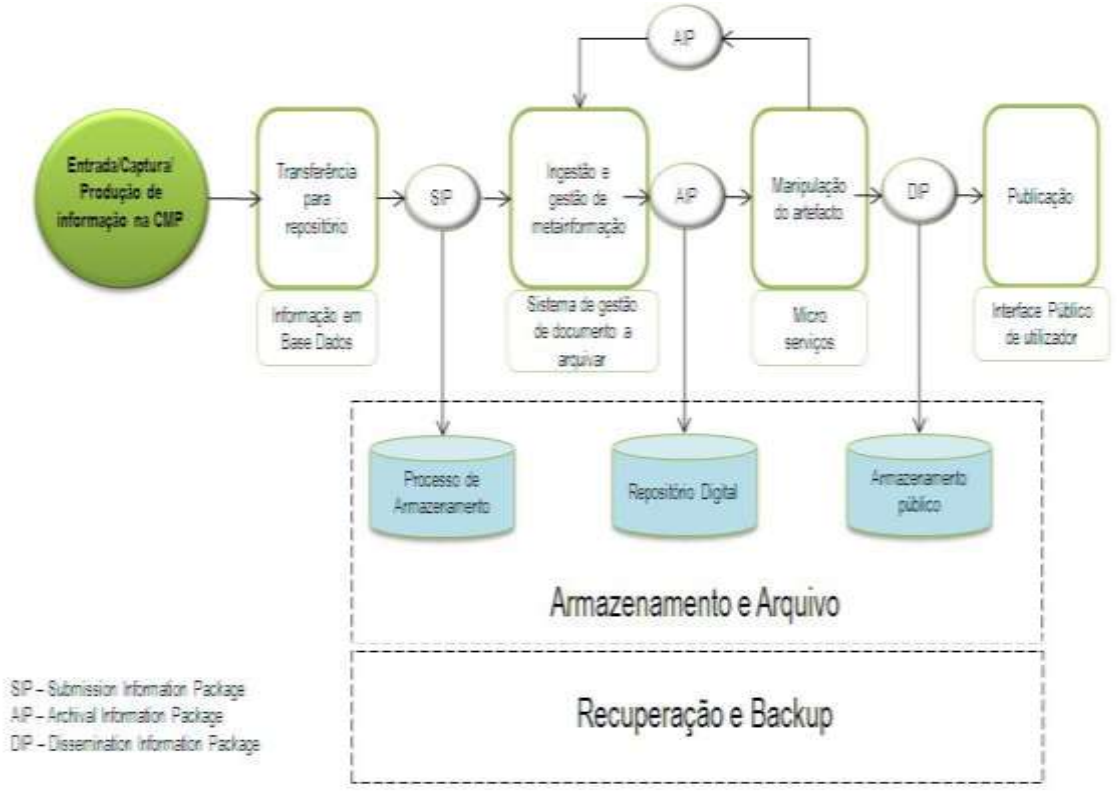


Ilustração 18 – Macroprocesso do "*Serviço de Gestão da Preservação - Informação Digital*" na CMP

4.2. Do Modelo ao Plano de Preservação da Informação

O ***Modelo de Preservação e Segurança da Informação*** (MP&SInf) consiste numa representação de alto nível que constitui uma pré-condição indissociável da elaboração

de um *Plano de Preservação* ou mesmo da concretização de um objetivo estratégico como o da certificação de um *Repositório Digital*, congregando a Gestão do Sistema de Informação (SI) e a Gestão do Serviço de TI (STI), numa visão holística e integradora que orientará o desenvolvimento dos diversos planos que envolvem o SI e o STI do Município do Porto.

Este deverá existir em qualquer instituição, organização ou setor de atividade. Sendo o Município do Porto o contexto organizacional em que foi desenvolvido, considera-se o seu particular interesse para adequação a outros Municípios, o que não obsta a que possa ser, de facto, uma base orientadora para o desenvolvimento do quadro organizacional, informacional e tecnológico que conduzirá, à certificação do Arquivo Digital.

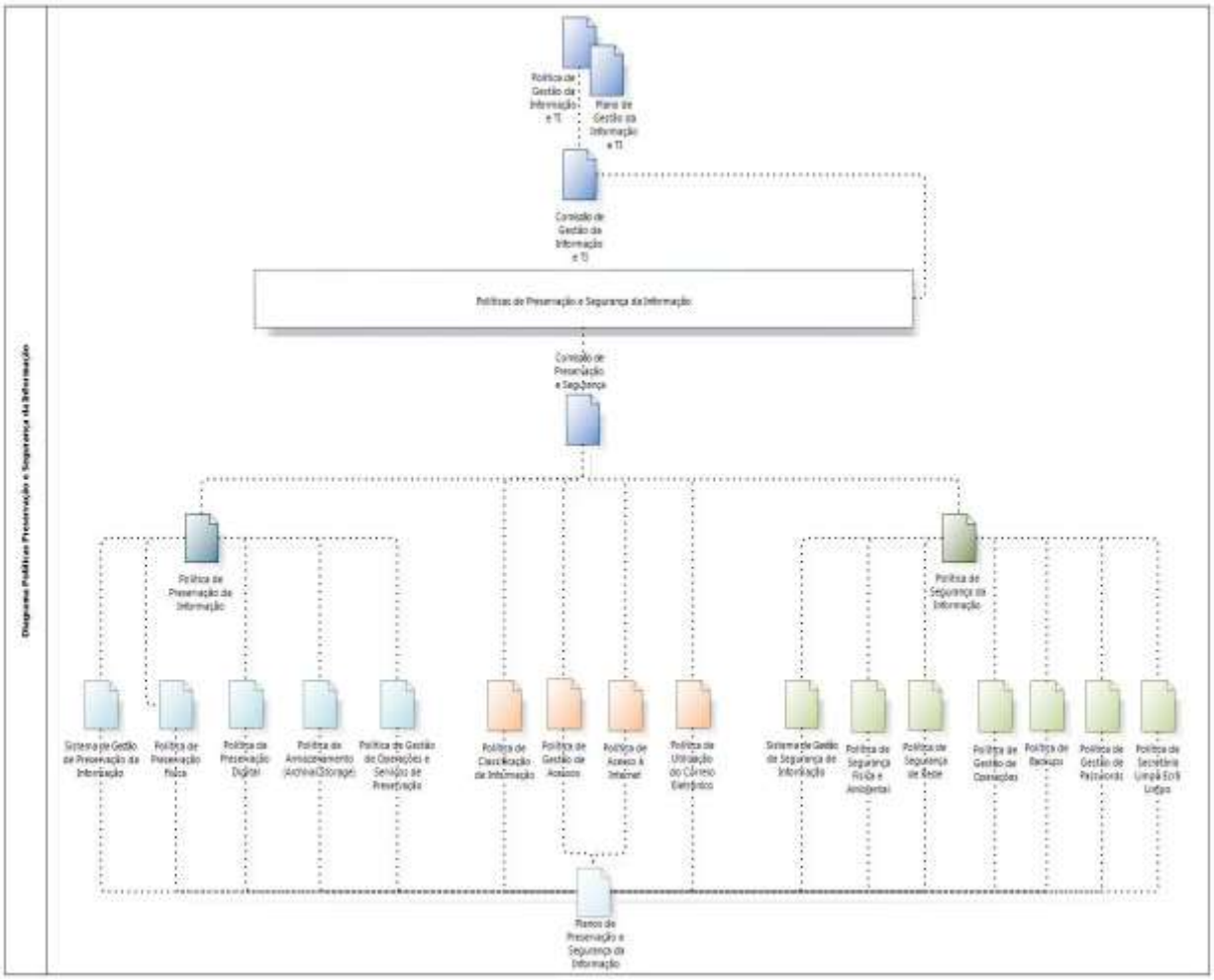


Ilustração 19 - Modelo de Preservação e Segurança da Informação v.2 (MP&SInf) (baseado na v.1 de Sousa, 2013)

Na nova versão do modelo, que partiu da formulação de Sousa que criou a matriz base e desenvolveu a componente de segurança da Informação (Sousa, 2013), constata-se a importância e a inter-relação entre as *Políticas de Segurança de Informação* e as *Políticas de Preservação de Informação*, alicerçadas por uma *Política de Gestão da Informação e TI*, e respetivo *Plano*, sob a monitorização de uma *Comissão de Gestão da Informação e TI* que

supervisiona a *Comissão de Segurança e Preservação*, colocando na sua base a cooperação entre a gestão dos Sistemas Tecnológicos de Informação e a GI, uma visão holística e integrada dos planos a desenvolver, assim como a perspetivação quer em termos físicos (infraestruturas/suporte material), quer em termos lógicos.

Assim, partindo da *Comissão de Preservação e Segurança da Informação* (CPSI) e do seu controlo, esta, deverá ter por base um conjunto de documentos essenciais, de entre os quais se destacam a *Política de Segurança da Informação* e a *Política de Preservação da Informação*.

Como Políticas comuns a ambas as áreas (Preservação e Segurança) a serem estabelecidas pela CPSI, podemos encontrar: *Política de Classificação da Informação; Política de Gestão de Acessos; Política de Acesso à Internet; Política de Utilização do Correio Eletrónico*.

No que diz respeito à Política de Segurança da Informação, esta contém como elementos base:

Sistema de Gestão de Segurança da Informação (SGSI); Política de Backups; Política de Gestão de Passwords; Política de Gestão de Operações; Política de Segurança Física e Ambiental; Política de Segurança de Rede; *Política de Secretária Limpa Ecrã Limpo* (Anexo 1).

Quanto à Política de Preservação da Informação, esta, tem como principais componentes:

Sistema de Gestão de Preservação da Informação; Política de Preservação Física; Política de Preservação Digital; Política de Armazenamento (Archival Storage); Política de Gestão de Operações e Serviços de Preservação.

Todos estes elementos constituintes, tanto da Preservação como da Segurança da Informação, em conjunto servirão de base para que se possa construir quer o *Plano de Preservação da Informação* quer o *Plano de Segurança da Informação* do município do Porto.

Como atributo da CPSI, será também implementado, um *Comité de Planeamento de Preservação Digital* (CPPD) que irá agir como um grupo consultivo para projetos e desenvolvimento de sistemas dentro da CMP que dizem respeito à preservação digital. Este irá desenvolver políticas para os níveis de preservação, metainformação de preservação e ações de preservação incluídas no Plano de Preservação da Informação digital no Município do Porto, com base em requisitos das partes interessadas, as prioridades instituição e as

melhores práticas. O comité irá informar os requisitos do sistema para a implementação dessas políticas.

O CPPD será composto por profissionais da DMSI e da DMAG com perícia e responsabilidades para o programa de preservação digital, políticas e desenvolvimento de serviços. Algum conhecimento adicional pode ser solicitado, através de técnicos destas mesmas unidades orgânicas.

Desta forma, podemos considerar que, tanto a preservação como a segurança da informação enfrentam enormes desafios sendo muitos os riscos e respostas a dar que têm em comum, pelo que, uma das principais preocupações é assegurar a existência de uma GI que se revele eficaz e tenha em conta os atuais problemas advindos, sobretudo, do meio digital, sendo este uma realidade para a qual muitas das organizações só agora despertaram.

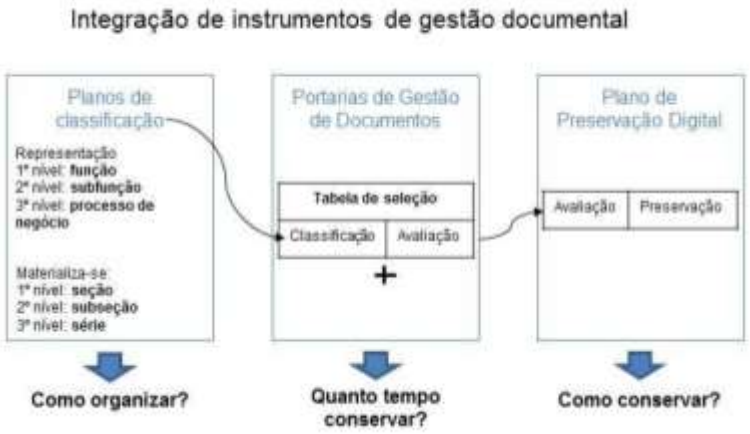


Ilustração 20 - Integração de instrumentos de gestão documental (DGLAB, 2011)

Uma necessidade e alerta que se justificam ainda mais se tomarmos como ponto de comparação a base atualmente usada como orientação para a Administração Pública no que respeita à gestão documental. De facto, trata-se de uma visão que se confina a um âmbito específico mas que pode promover a ideia de uma uniformidade, simplicidade e linearidade que não corresponde à complexidade e às rápidas mudanças a que estão sujeitas as organizações e instituições na sociedade atual.

São diversos os modelos, métodos, metodologias técnicas e ferramentas que estão ao nosso dispor para que possamos chegar com eficácia ao Plano de Preservação da Informação mas não podemos prescindir de uma visão holística, sistémica e integrada, desde logo no que diz respeito às próprias *políticas e estratégias organizacionais* de âmbito mais alargado como são exemplo as *Políticas e Estratégias de GI e TI* que constituem a base de todo este processo e que, consequentemente, culminam na elaboração de um *Plano de Preservação*

Digital, fazendo este parte de uma estrutura informacional de suporte, sendo um entre vários os vários instrumentos a criar para a certificação do Repositório.

Desta forma e como é possível observar na ilustração 21, a visão aqui defendida é que, a montante deve surgir como pedra basilar neste processo, as *Políticas e Estratégias de GI e TI*, embebidas nas próprias políticas e estratégias organizacionais, dando origem ao consequente Plano, quer ao nível da GI como de TI.

Alicerçadas nessas Políticas desenvolvem-se as *Políticas de Preservação e de Segurança da informação*, as quais constituirão, por sua vez, a base dos respetivos *Planos*.

Desta forma, surge uma estrutura que está na base da criação destas Políticas e dos seus respetivos Planos, como podemos verificar pela ilustração 16.

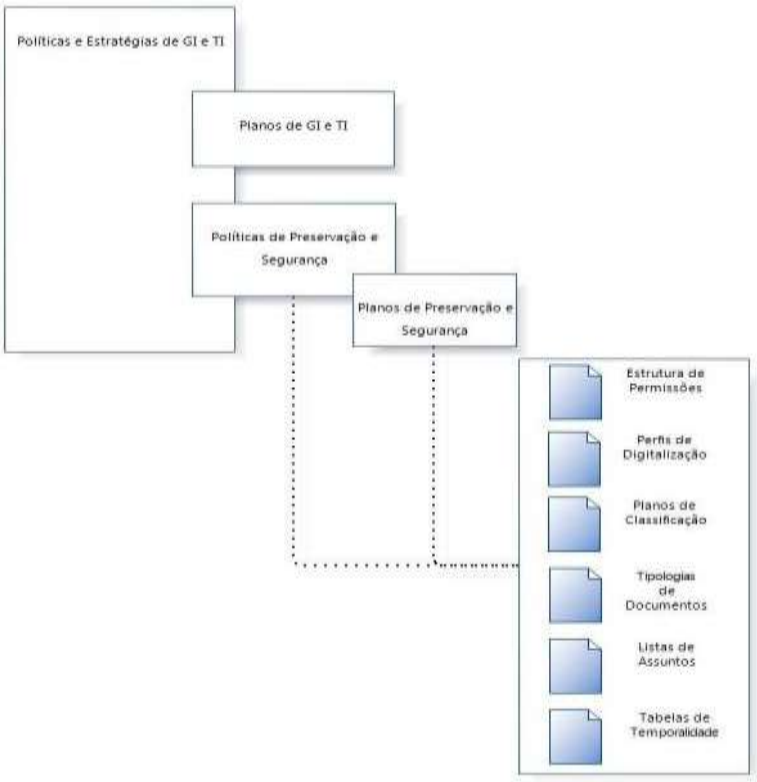


Ilustração 21 - Estrutura de Políticas e de Planos de Preservação e Segurança da Informação

Assim, somente alicerçados pelas políticas e estratégias de GI e TI é possível desenvolver os respetivos planos, bem como as estabelecer as políticas quer de Preservação quer de Segurança da Informação. Com base na construção destas políticas e nos seus planos torna-se exequível a criação de vários instrumentos que integram a chamada Gestão Documental como por exemplo, os planos de classificação, as listas de assunto ou as tabelas de temporalidade.

4.3. O *Documento de Requisitos* para a criação do Repositório Digital Confiável

Este documento tem como propósito especificar um conjunto de requisitos de implementação e inovação para o *Arquivo Digital* da Câmara Municipal do Porto, com vista à definição de bases para uma futura certificação normativa (ISO 16363:2012 – *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*).

Para tal, foi realizado o diagnóstico tendo sido necessário aplicar todos os requisitos compreendidos na norma ISO 16363:2012 ao qual se seguiu uma comparação de correspondência com a tabela de certificação de requisitos do projeto Portico. Na última coluna apresenta-se a conformidade de documentos que foram criados no âmbito deste projeto de dissertação para que possam ser submetidos a avaliação aquando de uma futura auditoria para a certificação do repositório digital.

Esta normativa é relevante por consistir numa revisão da *checklist* do TRAC - *Trustworthy Repositories Audit & Certification: Criteria and Checklist*. De acordo com os seus critérios, torna-se 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 sua missão de preservação digital.

Este documento de especificação de requisitos para a implementação do *Arquivo Digital Confiável da CMP*, encontra-se dividido em quatro capítulos, a saber:

- Introdução – Neste capítulo do documento é abordado o propósito e a vista geral do próprio documento e também o âmbito do repositório.
- Descrição Geral – É apresentada uma primeira secção de descrição geral do repositório, em que de seguida se procede a uma abordagem das funções do repositório assim como as suas características e as dos seus utilizadores.
- Requisitos Específicos – Este capítulo é aquele que contém a tabela de especificação dos respetivos requisitos, encontram-se estes estruturados em três grandes divisões.
- Apêndice – Na última parte do documento de requisitos estão referenciados os prossupostos e as dependências do repositório, bem como as definições, acrónimos e abreviaturas utilizadas na elaboração do documento.

Para a realização da tabela de especificação de requisitos (anexo 3) foi necessário aplicar todos os requisitos compreendidos na norma ISO 16363:2012 ao qual se seguiu uma comparação de correspondência com a tabela de certificação de requisitos do projeto Portico, que foi o primeiro repositório digital certificado por esta normativa, encontrando-se assim as evidências (documentos) que foram avaliados para a certificação deste repositório, assinaladas a "azul". Por último foi efetuada uma conformidade relativamente aos DSE criados no âmbito desta dissertação, permitindo desta forma uma visão mais holística e sistémica de quais os requisitos que o arquivo digital confiável da CMP necessita de cumprir ou elaborar para que possa ser corretamente certificado internacionalmente.

Desta forma, os DSE criados servem como guias de referência para que se estabeleçam os documentos finais para assim se atingir o objetivo da certificação do arquivo digital no município do Porto.

Para uma leitura e compreensão mais inteligível os requisitos foram dispostos conforme se encontram na norma, ou seja, estruturados em três grandes secções:

- Infraestrutura Organizacional;
- Gestão de Objetos Digitais;
- Infraestrutura e Gestão de Riscos de Segurança.

Estas secções encontram-se por sua vez, subdivididas nos vários aspetos relativos à sua secção.

Com a elaboração deste documento torna-se claro que ainda existe um caminho a percorrer até que se consiga atingir a certificação do repositório digital da CMP, embora se encontre dado um passo importante nomeadamente na identificação e elaboração de uma estrutura documental de suporte que sirva de base para o processo de certificação.

Deve se, por isso, ter em conta as constantes inovações tecnológicas com que nos deparamos a cada dia para que o repositório seja capaz de fazer face às necessidades de armazenamento seguro, acesso controlado e preservação de informação (documentos digitalizados e nado-digitais) no longo termo e que possa corresponder à procura interna por parte dos prossumidores que constituem o universo de colaboradores da CMP e respetivos serviços, bem como à procura externa de informação gerida pelo Arquivo Municipal, correspondendo ao requisito de disponibilização e partilha da informação, tão focada nas políticas nacionais e internacionais.

A título exemplificativo do muito trabalho que ainda há para fazer, apresentam-se de seguida dois casos práticos de produção informacional considerados prioritários no contexto

da CMP. Um que ilustra as tarefas e especificações a desenvolver e outro que já resulta do trabalho realizado nos últimos anos e que envolveu a adoção da *estratégia de preservação de normalização de formatos a ingerir no repositório digital*:

1) produção informacional recebida via email;

2) adoção do formato PDF/A.

4.4. O caso da produção informacional via *email*[9]

O uso do @ na sociedade contemporânea é de imediato associado ao *email* (correio eletrónico), e este, por sua vez, ao ato de compor, enviar e receber mensagens através das Tecnologias de Comunicação e Informação (TIC).

De facto, trata-se de um novo meio de comunicação, muito marcado pela informalidade da mensagem / discurso, que rapidamente se arreigou no quotidiano de pessoas, instituições e organizações, substituindo progressivamente as tradicionais vias de comunicação, como o correio postal, fax, telefone, etc.

A velocidade da utilização do *email* nas rotinas diárias não foi, no entanto, acompanhada pela consciencialização da sua importância como "produto informacional". Se o ofício recebido em suporte papel continuava a ser objeto de registo, organização, descrição, instalação e armazenamento sob controlo, para posterior recuperação e uso, o *email* recebido mantinha o cunho informal e um tratamento aligeirado e confinado ao âmbito pessoal do recetor, não se diferenciando, de forma substancial, se, em termos comportamentais, esse recetor se encontrava em contexto pessoal ou no contexto das suas atividades profissionais ou cívicas.

Não obstante, ao nível institucional e organizacional vem ocorrendo nos últimos anos a lenta mas progressiva consciencialização da sua importância como matéria-prima, evidência e suporte para as respetivas atividades, emergindo a necessidade de atribuir ao "*email*"/mensagem recebida por via digital, uma componente formal que assegurasse a manutenção continuada da relevância informacional que possuía, bem como os atributos de autenticidade, integridade, fidedignidade, confidencialidade, inteligibilidade e usabilidade

[9] Este subponto foi objeto de submissão para publicação em revista com *peer review*, tendo sido aceite (Páginas a&b, número 2 de 2014 a publicar), tendo também sido aceite uma comunicação para a edição de 2014 do EIA (Encontro Internacional de Arquivos.) encontrando-se em preparação outras participações em Congressos e Encontros com base no trabalho desenvolvido nesta dissertação.

exigidos à informação que integra o sistema de informação, recurso de gestão e memória de indivíduos, instituições e organizações.

Um processo que, todavia, está longe de ser linear e que se confronta com consideráveis dificuldades. Desde logo ao nível da dissociação do ato do foro pessoal, daquele que respeita ao foro institucional/organizacional em que se insere o "agente", até às dificuldades inerentes ao uso da tecnologia e à rápida obsolescência que lhe é inerente, a par da crescente perceção da complexidade decorrente da pluridimensionalidade que envolve a unidade informacional recebida ou expedida via *email* e que, de facto, integra um conjunto de componentes informacionais e meta-informacionais digitais que, só em conjunto, garantem a unidade de sentido que constitui, efetivamente, a unidade de informação.

Pretende-se, assim, apresentar o que é e como funciona genericamente o *email,* bem como a importância que lhe deverá ser atribuída no âmbito da *Gestão da Informação* (GI).

Uma perspetivação que envolve o desenvolvimento de uma política de gestão de *emails*, o processo de gestão do *email* ao longo de todo o seu ciclo de vida, assumindo a sua preservação numa perspetiva de acesso e uso continuado no longo prazo, só possível se for efetivamente integrada nos processos de gestão do *sistema de informação organizacional* (SIO), da produção/captura à conservação definitiva.

Uma reflexão que aborda apenas um tópico, dos muitos que o desafio da preservação da informação em meio digital coloca no topo das prioridades informacionais de instituições e organizações, mas que contribuirá decisivamente para o desenvolvimento do *Plano de Preservação da Informação* que deverá existir qualquer que seja a instituição, a organização ou setor de atividade em que estas se insiram, e que, neste caso, teve como contexto o projeto desenvolvido no Município do Porto.

4.4.1. Em que consiste e como funciona o email?

Electronic Mail, e-mail, email ou *correio eletrónico* designa, desde logo, um serviço que permite compor, enviar e receber mensagens através de redes e sistemas eletrónicos de comunicação.

Uma mensagem de *email* é estruturada por dois componentes essenciais, o cabeçalho da mensagem e o corpo da mensagem, constituído pelo conteúdo do *email*, a que se acrescem os anexos. O cabeçalho da mensagem contém informação de controlo, incluindo, como elementos básicos, o endereço de correio eletrónico de um remetente e um ou mais endereços de destinatários.

Quando um email é enviado, a mensagem é encaminhada de servidor para servidor,

para o servidor de *email* do destinatário. Mais precisamente, a mensagem é enviada ao servidor de correio encarregado de transportar *emails*, chamado MTA (*Mail Transport Agent*), para o MTA do destinatário. Este entrega o *email* para o servidor de correio recebido, chamado de MDA (*Mail Delivery Agent*), que o armazena, aguardando que o utilizador o aceite. Na Internet, os MTA comunicam entre si utilizando o protocolo SMTP, e, assim, são chamados logicamente servidores SMTP (*Service Mail Transfer Protocol*). São dois os principais protocolos utilizados para a recuperação de *email* do MDA:

- POP3 (*Post Office Protocol*), o mais antigo e usado para a recuperação de *email* e que, em certos casos, deixa uma cópia no servidor.
- IMAP (*Internet Message Access Protocol*), que é usado para coordenar o estado do email (ler, apagar, mover) em vários clientes de email. Com o IMAP, é guardada no servidor uma cópia de cada mensagem, de modo a que a tarefa de sincronização possa ser concluída.

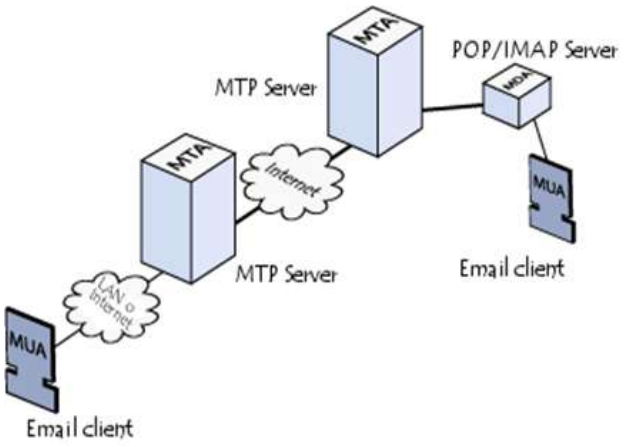


Ilustração 22 - Processo de envio/receção de um email

Os MTA funcionam como uma estação de correios (a área de triagem e o carteiro, que lida com o transporte de mensagens), enquanto o MDA funciona como caixa de correio, que armazena mensagens (tanto quanto o seu volume permita) até ao momento em que os destinatários verificam a caixa. Isto significa que não é necessário que os destinatários estejam ligados para lhes serem enviados *emails*. Para manter a confidencialidade dos *emails* de todos os utilizadores, o MDA é protegido por um nome de utilizador (*login)* e por uma senha (*password*).

A recuperação de *email* é efetuada através de um programa de *software* designado por MUA (*Mail User Agent*). Quando o MUA é instalado no sistema operativo do utilizador, é denominado de cliente de *email* (como o *Mozilla Thunderbird* ou o *Microsoft Outlook*), quando é uma *interface web* usada para interagir com o servidor de mensagens recebidas, é

conhecido por *webmail*.

4.4.2. A gestão e preservação de emails

Identificado o contexto tecnológico torna-se necessário perceber que o que está em causa não é apenas o "serviço" referenciado mas a gestão do "produto informacional", conscientes que, "numa qualquer organização a preservação começa, desde logo, com a análise dos contextos de produção da informação, dos seus fluxos, do seu uso, dos meios de armazenamento e acesso, bem como dos instrumentos de controlo existentes (planos de classificação, linguagens de indexação, controle de autoridade nos pontos de acesso, etc.), do processo de automação desenvolvido e a desenvolver, apontando para a gestão integrada do ciclo de vida da informação (integrando, por exemplo, o *software* aplicacional e de suporte com o *software* de gestão do sistema de informação), o que terá repercussão na alteração dos processos de gestão da informação, atores e serviços responsáveis. Esta análise será essencial, por exemplo, para a especificação/validação dos requisitos de aquisição/desenvolvimento de aplicações informáticas ditas de Gestão Documental e de *Workflow*, bem como para a desmaterialização sustentada dos processos organizacionais" (Pinto, 2014).

Tendo em mente que o Sistema de Informação Organizacional (SIO) 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" (Silva, 2006) e, numa perspetiva holística e sistémica, a gestão da informação procura assumir um único ciclo de gestão que acompanha todo o ciclo de vida da informação e, neste caso, todo o ciclo de vida do *email*.

A preservação da informação é assumida como uma *variável da gestão da Informação*, estando, assim, presente em todo o ciclo de vida informacional, convocando as áreas da Produção Informacional, da Organização e Representação da Informação e do Comportamento Informacional e podendo ser considerada quer nos estudos científicos, quer na resolução de casos concretos, mantendo os objetivos de garantir a autenticidade, fiabilidade, integridade e inteligibilidade da informação, bem como o acesso continuado no longo prazo.

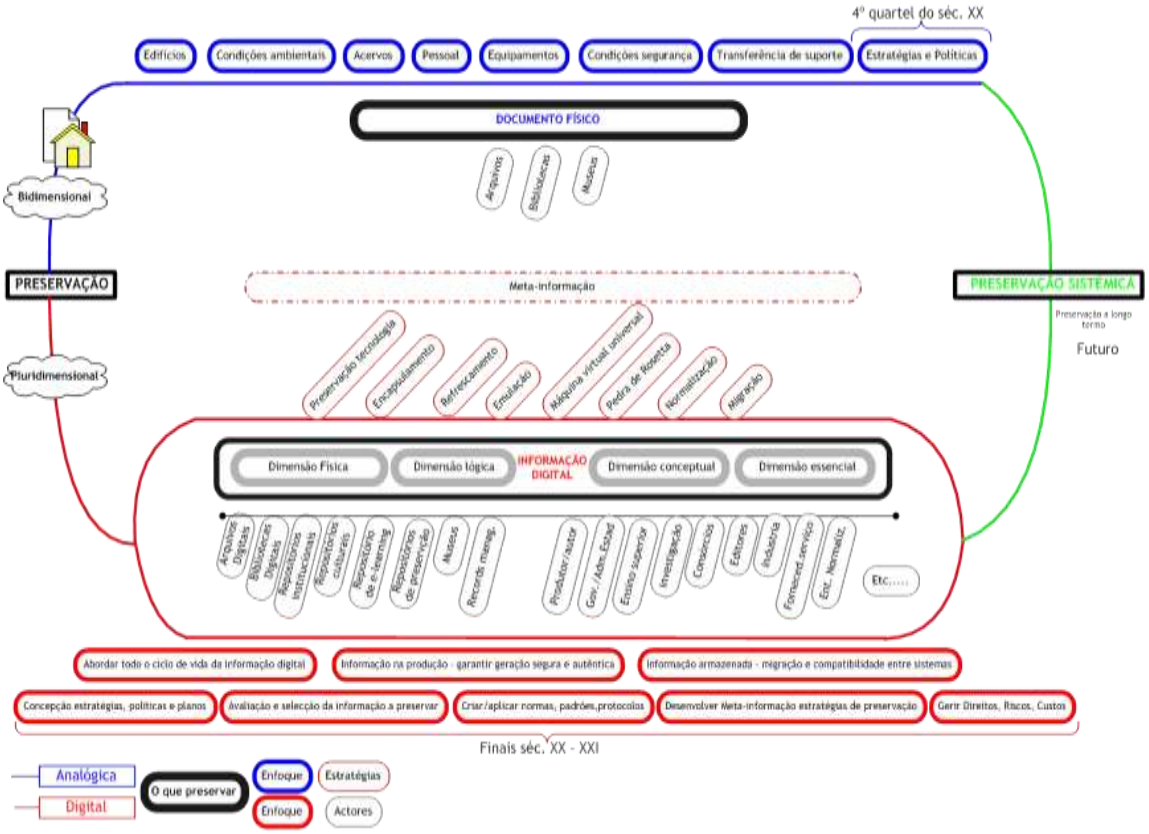


Ilustração 23 - Um percurso que conduz à Preservação da Informação em sentido sistémico - PRESERVMAP (Pinto, 2010)

Como refere Pinto (2014), ultrapassando posicionamentos que dicotomicamente enfatizavam ora a dimensão informacional, de difusão e de acesso, sobretudo ligado a bibliotecas, ora a dimensão probatória e de armazenamento e preservação a longo prazo, que colocava a questão da "autenticidade" no centro das preocupações da preservação dita digital, sobretudo em arquivos, ou que apontavam para o pendor tecnológico, temos decididamente que atender a todas as fases do ciclo de vida da informação e integrar o problema da preservação em meio digital no funcionamento corrente da organização, nas suas políticas e estratégias, bem como no quadro da implementação de modelos de processos e relações formais entre os diferentes atores no âmbito da economia/sociedade digital, apontando para a própria certificação dos repositórios, processos e serviços de gestão de informação (incluindo a gestão da Preservação), solidamente alicerçados numa base teórico-metodológica que suportará a efetiva gestão do Sistema de Informação Organizacional (SIO).

A informação a preservar, deverá ser considerada na sua globalidade e complexidade apelando a uma preservação sistémica aos vários níveis e entre os vários níveis a saber: nível da unidade informacional (informação e metainformação); nível do SIO. (seja digital, analógico ou híbrido); nível do STI (toda a arquitetura computacional), ao nível da

organização (estrutura, processos, pessoas, SIO e STI; contexto interno e externo); nível interorganizacional; nível nacional; ao nível global (Pinto, 2010).

Também no casos da produção informacional via *email*, e independentemente desta integrar um um SIO totalmente digital, híbrido ou mesmo analógico (via versão impressa), será o sistema de informação e a missão/necessidades da Organização que o produz, acumula e usa que norteia a função preservação e os profissionais da informação por ela responsáveis, não estando a sua existência/configuração condicionada, por exemplo, por uma determinada tipologia de serviço de informação ou prévia classificação de caráter patrimonial, nem devemos aqui consagrar qualquer distinção em termos de suporte como indiciado pela utilização do termo "Preservação Digital" (Pinto, 2014).

Significa, pois, que a preservação da informação começa, desde logo, na concepção e implementação da plataforma tecnológica na qual será produzida, recebida, capturada, organizada, armazenada e difundida a informação, nomeadamente no *software* utilizado, nos formatos adotados, na recolha, na fase e momento próprio, da metainformação administrativa, técnica, estrutural, descritiva ou de preservação que permita a sua futura referenciação 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. Um papel que não poderá ser imputado a "informáticos", mas que convoca permanentemente parcerias entre o gestor da informação e os diferentes atores, informáticos incluidos (Pinto, 2014).

Como se constata pela ilustração 4, desenvolve-se um complexo **processo integrado de gestão** que convoca conhecimento teórico, instrumentos, ferramentas e técnicas de operacionalização que estarão presentes ao longo de todo o ciclo de vida e gestão da informação, abarcando momentos que, ainda hoje, são frequentemente assumidos de forma segmentada e sem articulação entre si.

4.4.3. A política de gestão do email

Inserida na *Política de Gestão da Informação* da organização, terá, pois, que ser considerada uma *Política de Gestão de Email*. É certo que esta já vem sendo adotada por várias organizações, apesar de maioritariamente ativada pela via informática e ainda muito confinada a aspetos como a segurança e a confidencialidade, não perspetivando, por exemplo, o processamento, armazenamento e preservação dos *emails* para acesso continuado no longo prazo.

A definição de políticas tende a resultar do impacto da utilização das TIC em termos

dos potenciais prejuízos que podem trazer aos colaboradores no contexto organizacional. Foi o caso do Departamento de Administração do Estado do Wisconsin, nos Estados Unidos, no âmbito do qual foi desenvolvida uma *Política de Uso de Internet e Email* com vista a incentivar o uso adequado da Internet e do *email* por parte dos funcionários desse mesmo departamento, minimizando os riscos de utilização de ambas as ferramentas.

As diretrizes incentivam todos os funcionários a usar o bom senso quando recorrem à Internet do Departamento ou acedem ao *email*. Embora essas diretrizes definam como os funcionários podem ou não podem utilizar a Internet e o *email*, estas não conseguem cobrir todas as situações possíveis, surgindo aqui o apelo ao bom senso e sentido profissional de todas as partes. A título de exemplo, enquanto o uso pessoal limitado da Internet e do email é permitido, o acesso excessivo a *sites* não relacionados com trabalho não é permitido (caso do desporto, férias e planeamento de viagens, produtos de consumo e entretenimento).

De acordo com Prom (2011) existem três passos básicos que as instituições que visam implementar projetos de preservação de *email* devem realizar: a definição de políticas, a escolha de ferramentas apropriadas e a sua implementação à luz de fatores ambientais locais e recursos disponíveis. Desta forma, as instituições devem começar por definir as *Políticas de Gestão* e de *Preservação de email*.

Segundo Prom (2011), as políticas de *email* devem esboçar:

1. Um compromisso institucional para a preservação de *email* e ações específicas que serão tomadas, assim como apoiar procedimentos;
2. As expectativas do utilizador final, as responsabilidades e os direitos sobre o acesso, uso, privacidade e controlo das unidades informacionais que integram um *email*.

As *Políticas* devem identificar os "tipos" de *email* que são efetivamente pertinentes e relevantes para a atividade, gestão e memória organizacional/institucional.

Por sua vez, os *Procedimentos* vão definir como os sistemas apoiam a política, e como os utilizadores interagem com os sistemas, permitindo à organização gerir o *email* durante todo o ciclo de vida.

Definidas as políticas adequadas, as instituições devem selecionar e implementar ferramentas apropriadas que suportem as políticas. A implantação tem de ser realizada em colaboração com os utilizadores de *email*, os gestores de informação e os gestores de TI. As instituições devem ter particular atenção em não impor inadvertidamente configurações de preservação que possam dificultar o envolvimento dos utilizadores. Isto pode ser conseguido fornecendo espaço de armazenamento adequado e evitando configurações de autoeliminação.

Quanto aos utilizadores, estes devem, em primeiro lugar, familiarizar-se com o funcionamento do serviço de *email* que utilizam, bem como os "clientes" que usam para operarem. Entendida a estrutura das contas que possuem e a sua configuração para gerir o *email* de uma forma mais eficaz, os utilizadores podem usar ferramentas de *backup* simples, (como o aplicativo gratuito *MailStore Home* ou a ferramenta de *backup Time Machine* da *Apple*), para garantir a salvaguarda de uma cópia dos seus *emails* num local seguro, separado das cópias utilizadas diretamente pela aplicação informática.

Estes podem, ainda, utilizar um serviço baseado em nuvem (*cloud)* para fazer *backup* dos *emails*. Porém, devem considerar cuidadosamente os termos do serviço antes de o subscreverem. Alguns serviços de *backup online*, (tais como *Carbonit*e e *Mozy*), realizam um *backup* automático de tudo que exista nas pastas de dados de um computador pessoal, incluindo cópias locais de mensagens de *email,* mantidos em qualquer formato que a "máquina" cliente do utilizador utilize para armazenar.

Segundo a *Osterman Research* (2010) é importante perceber que fazer *backup* e arquivar *emails* são duas práticas cruciais embora não sejam substitutas uma da outra, ou seja, a diferença fundamental entre *backup* e *arquivo*, é que o primeiro é concebido como uma solução de curto prazo, tática, com foco na informação que é importante para restaurar o bom funcionamento de um servidor, enquanto o arquivo é uma solução mais estratégica e de longo prazo, focada em informação e metainformação que é importante para manter a integridade de toda a informação gerada ou recebida por uma organização ou instituição.

4.4.4. A produção/captura de email

Os The National Archives (TNA-UK) (2011), um serviço especializado de arquivo de âmbito nacional do Reino Unido, produziram um documento que tem como objetivo estabelecer as *Orientações para a Gestão e Preservação de emails* (The National Archives - *Email Management and Preservation Guidelines*), ou seja, fornecer um aconselhamento básico, para que o email seja gerido de uma forma que facilite a sua preservação a longo prazo e / ou eventual transferência para um *repositório de arquivo*.

Segundo os TNA (2011) *"Email programs are one common technology that people use to communicate with others, to share information, and to record decisions. The semi-formal nature of an email message means that it provides greater reliability as evidence than, say, a text message or a conversation".* Por esta razão, os *emails* devem ser geridos de forma adequada depois de terem sido enviados ou recebidos.

Assim e devido ao facto de cada programa de *email* guardar as mensagens de forma

diferente, o Guia referenciado aplica quatro princípios gerais para que cada pessoa possa gerir o seu correio eletrónico com vista a uma preservação eficaz a longo prazo.

- Usar as funções de "arquivo" do *email* com cautela: usar a função de "auto-arquivo" ou "arquivo" de um programa de *email* com cuidado, sendo necessário algum tempo para compreender e configurar estes recursos;
- Saber onde é armazenada a mensagem de *email* produzida ou recebida, pois os programas e servidores de *email* podem gravar ficheiros em vários locais do disco rígido;
- Organizar as suas mensagens para preservação, existindo muitas formas de organizar *email* "não-corrente" para que seja acessível de uma forma otimizada;
- Independentemente do método escolhido, o sistema deve ser fácil de usar e deve preservar as mensagens que têm valor a longo prazo;
- Usar as pastas locais de forma inteligente: às vezes é necessário armazenar as mensagens num computador local, em vez de num servidor central, devido às quotas impostas ou outro tipo de restrições.

Por seu lado, os *National Archives and Records Administration* (NARA, US), uma entidade congénere da referida, publicaram em 2011 o artigo *Guidance Concerning the use of E-mail Archiving Applications to Store E-mail* onde são apresentadas as vantagens e desvantagens das aplicações de arquivo de *email*, no contexto de áreas referenciadas como de "Gestão Documental" e de "Gestão de Arquivos". Este artigo fornece aos órgãos federais linhas orientadoras relativas ao uso de aplicações de arquivo de *email* e tecnologias semelhantes para a respetiva gestão. Salienta que, apesar dessas aplicações de arquivo de *email* poderem oferecer benefícios para os processos desenvolvidos por um determinado organismo, estes podem ser limitados na sua capacidade de manter e organizar a informação de acordo com os requisitos legais de gestão, regulamentos e políticas.

Tendo cada aplicação diferentes características e diferentes pontos fortes e dependendo da própria organização e dos seus objetivos comerciais, as aplicações de arquivo de *email* podem oferecer vários benefícios:

- Um armazenamento mais eficiente de *email*, pois é movido, de uma rede distribuída de servidores, aplicativos de *desktop* e outros locais a serem geridos, para um único lugar;
- A capacidade de pesquisa eletrónica avançada de conteúdo que pode ser pertinente para, por exemplo, uma intimação judicial, um pedido de acesso à informação, ou

algum propósito semelhante;

- Auxilio no *backup* e na recuperação de desastres.

De acordo com a iniciativa desenvolvida pelo Governo do Canadá deverá ser acompanhado todo o ciclo de vida dos registos de *email* a saber:

- Mensagens de *email* relativas aos negócios/atividades que devem ser mantidas pela instituição:
    - Mensagens de *email* criadas, recolhidas, recebidas ou transmitidas durante o curso normal das atividades da organização são registos do Governo do Canadá e por isso devem ser mantidas para garantir a integridade da memória da governação.
    - Mensagens de *email* cujo conteúdo seja de natureza pessoal, não são registos do Governo do Canadá, os exemplos incluem mensagens de email sobre informações pessoais de um funcionário, emails relativos a passatempos, publicidade não solicitada, etc. Essas mensagens devem ser apagadas uma vez que não são úteis.
- Mensagens de *email que* devem permanecer intactas:
    - Sempre as que mensagens eletrónicas e os seus anexos dizem respeito às atividades da instituição, estas devem permanecer intatas em termos da sua estrutura (*layout* ou formato e *links* para os anexos e documentos relacionados), conteúdo (a informação contida na mensagem) e contexto (informações relativas ao remetente e destinatários, bem como qualquer informação de cabeçalho e os dados de transmissão, tais como data e hora).
    - Mensagens de *email* devem ser capturadas num sistema informacional reconhecível:
    - Mensagens eletrónicas relacionadas com o Governo do Canadá devem ser arquivadas no sistema de informação de acordo com as práticas de gestão da informação da instituição.
    - Mensagens de *email* devem ser geridas de forma eficiente e eficaz:
    - Mensagens eletrónicas devem ser geridas de acordo com as boas práticas de gestão de informação/registos, a fim de preservar a integridade desta, atender às necessidades de negócios da instituição e cumprir com as responsabilidades.
    - Boas práticas de gestão de informação direcionada ao ciclo de vida do registo

criado, da fase de Planeamento à de Avaliação, irão garantir que as mensagens eletrónicas permanecem acessíveis, ou seja, recuperáveis e legíveis, ao longo do tempo.

- A gestão de *email* deve ser apoiada por políticas corporativas, diretrizes e procedimentos:
- As instituições governamentais devem garantir que as mensagens de *email* e os respetivos anexos permaneçam acessíveis no arquivo da instituição durante a sua vida útil até à sua eliminação final. A elaboração de políticas institucionais, diretrizes e procedimentos devem abarcar aspetos como:
    - Legislação e regulamentos específicos da instituição;
    - Gestão do sistema de *email* e responsabilidade pela informação contida nas mensagens de email enviadas e recebidas através do sistema;
    - Uso do sistema pelos funcionários para assuntos pessoais ou privados;
    - Responsabilidades para a gestão de mensagens eletrónicas, incluindo a identificação do centro responsável pela gestão do arquivo da instituição;
    - Responsabilidades e diretrizes para a retenção e eliminação dos registos de *email* e o papel do utilizador nesse processo.
    - Acesso e segurança de mensagens eletrónicas.

4.4.5. A avaliação e política de retenção

Em rigor, e numa perspetiva sistémica e integrada da gestão da informação, o *email* é apenas um novo meio de comunicação da informação que constitui a mensagem a comunicar. Como tal, essa informação produzida, recebida e acumulada no contexto da atividade da organização integra o seu sistema de informação e deve ser gerida com a especificidade requerida pelas propriedades que possui no âmbito de uma avaliação que considere sistemicamente o todo informacional (cf. Silva e Ribeiro, 2000 e Ribeiro e Silva, 2004)[10].

Segundo Celorrio (2010), num sistema de *email* coexistem mensagens irrelevantes, mensagens originais assinadas que devem ser mantidas, mensagens com informação

[10] SILVA, Armando B. Malheiro da; RIBEIRO, Fernanda – A Avaliação em Arquivística: reformulação teórico-prática de uma operação metodológica. *Páginas a&b: arquivos e bibliotecas*. Lisboa. ISSN 0873-5670. 5 (2000) 57-113; RIBEIRO, Fernanda; SILVA, Armando Malheiro da – A Avaliação de informação: uma operação metodológica. *Páginas a&b: arquivos e bibliotecas*. Lisboa. ISSN 0873-5670. 14 (2004) 7-37.

confidencial e possíveis ações judiciais e mensagens com anexos. Desta forma torna-se essencial fazer uma seleção, uma vez que não é de todo aconselhável optar por criar uma série documental que inclua todos os *emails*.

Celorrio (2010) recomenda três passos no processo de seleção:

- Formalizar os *emails* como documentos completos, utilizando os mecanismos de autenticação necessários;
- Incluir as regras de avaliação dentro das mensagens formalizadas pela classificação e as ligações necessárias com as regras de auto-execução;
- Eliminar as mensagens não formalizadas ou não classificadas dentro de 15-30 dias da data de envio ou receção.

Há, no entanto, questões básicas elencadas por Celorrio que se podem colocar como ponto de partida mas que não obstam ao desenvolvimento de um processo de avaliação e seleção no âmbito do processo e/ou série informacional e entre as diferentes séries e processos de negócio, nomeadamente:

- A mensagem está relacionada com as atividades e funções da organização?
- A mensagem contém informação com utilidade imediata e unicamente de curto prazo?
- É um duplicado que chega para conhecimento?
- É um esboço/rascunho a eliminar com a criação da versão final?

Em matéria de gestão de *emails* e documentos eletrónicos em geral, a autora defende que a solução é a implementação de um *sistema de gestão de documentos eletrónico* (EDMS) a menos que se prefira transferi-los para suporte analógico. Esta é uma abordagem básica, ainda em utilização por inúmeras organizações, quer de âmbito público como privado, mas que ignora o ponto de partida fundamental que consiste na constatação de que o que nasce em meio digital só poderá ser efetivamente preservado em meio digital. O próprio sistema de "Gestão Documental" poderá ser contraproducente caso não seja assumido no âmbito de uma política integrada de gestão de informação.

Como se constata, dado o crescimento exponencial da utilização da comunicação via *email* e a facilidade da sua produção através das TIC, o processo de avaliação, seleção e determinação do destino final adquire um papel determinante entre os procedimentos de gestão das mensagens de *email*, influenciando, inclusive, os custos relacionados com a sua posterior gestão e preservação.

A eficaz gestão do *email* não só é necessária como se afirma como um objetivo fundamental no âmbito da gestão da informação. Nos *emails* está contida informação relevante que, em muitos casos, pode ser o único registo criado que documenta uma transação, decisões tomadas ou a determinação ou interpretação política.

As regras devem especificar consistentemente quer a estrutura organizacional e informacional em que se inserem, quer a definição das permissões para quem pode aceder, alterar ou excluir mensagens, anexos e outros registos.

Lundgren (2009), acresce que para atingir este objetivo as organizações devem guiar-se através do processo de desenvolvimento, implementação, monitorização e auditoria do que designa como uma completa política de retenção de *email* utilizando os 10 passos que se seguem:

1. Definir uma política de retenção de *email*;
2. Eliminar as variáveis dificultando a centralização;
3. Instruir os funcionários sobre a política de retenção;
4. Incorporar os regulamentos relevantes para a política de retenção;
5. Identificar os papéis com requisitos de retenção exclusiva;
6. Equilibrar as diretrizes de retenção relacionadas com os custos de TI;
7. Fornecer aos funcionários acesso às mensagens arquivadas;
8. Assegurar que as políticas de retenção possam acomodar os documentos de retenção legal;
9. Verificar que todas as mensagens são arquivadas;
10. Usar a tecnologia para aplicar políticas de retenção.

Numa perspetiva sistémica as mensagens de *email* integram o conjunto informacional que corporiza o sistema de informação e, como tal, serão objeto da operação de avaliação da informação que se deverá orientar pelas propriedades da informação, tal como proposto por Silva e Ribeiro (2000).

4.4.6. A organização e armazenamento de emails

De acordo com a HP (2010), as organizações de todas as dimensões enfrentam o desafio do crescimento explosivo de *email*. Em 2010 já era referenciado que 85% das comunicações empresariais ocorriam através de *email* e 183 bilhões de mensagens de

negócios eram enviadas por dia[11].

Por seu lado, os "gestores de armazenamento" tentam conter uma espiral de custos de gestão e armazenamento das caixas de correio e os administradores e advogados corporativos necessitam de uma cada vez mais rápida e rentável forma de pesquisar e recuperar a informação contida em *emails*.

Numa abordagem de âmbito geral, Henriksen *et al.* (2013) elaboraram um guia de boas práticas para a construção de uma infraestrutura de armazenamento digital com vista à preservação de informação digital no longo prazo.

Nesse estudo apresentam uma visão geral dos tipos de suporte de armazenamento e dos sistemas disponíveis para a criação do que consideram "uma boa infraestrutura de armazenamento". Cada tipo de armazenamento é explicado em termos de suas propriedades e quais as vantagens e os riscos do sistema com vista à preservação a longo prazo.

Identificam, assim, várias infraestruturas de armazenamento podendo estas ser de diferentes tamanhos:

- Um pequeno sistema que pode ser autónomo e manipulado manualmente;
- Um sistema maior mas que muitas vezes precisa de sistemas de gestão automatizados e funções de recuperação.

Alguns tipos de suportes de armazenamento surgem e desaparecem rapidamente, tal como os formatos e o próprio *software*. Um exemplo de *hardware* que já se encontra obsoleto são as fitas DAT (*Digital Audio Tapes*) e também as muito comuns disquetes.

De acordo com os referidos autores as propriedades requeridas em termos de suportes de armazenamento são:

- **Fácil de usar**: Um pequeno número de meios de comunicação é mais fácil de manusear e manter;
- **Fácil de copiar**: Quão rápido e fácil é copiar entre dois meios do mesmo tipo? Pode ser feito sem o risco de perda de dados?
- **Ampla utilização**: Quanto mais difundida é a tecnologia, mais tempo tenderá a sobreviver no mercado;
- **Baixo preço**: Qual é o custo da obtenção de novas versões do mesmo suporte? Quanto espaço de armazenamento pode obter com a verba disponível e quanto será

[11] Dados referentes ao ano de 2010.

necessário no futuro? Pensando a longo prazo, isto é, o que no arranque pode ser uma solução barata, no longo prazo pode tornar-se caro.

- **Durabilidade**: Qual é a expectativa de vida do suporte, antes de ocorrer qualquer risco de erro? Certificar se é um formato estável e se tem um ciclo de vida bem conhecido.

Os autores apresentam, ainda, algumas vantagens e desvantagens por cada tipo de suporte de armazenamento que se sistematizam de seguida:

Tabela 2 - Tipos de suporte de armazenamento (Adapt. de Henriksen, et al., 2013)

Tipo de Suporte	Vantagens	Desvantagens
Fitas de Áudio (DAT)	Baixo preço. Escalabilidade. Poupança de energia. Taxas relativamente elevadas de transferência. Baixas taxas de erro em relação a unidades de disco rígido. Suporta compressão e encriptação.	Escreve de forma linear, o que significa que o acesso excessivo não é recomendado, pois a fita vai sofrer um maior desgaste. Os tempos de acesso são longos. Movimentação manual a menos quando conectados em carregadores automáticos. Pode tornar-se uma solução cara, se são necessários carregadores automáticos robóticos. O equipamento leitor / gravador não é compatível com as futuras gerações e precisa ser atualizado.
Discos rígidos	Acesso aleatório e rápido. Contém índice de ficheiros	Para dimensionar o conteúdo pode ser uma solução cara.

Tipo de Suporte	Vantagens	Desvantagens
	gerido por sistemas de índices de ficheiros. Múltiplos ficheiros podem ser abertos e utilizados ao mesmo tempo por vários utilizadores. Portátil entre plataformas e sistemas operacionais. Escalável.	Desperdiça energia. Sistemas SATA HDD têm provado ter taxas de erro mais elevadas do que as fitas magnéticas. Vida útil de apenas cinco anos.
Discos de estado sólido (SSD)	Baixo consumo de energia. Tamanho compacto. Resistente ao choque. Alto desempenho para acesso a dados aleatórios.	Preço elevado. Baixo desempenho na escrita de dados (isso pode ser melhorado com um determinado *software* incorporado). Tempo de vida incerta.
Discos Óticos (*Blu-Ray*)	Possui uma melhor qualidade de imagens que proporciona um melhor aproveitamento de um vídeo, filme. Contém grande espaço de memória para armazenar dados.	É uma tecnologia cara. Os equipamentos e manutenção deste tipo de tecnologia têm custos elevados.
Armazenamento em nuvem (*Cloud*)	Custo / benefício. Pode ter redução de custos. Uma menor pressão sobre o departamento de TI para manutenção. Fácil acesso, também fora das instalações da organização. Melhor e mais fácil colaboração – geograficamente.	Segurança. Sem plano de preservação Sem controlo e verificação da integridade dos ficheiros. Ainda não é ideal como uma solução de preservação a longo prazo. Menos controlo sobre os próprios conteúdos.

Incidindo especificamente sobre a gestão de *email,* Houston (2008) analisa a identificação, organização e preservação de email com vista à sua preservação a longo termo.

De acordo com o *Electronic Communication Guidance for University Records*

(UNIVERSITY OF WISCONSIN, 2012) deve-se começar com a criação de um sistema normalizado de arquivo (etiquetas/metainformação, ordenação e organização) para armazenar as mensagens e para se poder recuperar e usar a informação eficientemente ou tomar decisões com base nesta.

Deverão ser usados estruturas de nomeação de ficheiros consistentes dada a sua importância para aceder e recuperar informação de uma forma adequada, permitindo, assim, responder a pedidos ou agir no âmbito do fluxo de trabalho diário.

Ainda segundo o *Electronic Communication Guidance for University Records*, (UNIVERSITY OF WISCONSIN, 2012) uma sugestão para a criação de uma estrutura de arquivo é utilizar como referência as políticas de retenção e arquivo de correspondência em papel, o que, na nossa perspetiva deverá ser ponderado não em função unicamente desta série em especifico mas no âmbito do processo informacional em que se integra cada *email*, tal como a restante produção informacional, a série correspondência tenderá a ser uma entre várias.

Desta forma, e uma vez que foi desenvolvida uma estrutura de pastas, que, na nossa perspetiva, tende a coincidir com a estrutura de classificação adotada pela organização, devendo esta ser utilizada e aplicada consistentemente para facilitar o acesso, recuperação e consulta de informação.

Estando a gestão de *email* orientada para o utilizador, cabe, desde logo, ao utilizador/produtor (que identificamos como possuidor) gerir o seu email de forma adequada e de acordo com as políticas da organização, a que acrescemos a necessidade do seu desenvolvimento sob uma abordagem holística, sistémica e integrada do SIO face à Missão e ação da organização.

A título exemplificativo é apresentado pelo *Electronic Communication Guidance for University Records*, um quadro geral de *emails* rececionados que apresenta as seguintes tendências:

- Aproximadamente 50% dos *emails* serão designados como *não-registos*.
- Cerca de 25% será de natureza transitória.
- Cerca de 15% será de natureza rotineira.
- Cerca de 10%, ou menos, será gerido de acordo com a análise resultante do processo de avaliação e seleção da informação (UNIVERSITY OF WISCONSIN, 2012).

Desta forma, a chave para a gestão de *email* é excluir os *não-registos* (informação

transacional) e gerir quaisquer registos de rotina ou transitórios, segundo a Tabela Geral de Temporalidade aplicável à informação de comunicação organizacional.

Independentemente das diferenças patentes nas abordagens desta fase do ciclo de vida da informação, ressalta-se o foco na operação cada vez mais importante da "Avaliação da Informação" que, na nossa perspetiva, deverá ser objeto de um apurado estudo do sistema de informação e ocorrer cada vez mais no início do ciclo de vida e de gestão da informação.

4.4.7. A preservação de emails

Tal como qualquer outro tipo de informação, a preservação da produção informacional comunicada via *email* terá que considerar quer a componente física, quer digital. Como refere Pinto (2010), estando em causa informação produzida em meio digital, a questão física também se coloca, dado que aquela mantém a necessidade de ser registada, uma materialização que ocorre através de plataformas tecnológicas com componente de *hardware* e *software* (física e lógica), podendo mesmo ser acompanhada pela impressão da mensagem e/ou anexos em papel.

Na perspetiva da unidade informacional esta apresenta-se como pluridimensional, isto é, possuindo várias dimensões e exigindo cada uma delas uma atenção particular: a dimensão física, a dimensão lógica, a dimensão conceptual e a dimensão essencial (as três primeiras referenciadas e designadas como "*multi-layered nature of digital objects*" por Thibodeau, 2002).

A preservação da informação digital requer, pois, diferentes abordagens, quer técnicas, quer organizacionais pelo que, abordam-se, de seguida, alguns dos principais problemas e estratégias de preservação a considerar no caso de *emails*.

4.4.7.1. Problemas para a preservação de emails

A preservação de *emails* coloca vários problemas, muitos deles similares à restante informação digital. Apesar de ser mais fácil criar, corrigir e distribuir informação digital, os sistemas de armazenamento são mais frágeis do que os tradicionais. Garantir o acesso a longo prazo da informação armazenada digitalmente é um desafio e, cada vez mais, é vista como uma parte importante da gestão de informação em meio digital.

A preservação envolve a retenção da informação, relativa quer ao "objeto" quer ao conteúdo, sendo de acrescer, em termos de complexidade, a dependência que do "meio" tecnológico que medeia a produção, gestão e acesso à mesma. A constante evolução da tecnologia provoca ciclos de obsolescência extremamente rápidos, provocando uma

descontinuidade com a consequente possibilidade de inacessibilidade ao nível das várias dimensões identificadas. Daí que se possa afirmar que os recursos informacionais digitais apresentam mais problemas do que os recursos tradicionais.

Centrando-se na preservação de *emails* a longo prazo, Houston (2008) considera ser necessário questionarmo-nos sobre três vertentes essenciais:

- O *Suporte/plataforma*: o meio de armazenamento é durável o suficiente para manter a sua integridade ao longo do tempo?
- A *Mensagem*: o conteúdo do documento é devidamente preservado?
- A *Metainformação*: existe suficiente informação complementar para contextualizar o documento?

Estes componentes deverão existir em simultaneidade. Caso se perca apenas um desses componentes da mensagem eletrónica, a preservação desta não será realizada de forma adequada.

Tomando como exemplo o armazenamento da informação em meio digital, ter-se-á que referenciar este aspeto da preservação e "automaticamente" pensar nas condições ambientais a que os dispositivos de armazenamento de *hardware* serão expostos, sendo que ao armazená-los corretamente pode-se aumentar a expectativa de vida da informação.

De acordo com Henriksen, et al. (2013), o meio ambiente para um armazenamento físico ideal deverá ter as seguintes características:

- Humidade relativa mantida entre 35% -40%.
- Temperatura mantida entre 15-21 ° C (dependendo do tipo *de hardware*).
- Monitorização da temperatura e da humidade relativa.
- Alarme de incêndio.
- Sistema de extinção de incêndio sem recurso a água.
- Acesso restrito à área de armazenamento.
- Existência de filtros de ar.
- Blindagem magnética (especialmente para fitas magnéticas).
- Ter instaladas câmaras de vigilância.
- Possuir fonte energia para *backup* em caso de desastre.
- Na iluminação prever proteção de raios ultravioleta assim como em todas as janelas.

- Excluir condutas de água perto, ou por cima, da área de armazenamento.
- A área de armazenamento não deve ser construída em cimento (aumenta a humidade para quase 100% em casos de incêndio).

Assumindo a Preservação como variável da Gestão da Informação foi referido que aquela ocorre desde que se está a preparar a especificação da plataforma tecnológica que suportará a produção informacional.

A informação produzida em meio digital deverá ser mantida e preservada nesse meio. No entanto, não se pode esquecer que as suas morfologias podem ser várias: textos, bases de dados, imagens (fixas ou em movimento), gravações sonoras, material gráfico, programas informáticos e, entre outros, as mensagens de *email*. Os anexos dos *emails* não têm apenas um tipo de conteúdo, comportando texto, imagens, vídeos, animações. Daí que a grande diversidade de formatos não permita uma solução única de preservação, tornando-se necessária uma estratégia mais ampla para atender, pelo menos, aos tipos de formatos mais utilizados.

A informação em meio digital possui características específicas. Não se tem a perceção direta da informação existente e onde está armazenada. A sua estrutura e conteúdo configuram-se no momento da visualização, é uma estrutura lógica e não física. Há, por isso, uma grande dificuldade em localizar os documentos em meio digital e identificar os procedimentos que lhe estão na origem.

No caso da informação de um *email*, esta tem um armazenamento distribuído, está armazenada em diferentes servidores, possivelmente em diferentes partes do mundo, e pode ser acedida de diversos pontos físicos. Para a sua gestão é necessária a existência de metainformação, que integra a dimensão essencial construída ao longo de todas as outras, possibilitando uma identificação completa e inequívoca, de modo a garantir segurança em todo o seu ciclo de vida (Delgado e Barbosa, 2009).

No que respeita ao enquadramento legal, o *email* é afetado por uma série de legislação que carece de definição (direitos de autor, privacidade, marcas registadas, segredos comerciais, questões de importação/exportação, etc.). Essa legislação tem de ser tida em conta aquando da sua preservação. A par das mudanças tecnológicas, há também constantes mudanças no campo dos regulamentos e legislação, o que pode requerer mudanças no sistema de gestão da preservação definido.

Temos, ainda, que estar conscientes de que, apesar de poderem ser usados como prova de transações ou comunicações, é possível criar *emails* fraudulentos e depois apresentá-los

como algo verídico. Ao arquivar tem que ser garantida a integridade e a autenticidade dos emails que vão ser preservados.

Desta forma e segundo Prom (2011) supondo que o *email* pode ser capturado e guardado, há de facto uma área legal adicional que precisa de atenção aquando do desenvolvimento de um programa de preservação de email – nomeadamente leis de direito de autor e de propriedade intelectual. O direito de autor inerente a qualquer dos componentes de uma mensagem de *email* irá afetar o que pode ser feito com a mesma no longo prazo.

4.4.7.2. Estratégias para a preservação de emails

São várias as estratégias de preservação a desenvolver em meio digital, não passando as opções pela adoção de uma única. Para a preservação de *email* Houston (2008) apresenta três soluções a longo prazo:

- **Imprimir os *emails:***
  - Vantagem: evita os problemas de obsolescência
  - Desvantagem: não é pesquisável nem reutilizável em meio digital, constituindo uma reprodução incompleta do mesmo;
- **Retenção dos *emails* no cliente:**
  - Vantagem: armazena documentos criados por aplicativos; uma opção mais fácil para a maioria dos utilizadores, quando bem organizados.
  - Desvantagem: afeta o desempenho do sistema; problemas ao nível de *backup*;
- **Armazenar os *emails* num formato neutro:**
  - Vantagem: arquivos convertidos para um formato *open source* (TIFF, XML, PDF/A) e armazenados remotamente; reduz / elimina a necessidade de migração ou emulação; oferece opções de *backup*;
  - Desvantagem: a conversão para estes formatos pode envolver um trabalho intensivo.

Nos Estados Unidos, e face aos problemas existentes, os estados do Kentucky e da Carolina do Norte (Arquivos da Carolina do Norte, Kentucky e Pensilvânia) desenvolveram em parceria um projeto de *gestão e preservação de emails*.

Este projeto caracteriza-se por utilizar servidores *email open source*, ter a possibilidade de criar pastas no *Servidor de Arquivo* (SA), sendo que as mensagens que forem assinaladas

como tendo “valor arquivístico” podem facilmente ser copiadas e arquivadas no SA, usando um posto cliente, caracterizando-se, ainda, por ser capaz de copiar a estrutura completa entre uma pasta comum e uma pasta do SA.

Dele resultou uma ferramenta de gestão e preservação de *emails* (EMCAP) usada para converter email no seu formato nativo para o formato XML por forma a permitir que os utilizadores "arquivem" os seus emails numa base sistemática, isto é, de acordo com um plano de classificação, e que fosse capaz de suportar vários tipos de ficheiros, minimizando o suporte das TI.

Assim nasce a ferramenta EMCAP, uma ferramenta *open source*, que permite que o cliente tenha uma estrutura de ficheiros mapeada num servidor e reúne os seus emails numa mesma “coleção” (classe ou subclasse numa estrutura). Depois de os dados serem sincronizados, são gerados ficheiros XML das mensagens, que em conjunto com a versão original da mensagem são armazenadas num repositório.

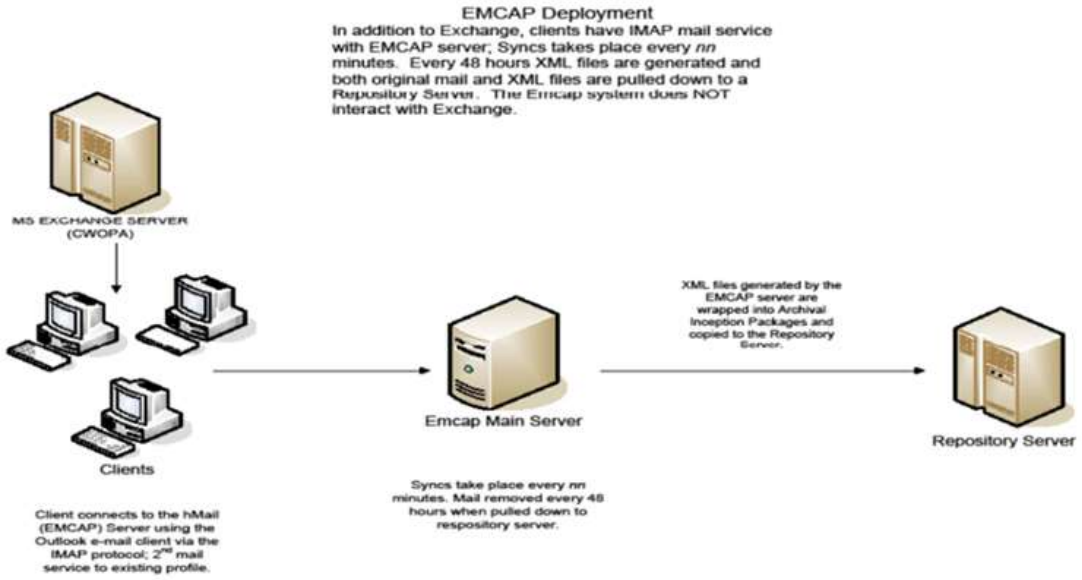


Ilustração 24 - Arquitetura da ferramenta EMCAP (Mcaninch e Eubank, 2008)

A ferramenta que gera o XML das mensagens contém as seguintes funcionalidades:

- Esquema XML que descreve todos os *emails* numa conta;
- Desenvolvimento de um "esquema comum", com concessão CERP (*Collaborative Electronic Records Project*);
- Análise das informações de cabeçalho no *email;*
- Armazenamento de todos os fluxos de *bits* originais no formato nativo;
- Caso o ficheiro seja externo grava uma síntese da mensagem que é criada com um

identificador único;

- Os testes preliminares mostram conversão com 95% de eficácia.

Quanto à *gestão dos anexos* enviados nas mensagens de correio eletrónico, esta ferramenta permite que:

- Os *links* para anexos sejam mantidos em formato nativo e convertidos para Unicode;
- A migração ou conversão podem ser necessárias no futuro para arquivos binários (.pdf .doc, etc.);
- O sistema deixa marca no código XML para facilmente se identificar o anexo.

O desenvolvimento de um Esquema XML para Conta de *Email* (*E-Mail Account XML schema*) é uma outra possibilidade e viabilizou a preservação de numerosos *emails* relacionados (todo o conteúdo da conta de *email*) num único ficheiro XML.

Procurando reter a metainformação inerente a uma conta de *email* e na apresentação das mensagens de *email*, o CERP (*Collaborative Electronic Records Project*) e o EMCAP trabalharam em conjunto para definir um esquema XML que efetivamente capture e preserve as mensagens de *email* de uma forma que estas retenham de forma completa a sua autenticidade e integridade, permitindo aos investigadores, usar uma pesquisa robusta e estratégias de pesquisa de dados para identificar conteúdo valioso em mensagens individuais, dentro de pastas ou contas (Ferrante e Fuhrig, 2009).

O esquema utiliza uma estrutura de marcação XML, para incorporar a organização e a estrutura inerente a uma conta de *email*. Além da estrutura organizacional mais básica de uma conta de *email* com uma pasta que contém pelo menos uma mensagem, o esquema precisava de ser robusto o suficiente para lidar com mensagens multiformato, mensagens com anexos e mensagens com mensagens anexadas, e, ao mesmo tempo, capturar a estrutura em múltiplas camadas inerente à organização atribuída pelo proprietário da conta ao *email* nela contido.

De acordo com Ferrante e Fuhrig (2009) a estrutura do esquema da conta de *email* apresenta as mensagens de correio eletrónico nas pastas que os contêm, como é parcialmente ilustrado na seguinte ilustração:

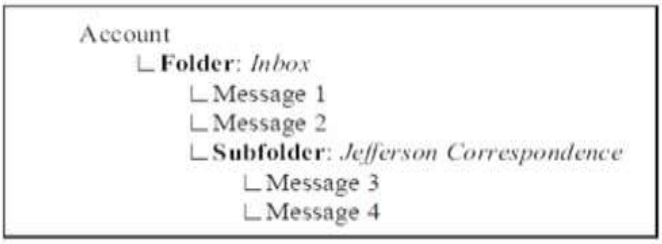


Ilustração 25 - Estrutura parcial de uma conta de email preservada (Ferrante e Fuhrig, 2009)

Este esquema suporta os elementos definidos na RFC 2822 (*Internet Message Format* - norma da Internet para mensagens) para mensagens em conta de email. Assim, os componentes preservados de uma mensagem de *email* prolongam-se para além do conjunto limitado de elementos visíveis por um utilizador típico.

O esquema suporta a incorporação de anexos de mensagens de *email* no ficheiro da conta preservada. Quando isso ocorre o anexo incorporado é mantido dentro da mensagem. Alternativamente, o esquema permite que um anexo de uma mensagem seja arquivado num ficheiro XML externo à conta de *email.*

O resultado final é a completa concretização da preservação de uma mensagem de *email* na sua totalidade - cabeçalho, mensagem e anexos -. Quer seja um *email* de texto simples, sem anexos, ou um email multicorpo com documentos, imagens, vídeos e outros *emails* anexados, este leque de possibilidades é considerada na definição do próprio esquema (Ferrante e Fuhrig, 2009).

Segundo estes autores, o esquema conta de *email* é distinto:

- No seu paradigma baseado na *conta;*
- Na granularidade dos dados capturados;
- No alinhamento com a norma para mensagens de *email* RFC 2822;
- Em ter um único ficheiro XML por conta;
- Na sua incorporação em duas aplicações (*software*) de preservação de email desenvolvidas separadamente.

O valor-chave desta abordagem é que as inter-relações das próprias mensagens de *email* são preservadas sem a necessidade de documentação adicional, como a informação já existente na conta.

O esquema em si serve como um meio de validar que uma migração de preservação foi concluída com êxito, quando as contas contêm dezenas de milhares de *emails*, torna-se essencial um meio eficiente de verificar a qualidade dos processos de preservação concluídos

(Ferrante e Fuhrig, 2009).

A adesão ao RFC 2822 fornece uma gama mais abrangente e completa de dados, organizados num formato baseado num padrão que o torna mais acessível. A granularidade da estrutura do esquema facilita a acessibilidade e compreensibilidade das contas de *email* preservadas e das suas mensagens, permitindo que estratégias de busca avançada sejam aplicadas a uma ou mais contas simultaneamente (Ferrante e Fuhrig, 2009).

Devido à estrutura do esquema, é possível pesquisar em toda a conta e recuperar apenas as mensagens que cumpram os critérios estabelecidos e disponibilizar para posterior visualização pelo utilizador.

No âmbito governamental é de salientar logo no início do séc. XXI um projeto do governo holandês especialmente direcionado para as bases de dados relacionais por estas serem amplamente utilizadas no suporte à atuação do governo holandês.

No âmbito deste projeto destaca-se o *Testbed XMaiL - Digital Preservation Testbed*, desenvolvido entre 2001-2003 e direcionado à investigação da preservação digital a longo prazo de diferentes tipos de documentos, nomeadamente: *emails*, documentos de texto, bases de dados, entre outros. Para o caso das mensagens de correio eletrónico, foi criado um protótipo de uma aplicação informática na qual é personalizado o *Microsoft Outlook* com vista a permitir a comunicação com um servidor central onde é recolhida a metainformação e, posteriormente, as mensagens e a metainformação são convertida e armazenadas em XML.

Mais recentemente, e não apenas centrado na busca de soluções tecnológicas, é de referir a iniciativa do Governo do Canadá, a par de outras que se vão multiplicando por todo o mundo. Esta iniciativa envolve a Biblioteca e Arquivos do Canadá destacando-se a publicação do *Guia* para a Gestão do *email* no governo do Canadá (LIBRARY AND ARCHIVES CANADA, 2006).

Este guia aborda questões pertinentes para a gestão do *email*[12], tais como o ciclo de vida dos *records*[13] (registos) de *email*, algumas definições importantes, os procedimentos e

[12] "**Electronic mail** (email) messages are communications, sent or received internally or externally on an electronic mail system, and include any attachments transmitted with the message as well as the associated transmission and receipt data".

[13] "***Record*** *includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine readable record, and any other documentary material, and any copy thereof. (National Archives of Canada Act, 1987, Access to Information Act R.S. 1985)*". Definem, também, os "**Transitory Records** are those records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record. Transitory records do not include records required by government institutions or Ministers to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of government. (Authority for the Destruction of Transitory Records, Library and Archives Canada 1990) www.collectionscanada.gc.ca/government/disposition/007007-1016-e.html.

papéis no que toca à gestão e proteção do *email*, bem como uma parte destinada para as questões mais frequentes que surgem. Nele é salientado que a quase totalidade dos *emails* produzidos, recebidos e acumulados pelo governo são "*records*", isto é, destinam-se à retenção no longo prazo:

> *"A record is under the control of a government institution when that institution is authorized to grant or deny access to the record, to govern its use and, subject to the approval of the Librarian and Archivist of Canada, to dispose of it. Regarding the question of physical possession, a record held by an institution, whether at headquarters, regional, satellite or other office, either within or outside Canada, is presumed to be under its control unless there is evidence to the contrary. A record held elsewhere on behalf of an institution is also under its control, for example at an employee's home or on business travel.*
>
> *Since most email messages are records, they must be managed in accordance with all applicable legislation and federal government policies such as the Access to Information and Privacy Acts, the Library and Archives of Canada Act, Treasury Boards Management of Government Information (MGI) Policy and the Government Security Policy" (LIBRARY AND ARCHIVES CANADA, 2006).*

O objetivo deste guia, é que o *email* seja visto como informação que tem de ser gerida e preservada. Ou seja, os *emails* que são criados, recolhidos, recebidos, transmitidos ou enviados no curso normal das atividades do governo, refletem as funções, as atividades e decisões, constituindo informação oficial do governo. Desta forma, devem ser geridos ao longo do seu ciclo de vida, sendo que para isso terão de existir iniciativas das instituições governamentais para que se estabeleçam serviços, programas, sistemas de gestão e ações de divulgação de informação de forma sustentável e coerente para ir ao encontro das necessidades dos utilizadores. A *gestão do email* deverá constituir parte integrante das políticas, orientações e processos organizacionais.

No âmbito da indústria de *hardware* e *software* esta é uma área para a oferta de novos produtos, sendo a HP, um exemplo entre outros, quando lança um *software* de arquivo de *email* para o *software Microsoft Exchange*. O objetivo deste é fornecer a possibilidade de retenção a longo prazo, a pesquisa de alta velocidade e a recuperação de mensagens e anexos para, assim, reduzir o impacto dos custos na organização.

Constata-se, assim, a lenta mas progressiva consciencialização que vem ocorrendo nos últimos anos, ao nível institucional e organizacional, da importância do *email* como uma via privilegiada para a comunicação interpessoal e interorganizacional / institucional envolvendo

informação que constitui evidência e suporte para as respetivas atividades, emergindo a necessidade de atribuir ao "email"/mensagem recebida por via digital a devida representatividade aos diferentes níveis da gestão assegurando-lhe a manutenção continuada da relevância informacional como informação que integra o sistema de informação da pessoa, instituição ou organização, assumida como recurso de gestão e memória de indivíduos, instituições e organizações.

4.5. O caso da adoção do formato PDF na CMP

A adoção do formato PDF vem-se impondo ao longo dos últimos anos tendo-se apresentado para a CMP como uma clara opção, no que respeita à adoção da *estratégia de normalização de formatos* que permite que hoje estejam já assegurados os requisitos para a preservação e acesso a longo prazo de grande parte da produção atual da CMP, bem como da digitalização retroativa realizada desde o início da entrada em funcionamento da UCD, o que não obsta a que se faça uma breve revisão da literatura e se apontem novas perspetivas, face aos últimos desenvolvimentos neste domínio.

A informação é hoje crescentemente produzida em meio digital (nado-digital), e quando tal não se verifica procede-se à designada "desmaterialização" (entenda-se: substituição da tramitação física pela tramitação digital) promovendo a sua digitalização.

Desta forma, o sujeito humano deixa de poder aceder diretamente a informação, envolvendo, agora, novas formas de estruturação e codificação das representações mentais - ou mentefactos - e da sua fixação para utilização futura. (Pinto, 2013).

Podemos, assim, afirmar que a preservação da informação começa, desde logo, na conceção e implementação da plataforma tecnológica na qual será produzida, recebida, capturada, organizada, armazenada e difundida a informação, nomeadamente no *software* utilizado, nos formatos adotados, na recolha, na fase e momento próprio, da metainformação administrativa, técnica, estrutural, descritiva ou de preservação que permita a sua futura referenciação 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. Um papel que não poderá ser imputado a "informáticos", mas que convoca permanentemente parcerias entre o gestor da informação e os diferentes atores, informáticos incluídos (Pinto, 2014).

Atualmente, o desafio que se coloca é precisamente o da gestão da informação em meio digital (Pinto, 2007), onde a obsolescência tecnológica, visível a vários níveis (*hardware*,

software, suportes de armazenamento, formatos, etc.), é um entre vários fatores a considerar.

Assim, desenvolve-se um complexo processo integrado de gestão que convoca conhecimento teórico, instrumentos, ferramentas e técnicas de operacionalização que estarão presentes ao longo de todo o ciclo de vida e gestão da informação, abarcando momentos que, ainda hoje, são frequentemente assumidos de forma segmentada e sem articulação entre si e que deverão, com esta proposta, integrar o ***Serviço de Gestão da Preservação da Informação***, tendo como referência a estrutura de ***Serviços*** a desenvolver em torno da GI (ilustração 4).

A necessidade de preservar a informação a longo termo resulta da dificuldade de o ser humano deixar de poder aceder diretamente à informação, precisando sempre da mediação tecnológica, depois porque o objeto digital é dinâmico, de acesso/comunicação assíncrona e multidirecional, facilmente reutilizado/manipulado em grande escala, incentivando o alargamento da complexidade que a "multidimensionalidade" da informação digital provoca, convocando as seguintes dimensões:

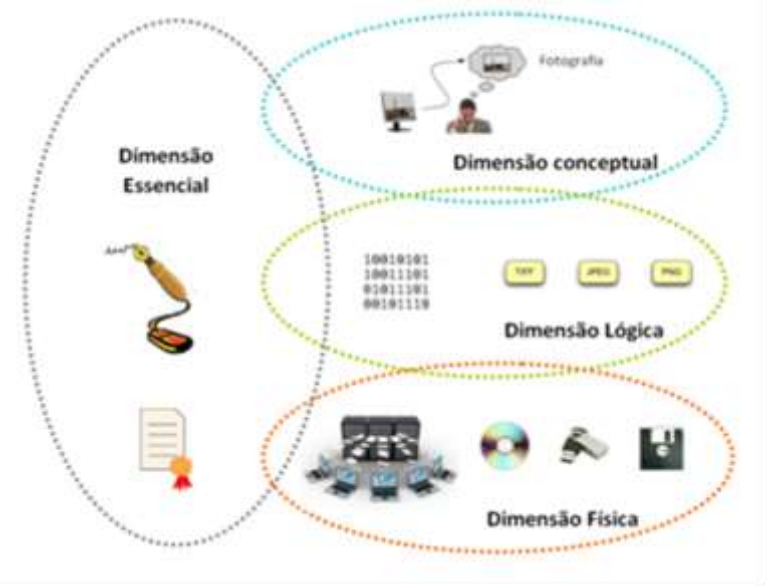


Ilustração 26 - Multidimensionalidade da Informação (Documento Interno CMP, 2012)

A problemática dos formatos situa-se, pois, ao nível da **preservação da dimensão lógica** obrigando a pensar a questão da obsolescência dos formatos, a necessidade de garantir a interoperabilidade, assim como o problema dos formatos proprietários, podendo aqui ser acionada a **estratégia de normalização de formatos**, indicando os mais adequados em função das necessidades e propriedades da informação em causa.

O ***Portable Document Format*** (PDF) cada vez mais utilizado é uma possibilidade,

no entanto exige que se atenda às diferentes especificidades para uma melhor eficiência e eficácia da sua utilização.

O PDF é um formato de ficheiro usado para apresentar os documentos de uma forma independente do *software* aplicativo, *hardware* e sistemas operativos.

Cada ficheiro PDF encapsula uma descrição completa de um documento plano de *layout* fixo, incluindo o texto, fontes, gráficos e outras informações necessárias para o exibir.

Este era um formato proprietário, controlado pela Adobe, até que foi lançado oficialmente como um padrão aberto em julho de 2008 e publicado *pela International Organization for Standardization* como ISO 32000-1:2008.

Os *National Archives and Records Administration* (NARA, US) definem *formato sustentável* como sendo "[...] a capacidade de aceder a um *record* eletrónico em todo o seu ciclo de vida, independentemente da tecnologia utilizada, quando foi originalmente criado" (Fanning, 2010a).

Como características de um formato sustentável apontam-se as seguintes:

- Documentação publicada e divulgação aberta;
- Adoção disseminada e o uso;
- Formatos de autodescrição;
- Dependência externa;
- Impacto de Patentes;
- Mecanismo de proteção técnica.

No que respeita ao PDF, entre as suas variantes encontra-se o **PDF/A** que se apresenta como:

- Um padrão de formato de ficheiro;
- É apenas um componente de uma estratégia de preservação abrangente (Fanning, 2010b).

O PDF/A visa responder a três questões principais:

- Definir um formato de ficheiro que preserva a aparência visual estática de documentos eletrónicos ao longo do tempo;
- Fornecer uma estrutura para a gravação de metainformação sobre os documentos eletrónicos;
- Fornecer uma estrutura para definir a estrutura lógica e propriedades semânticas dos documentos eletrónicos (Fanning, 2010a).

A implementação bem-sucedida do PDF/A não depende apenas da utilização do formato mas de uma atuação integrada que envolve:

- Políticas e procedimentos de gestão de registos;

- Requisitos e condições adicionais;
- Processos de garantia de qualidade.

O PDF/A é diferente de um PDF pela omissão de características inadequadas para o armazenamento de longo prazo, como fontes de ligação (em oposição à incorporação de fontes).

Da mesma forma, o formato de ficheiro **PDF/X** é especialmente adaptado para a impressão digital e artes gráficas.

Para existir uma boa apresentação/*renderização*, um documento PDF/A deve ter:

- Fontes e imagens incorporados;
- Elementos gráficos incorporados;
- Sem áudio ou vídeo;
- Não possuir referências diretas ou indiretas a recursos externos;
- Metainformação;
- Ausência de elementos de segurança ou criptografia;
- Ausência de ficheiros incorporados (Fanning, 2010c).

Os níveis de conformidade e versões envolvem, entre outros, o PDF/A1, o PDF/A2, PDF/A3, o PDF/X, o PDF/E:

No que respeita **PDF/A-1** a norma especifica dois níveis de conformidade para os arquivos PDF:

- **PDF/A-1a -** Nível A conformidade na parte 1
- **PDF/A-1b** - Nível B conformidade na parte 1

O PDF/A-1b tem o objetivo de garantir a reprodução fiável da aparência visual do documento, enquanto o PDF/A-1a inclui todos os requisitos da PDF/A-1b e o seu objetivo é garantir que o conteúdo do documento pode ser pesquisado e reaproveitado.

A parte da norma que diz respeito ao **PDF/A-2**, aborda alguns dos novos recursos adicionados com as versões 1.5, 1.6 e 1.7 da referência PDF.

O PDF/A-2 deve ser compatível, ou seja, todos os documentos PDF/A-1 válidos também devem ser compatíveis com PDF/A-2. No entanto, ficheiros compatíveis com PDF/A-2 podem não ser necessariamente compatíveis com PDF/A-1.

Esta parte 2, define três níveis de conformidade: PDF/A-2a, PDF/A-2b e um novo nível de conformidade, o PDF/A-2u. PDF/A-2u representa o nível B de conformidade (PDF/A-2b) com a exigência adicional de que todo o texto no documento tem mapeamento Unicode.

O **PDF/A-3** permite a incorporação de formatos de ficheiros (tais como XML, CSV, CAD, documentos de processamento de texto, folhas de cálculo e outros) em PDF/A como objetos arquivados completos.

Para Levenson (2008), o porquê de se escolher o formato PDF/A deve-se ao facto de:

- A necessidade do negócio e o mercado consumidor estarem muitas vezes dessincronizados;
- Modelo de aplicação de estação de trabalho atual em ciclos de três anos;
- Emulação de papel eletrónico;
- Migração mínima;
- Renderização precisa, consistente e previsível;
- Sem uma solução única para todos os problemas;
- Leitor livre, multiplataforma e formação mínima.

O **PDF/X** não constitui uma alternativa ao PDF, é um subconjunto focalizado de PDF especificamente concebido para o intercâmbio de dados de pré-impressão confiável. É uma norma de aplicação, bem como uma norma de formato de ficheiros. Ou seja, esta define como as aplicações que criam e leem ficheiros PDF/X se devem comportar.

Os objetivos imediatamente mensuráveis do PDF/ X são:

- Para melhorar a cor e a correspondências de conteúdo de prova para prova, prova para a impressão, e impressão para impressão;
- Para reduzir os erros de processamento em prova e pré-impressão;
- Para permitir a rápida, eficaz e automatizável pré-visualização de ficheiros no momento da receção do cliente;
- Para reduzir a complexidade e o custo da educação do cliente (Bailey, 2005).

Os padrões PDF/X são projetados para serem amplamente aplicáveis em muitos setores e áreas geográficas da indústria de impressão. Assim, constituem uma base muito forte para o desenvolvimento de especificações personalizadas, mais concretamente para um sector específico.

A combinação de duas divisões conduziu à criação de vários padrões PDF/X:

- PDF/X-1a. O padrão PDF/X-1a aborda os intercâmbios cegos onde todos os ficheiros devem ser entregues em CMYK, sem RGB ou dispositivo de dados (com gestão de cores) independentes. Esta é uma exigência comum em muitas áreas e setores de impressão.
- PDF/X-3. O padrão PDF/X-3 é um superconjunto do PDF/X-1a; um ficheiro PDF/X-1a atende a todos os requisitos técnicos de um PDF/X-3. Ambos os padrões PDF/X-3 e PDF/X-2 são claros sobre a forma como uma prova ou um dispositivo

placa-setter deve agir sobre as cores num ficheiro. Todas as ferramentas concebidas para ler PDF/X-3 também devem ser capazes de ler ficheiros PDF/X-1a.

- PDF/X-2. Tanto o PDF/X-1ª como o PDF/X-3 definem formatos de ficheiro para intercâmbios cegos. Em alguns fluxos de trabalho que não é exigido, ou um único arquivo por trabalho não é adequado, mas algumas restrições adicionais sobre a formatação do arquivo, em vez de apenas dizer "PDF" seriam desejáveis para aumentar a fiabilidade. O PDF/X-2 foi concebido para abordar os intercâmbios, onde há mais discussão entre o fornecedor e o recetor do ficheiro. (Bailey, 2005).

Por sua vez, o **PDF/E** é um subconjunto do PDF, projetado para ser um formato de troca aberta e neutra para documentação técnica e de engenharia para a criação de documentos utilizados na construção de *workflows* (Bailey, 2005).

Esta norma especifica como o *Portable Document Format* (PDF) deve ser utilizado para a criação de documentos em ***workflows* de engenharia**.

Os principais benefícios da norma PDF/E incluem:

- Reduzir os requisitos de *software* caro e proprietário;
- Menores custos de armazenamento e taxas (vs. papel);
- Troca confiável em vários aplicativos e plataformas;
- Independente.

A Norma não define um método para a criação ou conversão de papel ou documentos eletrónicos para o formato PDF/E. Esta foi criada para atender às necessidades das organizações que precisam de forma confiável criar, trocar e rever documentação de engenharia, no entanto, a primeira parte da norma não trata de 3D, vídeo ou outro conteúdo dinâmico, nem trata dados de origem integrados.

No caso em concreto da CMP, no que diz respeito à definição das classes dos objetos digitais que entram e são produzidos na organização, estes podem ser:

- Imagens;
- Documentos nado-digitais (estruturados, semiestruturados e não estruturados em vários formatos);
- Outra informação nado-digital, como bases de dados, entre outra.

A preservação da dimensão lógica não pode desta forma ser descuidada, revelando-se neste ponto a questão da obsolescência dos formatos, a interoperabilidade, assim como o problema dos formatos proprietários.

Para garantir a sua preservação a longo prazo é importante **definir os formatos**

normalizados, Tabela 3.

Porém, nem sempre o formato de preservação é o mais indicado para a fase em que o documento ainda está em tramitação.

Tabela 3 - Taxonomia de Propriedades Significativas (Documento Interno CMP, 2012)

Classes	**Formato transacional**	**Formato definitivo** (preferencial)
Texto estruturado	Word, Excel, OpenOffice, etc.	**PDF A**
Imagens	Png, Gif, Jpeg, vectorial (dwf), etc.	**TIFF, JPEG 100% e DWF X**
Base de dados relacionais	Access, Oracle, SQL Server	**DBML**

Ter-se-á, ainda que pensar necessariamente a captura e manutenção da metainformação que documente e assegure a recuperação dos objetos digitais, no tempo.

Resumindo, e seguindo o modelo OAIS, trata-se de criar para cada objeto o seu respetivo *Pacote de Informação de Submissão* (PIS).

Existem diferentes tipos de metainformação, Tabela 4, cuja captura e manutenção deve seguir normas internacionais. A seleção das normas a usar teve por base o reconhecimento internacional, dimensão e relevância dos organismos que neste domínio as têm aplicado.

Tabela 4 - Matriz de Tipos de Metainformação por Função e Normas (Documento Interno CMP, 2012)

Tipo de Metainformação	**Função**	**Normas**
Técnica	Preservação; pesquisa	NISO Z39.87
Estrutural	Apresentação, reconstituição do objeto	METS, Dublin Core
Descritiva	Acesso	EAD; ISAD(G); ISAAR(CPF)
Preservação	Autenticidade	PREMIS

Neste âmbito destaque-se a norma **NISO Z39.87** (*Techical Matadata for Digital Still Images*), ou a sua versão MIX (em XML) que é um esquema que define um conjunto normalizado de elementos de metainformação para imagens digitais, cuja organização é compatível com o PREMIS.

Na CMP todo o projeto relativo à estruturação da UCD teve em consideração estes problemas e possíveis soluções, passando quer pela adoção do PDF/A, quer pela captura/produção e registo de metainformação e implementação da construção dos pacotes previstos no modelo conceptual OAIS.

Assim, os campos de metainformação recolhidos pelas máquinas digitalizadoras incluem:

- Comprimento de imagem;
- Configurações de digitalização;
- Data de produção;
- Dimensão;
- Dispositivo de captura;
- Esquema de cor;
- Formato;
- Identificador;
- Indivíduo produtor;
- Largura de imagem;
- Modelo de dispositivo de captura;
- Nº de pixéis;
- Nome de fabricante;
- Nome do *Software*;
- Número de componentes digitais;
- Plataforma tecnológica;
- Profundidade de bits;
- Resolução espacial;
- Sistema Operativo;
- *Software* de captura;
- Versão de *Software* de captura;
- Versão do *Software*.

Quanto às características da digitalização ao nível da UCD (Unidade Central de Digitalização) foram especificadas as seguintes:

- JPEG a 100% (sem compressão);
- 24bits de profundidade;
- 200 Dpi's de resolução;
- a cores;
- Captura automática de metainformação técnica para um ficheiro XML, sendo que os campos registados estão de acordo com a norma NISO Z39.87.

Em anexo é apresentado um exemplo destes campos de metainformação devidamente preenchidos, onde é possível verificar o que é capturado pelo *software* utilizado aquando da efetiva digitalização.

Foi igualmente adotado o formato PDF/A para todos os documentos digitalizados pela UCD pois este é um formato não proprietário sendo também internacionalmente aceite, na

perspetiva da preservação e acesso continuado no longo termo. Estes objetos digitais são inicialmente ficheiros com o formato **JPEG 100%,** pois são mantidas as características fundamentais para uma imagem de boa qualidade, sendo a partir deste **formato matriz** que é criado/gerado o **formato PDF/A**, mais concretamente com o nível de **conformidade 1-b**.

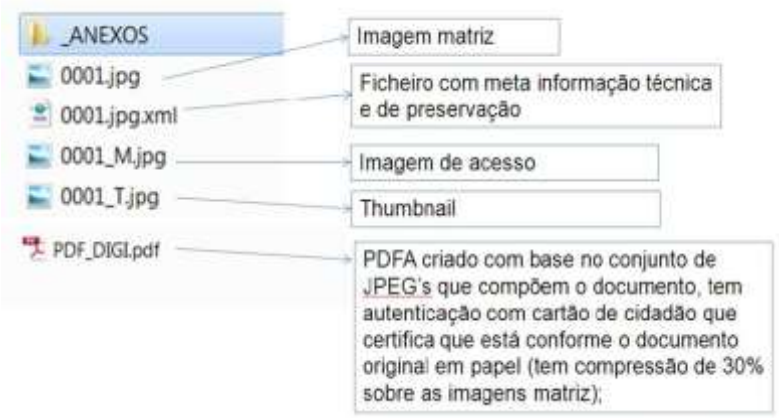


Ilustração 27 - Formatos de ficheiros armazenados no repositório digital da CMP

Como está representado na ilustração acima, são guardados vários formatos do mesmo ficheiro cada um com características e funções diferentes, seja em termos de preservação como para os casos de visualização.

Assim, é normal estabelecer para o mesmo documento um **formato transacional** e depois, quando este é arquivado, é transformado no **formato previsto para a preservação da informação a longo termo.**

Desta forma, e de acordo com o documento publicado pela *Library of Congress*, *Recommended Format Specifications* para que exista uma boa preservação dos ficheiros digitais existem várias características preferenciais que devem ser tidas em conta como boas práticas:

A. Características técnicas

1. Maior resolução disponível, não redimensionada ou interpolados
2. Maior profundidade de bits disponível, 16 bits por canal, se disponível
3. Especificado espaço de cor usado na versão publicada
4. Não-comprimidas
5. Não estratificadas
6. Melhor versão disponível, clareza total (por exemplo, maior resolução, maior a profundidade de bits, sem compressão)

B. Formatos, em ordem de preferência

1. TIFF (não comprimido)

2. JPEG2000 (sem perdas)
3. PNG
4. JPEG / JFIF
5. DNG (Negativo Digital)
6. JPEG2000 (com perdas)
7. TIFF (comprimido)
8. BMP
9. GIF

C. Metainformação

1. Se for suportado pelo formato, incluir a seguinte metainformação: título, autor, data de criação, local de publicação, editor / produtor / distribuidor, informações de contato. Incluir se disponível: língua de trabalho, outros identificadores relevantes (por exemplo, DOI, LCCN, etc), descrição de assunto, resumos, informações de produção chave ou referência a cada campo de dados e técnico.

D. Medidas de caráter tecnológico

1. Os ficheiros não devem conter nenhuma medida que controle o acesso ou uso do trabalho digital (tais como gestão de direitos digitais ou criptografia).

Este documento menciona, ainda, que apesar das descrições acima serem as ações preferenciais para a preservação de ficheiros digitais, existem também algumas medidas que são práticas igualmente aceitáveis no tratamento destes ficheiros:

A. Formatos

1. TIFF (em formato Planar)
2. PhotoShop
3. Camera RAW
4. JPEG 2000 Parte 2
5. FlashPix
6. Computação Gráfica Metafile (CGM, WebCGM)
7. PostScript encapsulado (EPS)

B. Compressão

1. Taxas de compressão mais baixas preferenciais
2. Discrete Wavelet Transform (**DWT**) preferido a Discrete Cosine Transform (**DCT**)

C. Medidas de caracter tecnológico

1. Os ficheiros não devem conter nenhuma medida que controle o acesso ou utilização da obra digital (como gestão de direitos digitais ou criptografia)

Desta forma e apesar de todos os esforços realizados pelas organizações, no qual se enquadra a CMP, no sentido de se estabelecerem as melhores práticas no que diz respeito à preservação da informação em meio digital ainda existem algumas barreiras a serem ultrapassadas, sobretudo, com a necessidade de *salvaguardar a informação com todos os seus atributos*, dado que, em comparação com a informação em suportes tradicionais/analógicos, esta tarefa revela-se bem mais complexa. Tal como refere Pinto (2009), este processo revela-se de um caráter de urgência, porque se com o analógico "amanhã é tarde demais", com o digital "hoje já pode ser tarde demais".

Conclusões e perspetivas de desenvolvimento

Num mundo cada vez mais digital, impõe-se uma reflexão sobre a forma de perspetivar, conceber e agir no âmbito da preservação e também da segurança da informação, para que possamos assegurar não só direitos e "ativos", mas também o acesso continuado à informação em meio digital no longo prazo.

Tal como refere Pinto (2004), "depois do "salto tecnológico" impunha-se a mudança fundamental que consistia na "mudança da estrutura organizacional da Administração Pública" e correspondente "mudança da cultura organizacional", no âmbito de uma sociedade caracterizada pela capacidade dos seus membros (Cidadãos, Empresas e Estado) obterem e partilharem qualquer tipo de informação e conhecimento instantaneamente, a partir de qualquer lugar e na forma mais conveniente".

Podemos afirmar que para a criação de um Repositório Digital Confiável, que garanta os atributos de autenticidade, integridade, inteligibilidade e de preservação da informação no longo prazo é exigida a definição e implementação de adequadas *Políticas, Estratégias e Planos de Preservação* que englobem todo o ciclo de vida da informação (conceção da plataforma tecnológica, produção/captura, fluxo, organização, representação e descrição, armazenamento, avaliação/seleção, preservação, acesso e uso) no quadro da Gestão não só do SI mas também dos STI no todo organizacional.

Neste sentido constata-se a importância e a inter-relação entre as *Políticas de Segurança de Informação* e as *Políticas de Preservação de Informação*. Estas devem então ser alicerçadas por uma Política de âmbito mais geral como a de *GI e TI*, e o respetivo *Plano de GI e TI*. As *Políticas de Segurança e Preservação da Informação* dão por sua vez origem a um conjunto de políticas comuns a ambas as áreas, entre as quais, *Política de Classificação da Informação; Política de Gestão de Acessos; Política de Acesso à Internet; Política de Utilização do Correio Eletrónico*.

Quanto às Políticas de Preservação da Informação, esta dá origem a elementos base como: *Sistema de Gestão de Preservação da Informação; Política de Preservação Física; Política de Preservação Digital; Política de Armazenamento (Archival Storage); Política de Gestão de Operações e Serviços de Preservação*.

Desta forma, consideramos a preservação da informação em meio digital como uma função que não pode ser evitada, devendo ser considerada como um conjunto de ações orientadas e regulamentadas sob a designação de ***Serviço de Gestão da Preservação***, a

desenvolver no âmbito da GI, integrando uma estrutura de Serviços GI que constituirá um futuro **Sistema de Gestão de Informação**.

Cada vez mais as organizações dependem, a médio e longo prazo, de informação produzida e mantida digitalmente. Esta dependência deve-se a motivos que se prendem com o modo de como operam as organizações, salvaguardam os seus interesses, incrementam a transparência administrativa e a credibilidade relativamente aos seus *stakeholders*, entre os quais se contam o Governo e o cidadão.

As pessoas revelam-se como os pilares centrais, na medida em que tem de existir um compromisso e envolvimento de todos, partindo da Gestão de Topo, para que estas Políticas e Estratégias de Preservação possam de facto funcionar e tornarem-se úteis para a organização, nomeadamente permitir a prestação de melhores e céleres serviços aos munícipes. Por esta razão, o projeto do Arquivo Digital Confiável envolve várias Unidades Orgânicas da CMP que, em conjunto, dão o seu contributo através do conhecimento que obtêm dos seus processos *core* e que naturalmente se irão traduzir numa mais-valia para o sucesso da implementação deste Arquivo Digital, que irá beneficiar toda a estrutura orgânica da organização, considerando o ciclo de vida da informação.

Como perspetiva de trabalho futuro, verifica-se a importância de, ao nível da chamada Gestão Documental, ser assumida a necessidade de evoluir de uma abordagem ao nível de uma *Gestão de Documentos,* corporizada no *software* DocInPorto, para um MSR (*Management System for Records,*- ISO 30300 e ISO 30301), isto é, para a implementação de um *Sistema de Gestão de Informação Ativa e Permanente*, que contemple todo o ciclo de vida da informação, a pluridimensionalidade e a interoperabilidade, direcionado à gestão de informação de qualidade e que envolve a definição nomeadamente da Política de Gestão de Informação que orientará o **Sistema de Gestão da Informação**.

Ainda como futuras perspetivas, encontra-se o desenvolvimento do Anexo relativo à *Segurança e Gestão de Riscos* (Série ISO 27000 *Information Security Management Systems* (ISMS) e ISO 31000:2009 - *Risk management : Principles and guidelines*), a agregar à especificação do *Plano de Segurança da Informação* e ao programa de auditorias internas e externas da organização.

Compreende-se, assim, que, face às questões que precisavam ser ponderadas e trabalhadas para a efetiva criação de um *Arquivo Digital* e respetiva transformação num *Repositório Digital Confiável/Repositório de Preservação*, este é um processo complexo que envolve diversas áreas e vários componentes, pois para além dos requisitos de preservação e gestão da informação, encontra-se uma base tecnológica que se requer robusta, obedecendo

aos critérios de segurança e respetiva integração de sistemas e aplicações existentes, se tenha com a presente dissertação procurado, apenas, contribuir para o objetivo organizacional de certificação do *Repositório Digital Confiável da CMP*, objetivo que consideramos cumprido e que desejamos vá ao encontro dos interesses da entidade que acolheu este projeto.

Referências bibliográficas

Abreu, A. (2009). Preservação de bases de dados, da web e do email: Problemas, projetos, estratégias. Trabalho para a unidade curricular: Preservação e Conservação. Licenciatura em Ciência da Informação: Faculdade de Letras da Universidade do Porto.

Araújo, C. A. (2009). Correntes teóricas da ciência da informação. *Ci. Inf.*, vol. 38, nº 3, (pp.192-204). ISSN: 0100-1965.

ARCHIVES NEW ZEALAND; NATIONAL LIBRARY OF NEW ZEALAND (2011). Digital Preservation Strategy. Consultado em Janeiro 4, 2014, em http://archives.govt.nz/sites/default/files/Digital_Preservation_Strategy.pdf

Bailey, M. (2005). PDF/X Frequently Asked Questions. Global Graphics Software Limited. Consultado em Abril 2, 2014, em http://pt.slideshare.net/GlobalGraphics/pdfx-frequently-asked-questions

Balcky, L. F. (2011). *O Arquivo na Era Digital*. Dissertação de mestrado, Universidade Nova de Lisboa, Lisboa, Portugal. Consultado em Novembro 28, 2013, em http://run.unl.pt/bitstream/10362/7275/1/O%20Arquivo%20na%20Era%20Digital.pdf

Barbedo, F. (2005). Arquivos digitais: da origem à maturidade. *Cadernos BAD 2005*, vol. 2, (pp. 6-18). ISSN: 0007-9421.

Barbedo, F., Corujo, L., Sant'ana, M. (2010). Recomendações para a produção de planos de preservação digital. Lisboa: DGARQ. Consultado em Outubro 30, 2013, em http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf

Barnes, N. (2011). Going Global with RIM Standards and Best Practices. ARMA International. Consultado em Novembro 28, 2013, em http://content.arma.org/IMM/Libraries/May_-_June_2011_PDFs/IMM_0511_going_global_with_rim_standards_best_practices.sflb.ashx

Beagrie, N., Semple, N., Williams, P., Wright, R. (2008). Digital Preservation Policies Study: Part 1: Final Report October 2008. Charles Beagrie Limited. Consultado em Novembro 11, 2013, em http://www.jisc.ac.uk/media/documents/programmes/preservation/jiscpolicy_p1finalreport.pdf>

Becker, C.; Rauber, A. (2011). Four cases, three solutions: Preservation plans for images. Vienna University of Technology, Austria. Consultado em Dezembro 11, 2013, em http://www.ifs.tuwien.ac.at/~becker/pubs/becker-four2011.pdf

Becker, C., et al. (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans. *International Journal on Digital Libraries,* vol. 10, nº 4, (pp. 133-157). Consultado em Fevereiro 12, 2014, em http://www.ifs.tuwien.ac.at/~becker/pubs/becker-ijdl2009.pdf

Bearman, D. (2007). Systemic solutions for preservation. *Preserving the digital heritage: principles and policies*. Ed. Yola de Lusenet, Vincent Wintermans. Hague: Netherlands National Commission for UNESCO, European Commission on Preservation and Access. (pp. 26-44). ISBN 978-90-6984-523-4. Consultado em Novembro 12, 2013, em http://www.knaw.nl/ecpa/publ/pdf/6190.pdf

Beynon-Davies, P. (2002). Information Systems: An Introduction to Informatics in Organisations. Basingstoke: Palgrave. ISBN: 978-0-333-96390-6.

Brandão, M. (2010). *Arquitectura de Sistemas de Informação alinhada com a política de gestão de informação das unidades orgânicas na Câmara Municipal do Porto*. Tese de mestrado integrado, Universidade do Porto, Faculdade de Engenharia, Porto, Portugal.

Candy, J., Karwal, V. How E-mail Works?. PCTE. Consultado em Janeiro 30, 2014, em http://www.slideshare.net/adkpcte/how-email-works

Celorrio, F. (2010). El correo electrónio como documento de archivo.

Choo, C. W. (2003). Gestão de informação para a organização inteligente: a arte de explorar o meio ambiente. *Das Bibliotecas & Informação*. Lisboa: Editorial Caminho, S.A.. ISBN: 972-21-1506-5.

CITY OF VANCOUVER (2013). City of Vancouver: Digital Strategy. Consultado em Dezembro 2, 2013, em http://vancouver.ca/files/cov/City_of_Vancouver_Digital_Strategy.pdf

Coutinho, C. (2007). O que é a Investigação-acção?. Consultado em Novembro 14, 2013 em http://claracoutinho.wikispaces.com/O+que+%C3%A9+a+Investiga%C3%A7%C3%A3o-ac%C3%A7%C3%A3o%3F

Coutinho, C. (2008). Investigação-Ação: metodologia preferencial nas práticas educativas. O que é a Investigação-Ação. Consultado em Dezembro 6, 2013, em http://faadsaze.com.sapo.pt/5_o_que%20_e_ia.htm

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

Fanning, B. (2010a). Demystifying PDFs. Consultado em Abril 4, 2014, em

http://pt.slideshare.net/bfanning/demystifying-pd-fs

Fanning, B. (2010b). What is PDF/A. Consultado em Março 29, 2014, em http://pt.slideshare.net/bfanning/what-is-pdfa

Fanning, B. (2010c). PDF/Archive: Preserving Electronic Assets. PRIA – Washington, DC. Consultado em Março 25, 2014, em http://pt.slideshare.net/bfanning/pdfarchive-preserving-electronic-assets

Fanning, B. (2010d). PDF/Archive: Preserving Electronic Documents. Consultado em Abril 5, 2014, em http://pt.slideshare.net/bfanning/pdfarchive-preserving-electronic-documents

Fernandes, D., Brandão, M., Costa, M. (2010). Desmaterializar para potenciar a informação em rede: o caso da UCD da CMP. *Políticas de Informação na Sociedade em Rede*, *Guimarães, 7, 8 e 9 abril, 2010: atas*. Lisboa: BAD. Consultado em Dezembro 5, 2013, em http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/171/166

Ferrante, R., Fuhrig, L. S. (2009). Digital Preservation: Using the Email Account XML Schema. Smithsonian Institution Archives. Washington, DC.

Ferreira, C. A. S. (2011). *Preservação da Informação Digital: uma perspectiva orientada para as bibliotecas*. Dissertação de Mestrado, Universidade de Coimbra, Coimbra, Portugal. Consultado em Janeiro 10, 2014, em https://estudogeral.sib.uc.pt/bitstream/10316/15001/1/Preserva%C3%A7%C3%A3o%20da%20Informa%C3%A7%C3%A3o%20Digital.pdf

Ferreira, M. (2006). Introdução à Preservação Digital: conceitos, estratégias e actuais consensos. Guimarães: Escola de Engenharia da Universidade do Minho. Consultado em Outubro 21, 2013, em http://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf

Ferreira, M. (2011). Certificação de Repositórios Digitais. *Seminário - (R)evolução da Informação Pública: preservar, certificar e acessibilizar*. Lisboa. Consultado em Novembro 10, 2013, em http://repositorium.sdum.uminho.pt/bitstream/1822/19412/1/Ceritificacao%20de%20repositorios%20digitais-0.2.pdf

Freitas, C. (2012). Garantir a autenticidade e o acesso continuado à informação digital: os desafios da preservação digital em arquivos. *11º Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas*, *11, Lisboa, 2012* – Integração, Acesso e Valor Social: atas. Lisboa: BAD. Consulado em Dezembro 13, 2013, em http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/272/pdf

GUILDHALL LIBRARY MANUSCRIPTS AND LONDON METROPOLITAN ARCHIVES (2004). Interim Digital Preservation Policy. City of London – Libraries, Archives and Guildhall Art Gallery Department. Consultado em Dezembro 17, 2013 em http://www.history.ac.uk/gh/digprespol.pdf

Gouveia, Luís Borges (2000). Gestão da Informação: Fluxos de informação e aplicações tipo. Consultado em Dezembro 12, 2013, em http://www2.ufp.pt/~lmbg/formacao/msc_tpe.pdf

Gouveia, L. B. (2004). Local e-government: a governação digital na autarquia. Porto: SPI-Sociedade Portuguesa de Inovação Consultadoria Empresarial e Fomento da Inovação, S. A. ISBN: 972-8589-41-7.

Gouveia, L. B., Ranito, J. (2004). Sistemas de Informação de Apoio à Gestão. Coleção Inovação e Governação nas Autarquias. Sociedade Portuguesa de Inovação, Porto. ISBN: 972-8589-43-3.

Henriksen, S., 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 Março 4, 2014, em http://www.dca-project.eu/images/uploads/banners/DCA_D62_Best_practices_for_a_digital_storage_infrastructure_20130506_Version1.pdf

Houston, B. (2008). E-mail and Records Management: Identifying, Organizing, and Preserving E-mail records. University of Wisconsin-Milwaukee. Consultado em Janeiro 28, 2014, em http://www.slideshare.net/herodotusjr/email-management-1862379

Lundgren, E. (2009). 10 Steps to Establishing an Effective Email Retention Policy. White Paper: 10 Steps to Effective Email Retention. Consultado em Janeiro 27, 2014, em http://www.ca.com/us/~/media/files/whitepapers/10-steps-email-retention-wp-us_198118.aspx

INTERNATIONAL COUNCIL ON ARCHIVES (2005). Electronic records: a workbook for archivists. Paris: ICA.

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

ISO TC 46/SC 11 (2010). Digital Records Preservation: Where to Start Guide. Consultado em Dezembro 28, 2013, em http://www.niso.org/apps/group_public/download.php/7273/Digital%20records%20preservation%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.

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.

Jones, V. A. (2012). RIM Fundamentals: Standards for Establishing Records and Information Management Programs. CRM; FAI. Consultado em Novembro 12, 2013, em http://content.arma.org/IMM/Libraries/July August_2012/IMM_0712_Rim_Fundamentals.sflb.ashx

Kirk, J. (1999). Information in organisations: directions for information management. *Information Research*, vol. 4 nº 3. (fev. 1999). Consultado em Dezembro 11, 2013, em http://informationr.net/ir/4-3/paper57.html

Kunde, N. M. (2008). CASE 7: Standards and Standards Development: The Development of Digital Records Conversion Process (ANSI/ARMA 16-2007). SAA. Society of American Archivists.

Levenson, S. P. (2008). PDF/A: Yesterday—Today—Tomorrow. PDF/A Competence Center. Consultado em Março 31, 2014, em http://pt.slideshare.net/Levenson/pdfa-keynote-presentation

LIBRARY OF CONGRESS (2014). Recommended Format Specification. Consultado em Maio 25, 2014, em http://www.loc.gov/preservation/resources/rfs/rfs20142015.pdf>

Liikanen, E. (2005). Políticas de Transição para a Sociedade em Rede na Europa. In "A Sociedade em Rede: Do Conhecimento à Acção Política". CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). Conferência. Lisboa: Imprensa Nacional - Casa da Moeda. P. 371 – 376. Consultado em Dezembro 10, 2013, em http://www.cies.iscte.pt/destaques/documents/Sociedade_em_Rede_CC.pdf

Lourenço, A., Henriques, C., Penteado, P. (coord.) (2013). Macroestrutura funcional (MEF). Lisboa: DGLAB. Consultado em Novembro 7, 2013, em http://www.adporto.pt/ficheiros_a_descarregar/2013-03-28_MEF-v2_0.pdf

Mcaninch, G., Eubank, K. (2008). Using EMCAP (Electronic Mail Capture and Preservation)

to Tame the E-Tiger. Consultado em Janeiro 17, 2014, em http://www.history.ncdcr.gov/SHRAB/ar/emailpreservation/docs/emcap_bpe_2008.pdf

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (2011). Guidance Concerning the use of E-mail Archiving Applications to Store E-mail. Consultado em Fevereiro 20, 2014, em http://www.archives.gov/records-mgmt/bulletins/2011/2011-03.html

NATIONAL ARCHIVES OF AUSTRALIA (2009). Digital Preservation Policy: Preserving Archival Digital Records Transferred from Commonwealth Agencies. Consultado em Outubro 14, 2013, em http://www.naa.gov.au/about-us/organisation/accountability/operations-and-preservation/digital-preservation-policy.aspx

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

Pennock, M. (2006). Instalment on "Curating E-Mails: A life-cycle approach to the management and preservation of e-mail messages. Digital Curation Manual. Consultado em Fevereiro 4, 2014, em http://www.dcc.ac.uk/resource/curation-manual/chapters/curating-e-mails/curating-emails.Pdf

Pinto, M. M. (2004). Gestão integrada de sistemas de informação em autarquias locais: uma abordagem sistémica. Porto: Universidade do Porto. Faculdade de Letras. Consultado em Outubro 25, 2013, em http://ler.letras.up.pt/uploads/ficheiros/3088.pdf

Pinto, M. M., Silva, A. M. (2005). Um Modelo Sistémico e Integral de Gestão da Informação nas Organizações. *2º Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação*. São Paulo, Brasil. Actas de Conferência Internacional. Consultado em Dezembro 1, 2013, em http://repositorio-aberto.up.pt/bitstream/10216/13461/2/modelo000071239.pdf

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 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, 2013, em http://www.bad.pt/publicacoes/index.php/congressosbad/article/view/560/370

Pinto, M. M. (2007b). A Preservação da informação em ambiente digital: Da Preservação do Documento à Preservação da Informação. Jornada de Profissionais da Informação.

[apresentação]. Arquivo Distrital da Guarda. Consultado em Novembro 12, 2013, em http://www.adguarda.pt/fotos/adg_mmgap_a_preservacao_informacao_era_digital_res.pdf

Pinto, M. M. (2009). Gestão da Informação e preservação digital: uma perspectiva portuguesa de uma mudança de paradigma. *CONGRESO ISKO-SPAÑA, 9, Valencia*. Nuevas perspectivas para la difusión y organización del conocimiento: actas. Valencia: Universidad Politecnica de Valencia. pp. 323-355. Consultado em Dezembro 2, 2013, em http://repositorioaberto.up.pt/bitstream/10216/25380/2/manuelapintogestao000100395.pdf

Pinto, M. M. (2009). Preservmap: Um roteiro de preservação na era digital. Porto: Edições Afrontamento. Coleção: Comunicação-Arte-Informação; 8. ISBN: 972-36-1070-1.

Pinto, M. M. (2011). Da transferência de suporte ao Sistema de Informação Organizacional: Um posicionamento urgente e estratégico. *Seminário - (R)evolução da Informação Pública: preservar, certificar e acessibilizar. Lisboa*. Consultado em Novembro 10, 2013, em https://sigarra.up.pt/flup/pt/publs_pesquisa.FormView?P_ID=30962

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. (2013). Da preservação de documentos à preservação da informação. In PINTO, Maria Manuela (2009). PRESERVMAP: Um roteiro da preservação na era digital. Porto: Edições Afrontamento; CETAC.Media.

Prom, C. J. (2010). Email Management and Preservation Guidelines. Consultado em Janeiro 31, 2014, em http://e-records.chrisprom.com/recommendations/develop-submissioningest-policies/email-management-and-preservation-advice/

Prom, C. J. (2011). Preserving Email. DPC Technology Watch Report.

Quivy, R.; Campenhoudt, L. V. (2008). Manual de Investigação em Ciências Sociais. S.l.: Gradiva. ISBN 9789726622758. Consultado em Dezembro 15, 2013, em http://www.fep.up.pt/docentes/joao/material/manualinvestig.pdf

Ribeiro, F., Silva, A. M. (2004). A Avaliação de informação: uma operação metodológica. Páginas a&b: arquivos e bibliotecas. Lisboa. ISSN 0873-5670. 14

Ribeiro, F. (2005). Organizar e representar informação: apenas um meio para viabilizar o

acesso?. I Encontro de Ciências e Tecnologias da Documentação e Informação – A informação nas organizações: o desafio da era digital. ESEIG, Vila do Conde.

Sagor, Richard (2011). The Action Research Guidebook: A Four-Stage Process for Educators and School Teams. 2nd Edition. Corwin. ISBN: 978-1-4129-8128-6.

SHEFFIELD ARCHIVES AND LOCAL STUDIES GROUP (2007). Preservation & Conservation Policy. Consultado em Novembro 13, 2013, em https://www.sheffield.gov.uk/dms/scc/management/corporatecommunications/documents/leisure-culture/libraries-copyright/archivespolicies/Preservation-and Conservation-Policy--PDF--73-KB-.pdf

SHEFFIELD ARCHIVES AND LOCAL STUDIES GROUP (2007). Digital Preservation Policy. Consultado em Novembro 14, 2013, em https://www.sheffield.gov.uk/dms/scc/management/corporatecommunications/documents/leisure-culture/libraries-copyright/archivespolicies/Digital-Preservation-Policy--PDF--107-KB-.pdf

Skinner, K., Schultz, M. (2010). A Guide to Distributed Digital Preservation. Atlanta: Educopia Institute. ISBN: 978-0-9826653-0-5. Consultado em Dezembro 10, 2013, em http://open.bu.edu/xmlui/bitstream/handle/2144/1351/GDDP_Educopia.pdf?sequence=1

Silva, A. M., Ribeiro, F. (2002). Das «ciências» documentais à ciência da informação: ensaio epistemológico para um novo modelo curricular. Porto: Edições Afrontamento (Biblioteca das Ciências do Homem. Plural; 4). ISBN: 972-36-0622-4.

Silva, A. M., et al. (1999). Arquivística – Teoria e Prática de uma Ciência da Informação. Porto: Edições Afrontamento.

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

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

Svärd, 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, (pp.159-176).

THE NATIONAL ARCHIVES (a). Digital Preservation Policy. Consultado em Outubro 24, 2013, em http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-preservation-policy.htm

THE NATIONAL ARCHIVES (b). Digital Preservation Strategy. Consultado em Outubro 27, 2013, em http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-preservation-strategy.htm

THE NATIONAL ARCHIVES (c). Guidance. Consultado em Outubro 28, 2013, em http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm

THE NATIONAL ARCHIVES (d). Digital Archiving. Consultado em Outubro 29, 2013, em http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-archiving.htm

Thibodeau, K. (2002). Overview of technological approaches to digital preservation and challenges in coming years. Consultado em Março 15, 2014, em http://www.clir.org/PUBS/reports/pub107/thibodeau.html>.

Thomaz, K. P. (2005). Gestão e preservação de documentos electrónicos de arquivo: revisão da literatura – parte I. *Arquivística*. vol. 1, nº 2, (pp. 8-30). (Jul./Dez. 2005).

Thomaz, K. P., Soares, A. J. (2004). A preservação digital e o modelo de referência Open Archival Information System (OAIS). *Data Grama Zero – Revista de Ciência da Informação*, vol. 5, nº 1 (fev. 2004) – Artigo 01. ISSN: 1517-3801. Consultado em Outubro 30, 2013, em http://www.dgz.org.br/fev04/F_I_art.htm

UK NATIONAL ARCHIVES (2011). Email Management and Preservation Guidelines. Consultado em Fevereiro 18, 2014, em http://e-records.chrisprom.com/recommendations/develop-submissioningest-policies/email-management-and-preservation-advice/

UMIC (2011a). Agência para a Sociedade do Conhecimento: Inquéritos sobre a Utilização de TIC na Administração Pública em 2011. Consultado em Dezembro 6, 2013, em http://www.umic.pt/images/stories/publicacoes5/III_AP_Electronica_2011.xls

UMIC (2011b). Agência para a Sociedade do Conhecimento: Experiência de Utilizador de Serviços Públicos Eletrónicos 2011. *Portugal no Topo do Ranking Europeu de Serviços Públicos Online*. Consultado em Dezembro 8, 2013, em http://www.umic.pt/index.php?option=com_content&task=view&id=3551&Itemid=111

UNIVERSITY OF WISCONSIN (2012). Electronic Communication Guidance for University Records. Madison Archives & Records Management. Consultado em Março 10, 2014, em http://archives.library.wisc.edu/records/bulletins/2012%20Electronic%20Communications%20-%20Final.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 Janeiro 7, 2014, em http://bad.pt/publicacoes/index.php/arquivosmunicipais/article/view/19/9

Wheatley, P. (2004). Institutional Repositories in the Context of Digital Preservation. *DPC Technology Watch Series Report 04-02*, Digital Preservation Coalition. University of Leeds. Consultado em Março 25, 2014, em http://dpconline.org/docs/DPCTWf4word.pdf

Wilson, T. (2003). Information Management. International Encyclopedia of Information and Library Science. Ed. by John Feather & Paul Sturges. London: Routledge.

Witt, M., et al. (2012). ISO 16363: Trustworthy Digital Repository Certification in Practice. *Libraries Faculty and Staff Presentations*. Paper 4. Consultado em Maio 14, 2014, em http://docs.lib.purdue.edu/lib_fspres/4

Zimmermann, R. (2010). *A colaboração e a gestão do conhecimento em instituições públicas*. Dissertação de mestrado, Universidade de Aveiro, Aveiro, Portugal. Consultado em Novembro 18, 2013, em http://ria.ua.pt/bitstream/10773/1810/1/2010001621.pdf

Anexos

Anexo 1: Políticas de Segurança de Informação

A gestão da Segurança da Informação é um processo essencial e imprescindível, sobretudo presentemente em que nos deparamos com o crescimento da quantidade da informação digital.

Como referido anteriormente, a segurança e a preservação da informação encontram-se interligadas, pelo que é igualmente necessária a elaboração de um conjunto de políticas de suporte que são essenciais para a observação dos três princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

As políticas devem seguir a estrutura aconselhada pela ISO/IEC 27003:

- **Introdução** – uma breve explicação do conteúdo da política;
- **Objetivo** – o propósito da política;
- **Âmbito** – define a que partes se aplicam os princípios enumerados na política;
- **Responsabilidades** – são definidos os responsáveis pelo cumprimento dos requisitos enumerados na política, incluindo a responsabilidade pelo conteúdo e pela atualização da política;
- **Conteúdo específico da política** – os requisitos e princípios inerentes à política em específico;
- **Condicionantes (ou Políticas e normas relacionadas)** – são definidas as limitações (se aplicável) e eventuais Políticas ou Normas que tenham relação direta.

Estas políticas são fundamentais, uma vez que permitem:

- A análise e identificação dos riscos, e respetivas categorias, que aliadas a um conjunto de controlos potenciam a deteção de ameaças e riscos;
- O tratamento dos riscos, através dos mecanismos necessários na prevenção e correção das ameaças e vulnerabilidades detetadas.

De acordo com as normas anteriormente referidas, uma Política de Segurança da Informação deve corresponder a alguns requisitos básicos:

- deve ser aprovada pela Direção, publicada e comunicada a todos os funcionários e partes externas relevantes;
- deve indicar o compromisso da gestão e a abordagem da organização relativamente à gestão da segurança da informação;

- deve 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;
- deve 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;
- deve conter um *framework* que estabeleça os objetivos de controlo e controlos, incluindo a estrutura de avaliação e de gestão do risco;
- deve conter uma definição das responsabilidades gerais e específicas para a gestão da segurança da informação, incluindo o registo dos incidentes de segurança da informação;
- deve conter uma breve explicação das políticas, princípios, normas e requisitos de conformidade que se revelem de particular importância para a organização;
- deve ser analisada criticamente a intervalos planeados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

A **Comissão de Gestão de Segurança da Informação** deve ser responsável por fornecer a direção e estratégia no âmbito da evolução da maturidade de TI/SI e do nível da segurança de informação para a camada de gestão da organização. É essencial, na medida em que, a gestão dos SI e da própria informação revela-se crucial a nível estratégico.

A **Política de Classificação da Informação** deve estabelecer os princípios e as melhores práticas de Segurança da Informação a aplicar na classificação da informação. Deve ser a base para a implementação de um processo adequado e controlado de gestão do ciclo de vida da informação, de forma a assegurar o seu correto tratamento, desde a sua criação, passando pelo seu manuseamento, distribuição, armazenamento e terminando na sua destruição.

O objetivo da **Política de Gestão de Acessos** prende-se essencialmente com o estabelecimento dos princípios a aplicar na gestão das contas de utilizadores e privilégios de acesso à informação.

- **Gestão de utilizadores e privilégios**

Foram, por isso, definidos os princípios relativos à gestão dos utilizadores e seus

privilégios, ressaltando a existência de um procedimento formal para registo de utilizadores de forma a conceder, alterar e revogar os acessos a todos os serviços e sistemas de informação. Os pedidos de acesso devem ser dirigidos à DMTC, onde seguirão um circuito de aprovação, envolvendo os respetivos dirigentes. Outro dos princípios implementado é o de que as contas de utilizador não usadas durante um determinado período de tempo devem ser desativadas e/ou removidas através de um procedimento periódico de revisão, excepto nos casos em que exista uma justificação formal. Os tempos são definidos de acordo com as características de cada sistema.

- **Identificadores *(User ID's)***

Cada colaborador ou entidade externa necessita de um identificador único e uma *password* intransmissível. A utilização de identificadores genéricos (contas genéricas ou de grupo) apenas é permitida quando o sistema não permite efetuar uma gestão de utilizadores individuais, sendo sujeita a aprovação dos Diretores da DMSI. A nomenclatura utilizada na geração dos identificadores encontra-se definida na Política de Gestão de *Passwords*.

- **Acessos Privilegiados**

Os acessos privilegiados devem ser restritos e controlados. Quando necessários, devem ser atribuídos a um identificador especial, diferente do identificador usual do utilizador. Este terá um período de validade, findo o qual terá que confirmar a necessidade de o manter.

- **Entidades Externas**

Os acessos atribuídos às Entidades Externas devem ter um período de validade associado durante a vigência do contrato com a CMP, findo o qual, e salvo pedidos aprovados, os acessos serão revogados.

- **Revisão dos Privilégios de Acesso**

Os privilégios de acesso devem ser revistos em intervalos regulares, pelo menos uma vez por ano, pela hierarquia, e sempre que ocorra uma alteração, como uma saída, uma mudança de funções ou de área.

A **Política de Gestão de *Passwords*** tem na sua base os princípios que devem ser mantidos na utilização das *passwords* de acesso aos sistemas de informação. Devem, por isso, ser definidas as regras de composição das *passwords* e verificadas automaticamente.

É igualmente definida a gestão das *passwords*, através dos passos necessários que vão da solicitação da criação de novo utilizador por parte da Chefia de cada UO, à verificação da sua existência na Base de Dados por um colaborador do Helpdesk, até à criação do *user*, caso

se comprove a sua inexistência e após teste ao funcionamento dos acessos. O utilizador é obrigado a alterar a sua *password* de 4 em 4 meses, conforme estipulado, não podendo reutilizá-la antes de 5 iterações.

Devem ser definidas as responsabilidades dos utilizadores que devem respeitar e seguir um conjunto de boas práticas de Segurança da Informação no que diz respeito à seleção e utilização de *passwords*.

A **Política de Utilização do Correio Eletrónico** aponta as principais regras a serem seguidas de forma a facilitar a proteção e salvaguarda da informação envolvida na troca de mensagens eletrónicas, assim como os princípios de utilização correta dos recursos do correio eletrónico.

São igualmente definidas as regras no que toca à informação sensível. A informação classificada como **Confidencial** não deve ser transmitida em redes públicas consideradas inseguras. A inclusão de endereços externos em listas internas de distribuição não deve ser autorizada, a fim de evitar qualquer transferência acidental de informação **Confidencial** ou de **Uso Interno** para o exterior. O serviço de correio eletrónico obedece também a limites, os quais são categorizados de acordo com o tipo de conta de e-mail. São definidos os limites da dimensão máxima das mensagens enviadas, do armazenamento de mensagens e do número máximo de destinatários em simultâneo. As caixas de correio que excedam os limites definidos em "Aviso" recebem uma mensagem de notificação, ficando proibidas de enviar novas mensagens a partir do limite definido em "Bloqueio".

A **Política de *Backups*** define o conjunto de procedimentos a levar a cabo para se salvaguardar os sistemas de informação.

Na aplicação que gere a realização de *backups*, é efetuado o seu planeamento. Diariamente é realizada uma verificação dos eventos gerados pela aplicação de *backups* e aos e-mails que a aplicação de *backups* gera em caso de falhas. Ocorrendo falhas, são analisadas as causas e realizados *backups* adicionais, se tal for possível.

Caso o problema com a realização de *backup* não seja resolvido, é informada a Chefia da DMTC para que se definam ações que permitam resolver o problema. O processo é encerrado quando o problema é resolvido. São também definidas as regras de *backups*, explicitando os casos em que estes garantem a segurança dos sistemas, assim como, a proteção antivírus que se encontra instalada em todos os computadores, sendo o programa atualizado remotamente de forma automática.

O objetivo da **Política de Acesso à Internet** é estabelecer os princípios e as

melhores práticas a aplicar no acesso à Internet e na utilização correta dos seus recursos.

Um ponto essencial é o definido na Informação Sensível, em que não é permitido fornecer o acesso a informação classificada como **Confidencial**, de **Acesso Restrito**, de **Acesso Público** ou de **Uso Interno** a pessoas não autorizadas; não é permitido usar o Messenger para divulgar este tipo de informação nem é permitida a participação em *chat-rooms* ou fóruns de discussão que possa comprometer a informação interna da CMP.

A **Política de Gestão de Operações** refere os princípios da gestão de operações, nomeadamente os procedimentos operacionais e responsabilidades, relativamente à documentação dos procedimentos operacionais, à gestão de alterações, à segregação de funções e à separação dos ambientes de desenvolvimento, teste e produção.

São também referidos os princípios relativos à gestão de serviços de terceiros, ou seja, os serviços de entrega, revisão e monitorização. Menciona-se o planeamento e a aceitação de sistemas e a proteção contra código malicioso.

A **Política de Secretária Limpa Ecrã Limpo** tem como objetivo a definição de um conjunto de regras e procedimentos que inviabilizem o acesso a informação sensível por parte de outros colaboradores ou de entidades externas, o acesso a áreas sujeitas a controlo, bem como o acesso aos computadores e aplicações.

O objetivo da **Política de Segurança Física e Ambiental** prende-se com os princípios a aplicar na gestão da segurança física e ambiental da organização, em sistemas da sua propriedade e gestão. São classificadas as instalações físicas, inclusivamente onde residam sistemas e/ou informação, com ocupação humana, temporária ou permanente, de acordo com o seu nível de criticidade, como áreas administrativas, salas de formação, etc. Devem também ser enumerados os princípios que têm como objetivo impedir o acesso físico, danos e interferência não autorizados ao perímetro e à informação, assim como os princípios relativos à proteção dos equipamentos para reduzir o risco de acesso não autorizado à informação e para protegê-los de perdas e danos.

A **Política de Segurança de Rede** compreende os princípios que visam reduzir os riscos associados ao acesso não autorizado à rede de dados de uma organização, através da definição das regras que devem ser cumpridas para utilização de equipamentos na rede.

Foram definidos os princípios na utilização de equipamentos na rede de dados da CMP, tais como: ligação de estações de trabalho, de dispositivos móveis, de servidores, de sistemas virtuais, de equipamentos ativos; utilização de sistemas que permitem acesso de/para o exterior da rede de dados da CMP; atribuição de recursos informáticos (*hardware* ou

software) e comunicações; identificação dos equipamentos na rede e localização dos pontos de rede na CMP.

Anexo 2: Tabela de Controlo de Documentos – Repositório Confiável/ Plano de Preservação

Controlo de documentos - Repositório Confiável / Plano de Preservação						
Código Documento	**Designação Documento**	**Nº Requisito ISO 16363:2012**	**Nº Requisito ISO/TR 18492:2005**	**Outros p/ Plano de Preservação**	**Execução**	**Obs.**
DMAG_DSE_01	Declaração de Missão	3.1.1; 3.1.3; 3.3.1; 3.3.2; 4.1.1		Londres; Sheffield; NAA	Feito	
DMAG_DSE_RC_01	Declaração de Missão	3.1.1			Feito	
DMAG_DSE_02	Declaração de Objetivos estratégicos de preservação		5.2			
DMAG_DSE_03	Declaração de Elementos estratégicos de preservação		6			
DMAG_DSE_04	Plano Estratégico de Preservação	3.1.2; 3.3.2.1	5.2		Feito	
DMAG_DSE_05	Atas de reunião	3.1.2			Feito	Documento Interno CMP
DMAG_DSE_06	Plano de Sucessão	3.1.2.1				
DMAG_DSE_07	Plano de Contingência	3.1.2.1; 3.4.1		NARA	Feito	
DMAG_DSE_08	Planos de Atividades	3.1.2.1				
DMAG_DSE_09	Acordos de custódia	3.1.2.1			Feito	Documento Interno CMP

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_10	Documentos que explicitem a intenção de garantir a continuidade do repositório	3.1.2.1				
DMAG_DSE_11	Políticas, planos, protocolos e documentos de análise financeira	3.1.2.2				
DMAG_DSE_12	Procedimentos de monitorização	3.1.2.2; 3.3.2.1; 3.3.5; 4.6.1.1	7.4			
DMAG_DSE_13	Política de Gestão da Coleção	3.1.3				
DMAG_DSE_14	Política de Preservação	3.1.3; 3.3.2; 3.3.2.1; 4.1.1.1; 4.1.1.2; 4.4.1.1	5.2; 7.1; 7.2	NAA; Sheffield; Londres	Feito	
DMAG_DSE_15	Estratégia de Preservação		5.2	ANZ; Vancouver	Feito	
DMAG_DSE_16	Matriz de funções, competências e responsabilidades dos funcionários	3.2.1; 3.2.1.1; 3.2.1.2			Feito	Documento Interno CMP
DMAG_DSE_17	Descrições de cada cargo	3.2.1; 3.2.1.1				
DMAG_DSE_18	Organograma	3.2.1; 3.2.1.2; 5.2.3				
DMAG_DSE_19	Plano de recursos humanos	3.2.1.1				
DMAG_DSE_20	Plano de formação	3.2.1.3			Feito	Documento Interno CMP
DMAG_DSE_21	Evidências de formações internas e/ou externas	3.2.1.3			Feito	Documento Interno CMP
DMAG_DSE_22	Documentação das despesas de formação	3.2.1.3				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_23	Cópias dos certificados de formação e acreditação	3.2.1.3				
DMAG_DSE_24	Definição da comunidade-alvo	3.3.1				
DMAG_DSE_25	Acordos de nível de serviço (SLA's) e condições de acesso dos utilizadores/permissões	3.3.1				
DMAG_DSE_26	Políticas de Segurança	3.3.2.1	7.3			
DMAG_DSE_27	Definição do ciclo de revisão da documentação	3.3.2.1				
DMAG_DSE_28	Contratos de serviços	3.3.3				
DMAG_DSE_29	Documentação de aquisição, implementação, atualização e eliminação de *software* e *hardware*	3.3.3	6.2			
DMAG_DSE_30	Documentos atuais e obsoletos (versões anteriores) de políticas e procedimentos	3.3.3				
DMAG_DSE_31	Relatórios de auditorias e certificações técnicas e financeiras	3.3.4				
DMAG_DSE_32	Documentação referente aos procedimentos de contratação pública	3.3.4				
DMAG_DSE_33	Contratos com outras entidades	3.3.4				
DMAG_DSE_34	Documentação dos procedimentos e mecanismos para monitorar as medidas de integridade e para responder a resultados de medidas de integridade que indicam se os conteúdos digitais estão em risco	3.3.5				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_35	*Checklists* de autoavaliação	3.3.6				
DMAG_DSE_36	Preparação para auditoria	3.3.6				
DMAG_DSE_37	Relatórios financeiros	3.4.1; 3.4.2				
DMAG_DSE_38	Orçamentos	3.4.1				
DMAG_DSE_39	Procedimentos de auditoria	3.4.1				
DMAG_DSE_40	Auditoria financeira anual e relatório	3.4.2				
DMAG_DSE_41	Política de Gestão do Risco	3.4.3				
DMAG_DSE_42	Análise de custo-benefício	3.4.3				
DMAG_DSE_43	Procedimentos de revisão e monitorização	3.4.3				
DMAG_DSE_44	Acordos de licença ou de depósito	3.5.1; 3.5.1.1; 3.5.1.2; 3.5.1.3				
DMAG_DSE_45	Procedimentos de revisão dos contratos	3.5.1				
DMAG_DSE_46	Especificação de direitos transferidos para diferentes tipos de conteúdo digital (se aplicável)	3.5.1.1				
DMAG_DSE_47	Recibos de confirmação enviados para o produtor/depositante	3.5.1.3				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_48	Políticas e procedimentos de acordo com os requisitos legais	3.5.1.4; 3.5.2				
DMAG_DSE_49	Definição de direitos e permissões de produtores e colaboradores	3.5.1.4				
DMAG_DSE_50	Procedimentos de ingestão de objetos digitais	4.1.1; 4.1.1.1				
DMAG_DSE_51	Registos do tipo de objetos digitais	4.1.1.2				
DMAG_DSE_52	Requisitos de transferência	4.1.2	5.2.7.2			
DMAG_DSE_53	Esquemas de metainformação	4.1.2; 4.1.3; 4.5.2				
DMAG_DSE_54	Pacote de Informação para os PIS (*SIP*)	4.1.3				
DMAG_DSE_55	Especificações de formatos de ficheiro	4.1.3				
DMAG_DSE_56	Registos de procedimentos e autenticações	4.1.4				
DMAG_DSE_57	Ficheiros de registo do sistema responsável pelo procedimento de ingestão	4.1.5				
DMAG_DSE_58	Procedimentos detalhados	4.1.5				
DMAG_DSE_59	Documentos que mostram o nível de controlo físico do repositório e a metainformação associados	4.1.6	7.3.3			
DMAG_DSE_60	Relatórios	4.1.7				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_62	Conjunto de metainformação ligados aos objetos digitais	4.1.8				
DMAG_DSE_63	Registos de decisões e de medidas tomadas	4.1.8				
DMAG_DSE_64	Documentação que identifica claramente cada classe de PIA (*AIP*)(definição) e a sua implementação no repositório	4.2.1; 4.2.1.1				
DMAG_DSE_65	Demonstração da utilização das definições para extrair informação	4.2.1.2				
DMAG_DSE_66	Descrição dos processos	4.2.2; 4.2.3; 4.2.3.1				
DMAG_DSE_67	Documentação da relação PIS (*SIP*)-PIA (*AIP*)	4.2.2; 4.2.3; 4.2.3.1				
DMAG_DSE_68	Documentação clara de como os PIA's são derivados dos PIS (*SIP*)	4.2.2; 4.2.3; 4.2.3.1				
DMAG_DSE_69	Registos de eliminação	4.2.3; 4.2.3.1			Feito	Documento Interno CMP
DMAG_DSE_70	Documentação da nomenclatura e evidência física da sua aplicação (registos)	4.2.4; 4.2.4.1; 4.2.4.1.1; 4.2.4.1.2; 4.2.4.1.3; 4.2.4.1.4; 4.2.4.1.5; 4.2.4.2				
DMAG_DSE_71	Registos de Informação de Representação (incluindo registos de formatos)	4.2.5; 4.2.5.1; 4.2.5.2; 4.2.5.3; 4.2.5.4				
DMAG_DSE_72	Registos que incluem Informação de Representação e indicadores persistentes para objetos digitais relevantes	4.2.5; 4.2.5.1; 4.2.5.2; 4.2.5.3; 4.2.5.4				
DMAG_DSE_73	Definição da ingestão de objetos digitais	4.2.6; 4.2.6.1; 4.2.6.2; 4.2.6.3				
DMAG_DSE_74	Documentação sobre a forma como o repositório adquire e gere a Informação de Descrição de Preservação	4.2.6; 4.2.6.1; 4.2.6.2; 4.2.6.3				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_75	Procedimentos de testes de acesso aos objetos digitais para verificação dos requisitos de acessibilidade, integridade, autenticidade e inteligibilidade	4.2.7; 4.2.7.1; 4.2.7.2; 4.2.7.3; 4.2.8	5.2.3; 5.2.6; 5.2.7; 5.2.7.4			
DMAG_DSE_76	Verificação de integridade dos dados	4.2.9; 4.4.1.2; 4.5.2; 4.5.3; 4.5.3.1				
DMAG_DSE_77	Documentação que identifica claramente cada classe de objetos digitais	4.2.9				
DMAG_DSE_78	Registo dos metainformação de preservação, armazenados e ligados aos objetos digitais	4.2.10; 4.4.2; 4.4.2.2				
DMAG_DSE_79	Documentação sobre as decisões e ações tomadas	4.2.10; 4.4.2				
DMAG_DSE_80	Estratégias de preservação de objetos digitais	4.3.1				
DMAG_DSE_81	Inquéritos à comunidade-alvo	4.3.2				
DMAG_DSE_82	Serviço de registo da Informação de Representação	4.3.2.1				
DMAG_DSE_83	Atualização das Políticas e Planos de Preservação	4.3.3				
DMAG_DSE_84	Definição do período de atualização (não superior a 5 anos)	4.3.3				
DMAG_DSE_85	Planos de Preservação	4.3.3.1				
DMAG_DSE_86	Serviço de registo de formatos	4.3.3.1				
DMAG_DSE_87	Esquemas de metainformação de preservação adequados	4.3.4				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_88	Prova de usabilidade de objetos digitais selecionados aleatoriamente dentro do sistema	4.3.4				
DMAG_DSE_89	Estratégias de armazenamento de objetos digitais	4.4.1				
DMAG_DSE_90	Workflows de preservação	4.4.1.1				
DMAG_DSE_91	Estratégias de armazenamento e de migração/conversão dos objetos digitais	4.4.1.1	6.4.1; 6.4.4; 6.4.5;			
DMAG_DSE_92	Documentação sobre as ações que podem ser executadas contra um PIA (*AIP*), erros e anomalias e procedimentos de monitorização	4.4.2.1				
DMAG_DSE_93	Informação Descritiva e metainformação	4.5.1				
DMAG_DSE_94	Documentação da relação entre o PIA (*AIP*) e a sua Informação Descritiva	4.5.2; 4.5.3; 4.5.3.1				
DMAG_DSE_95	Identificadores persistentes	4.5.2; 4.5.3; 4.5.3.1				
DMAG_DSE_96	Documentação do sistema e arquitetura técnica	4.5.2; 4.5.3; 4.5.3.1				
DMAG_DSE_97	Políticas de Acesso aos objetos digitais	4.6.1; 4.6.2				
DMAG_DSE_98	Matrizes de autenticação	4.6.1				
DMAG_DSE_99	Registo de falhas de acesso	4.6.1.1				
DMAG_DSE_100	Ferramentas de notificação em caso de problemas/anomalias	4.6.1.1				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_101	Relatórios de erros e ações tomadas	4.6.2.1				
DMAG_DSE_102	Procedimentos de trabalho	4.6.2.1			Feito	Documento Interno CMP
DMAG_DSE_103	Instruções de trabalho	4.6.2.1			Feito	Documento Interno CMP
DMAG_DSE_104	Procedimentos de avaliação da infraestrutura tecnológica	5.1.1	6.4.5.2.2; 6.4.5.2.3			
DMAG_DSE_105	Componente de exportação de registos autênticos para um sistema independente	5.1.1				
DMAG_DSE_106	Relatórios de avaliação/monitorização de tecnologia	5.1.1.1				
DMAG_DSE_107	Procedimento de manutenção de *hardware*	5.1.1.1.1; 5.1.1.1.5				
DMAG_DSE_108	Manutenção de um inventário de *hardware* atual	5.1.1.1.1; 5.1.1.1.5				
DMAG_DSE_109	Procedimento de monitorização às alterações de *hardware*	5.1.1.1.2; 5.1.1.1.6				
DMAG_DSE_110	Procedimentos de avaliação do *hardware*	5.1.1.1.3; 5.1.1.1.7				
DMAG_DSE_111	Evidência de ativos financeiros em curso reservados para aquisição de *hardware*	5.1.1.1.4; 5.1.1.1.8				
DMAG_DSE_112	Demonstração de redução de custos através de custo amortizado de um novo sistema	5.1.1.1.4; 5.1.1.1.8				
DMAG_DSE_113	Política de backups	5.1.1.2			Feito	

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_114	Plano de recuperação de desastres	5.1.1.2; 5.2.4		Sheffield	Feito	
DMAG_DSE_115	Testes de backups	5.1.1.2				
DMAG_DSE_116	Análise de risco	5.1.1.3; 5.2.1; 5.2.2				
DMAG_DSE_117	Relatórios de erros e incidentes	5.1.1.3				
DMAG_DSE_118	Análise da integridade dos objetos digitais	5.1.1.3				
DMAG_DSE_119	Procedimentos relativos à notificação de incidentes para os administradores	5.1.1.3.1				
DMAG_DSE_120	Registos de Metainformação de preservação	5.1.1.3.1	6.3			
DMAG_DSE_121	Rastreio de fontes de incidentes	5.1.1.3.1				
DMAG_DSE_122	Processo de registo de riscos e avaliação de atualizações de *software*	5.1.1.4	6.4.3			
DMAG_DSE_123	Documentação referente às instalações de atualização	5.1.1.4				
DMAG_DSE_124	Processos de mudança de suportes de armazenamento e alteração de *hardware*	5.1.1.5				
DMAG_DSE_125	Matriz de rastreabilidade entre processos críticos e requisitos obrigatórios	5.1.1.6				
DMAG_DSE_126	Registo de gestão de alterações na mudança de processos críticos	5.1.1.6.1				

Código Documento	Designação Documento	Nº Requisito ISO 16363:2012	Nº Requisito ISO/TR 18492:2005	Outros p/ Plano de Preservação	Execução	Obs.
DMAG_DSE_127	Avaliação de riscos	5.1.1.6.1				
DMAG_DSE_128	Procedimentos de teste	5.1.1.6.2				
DMAG_DSE_129	Documentação de resultados anteriores e avaliação/análise do impacto de alterações em processos críticos	5.1.1.6.2				
DMAG_DSE_130	Testes de validação da existência do objeto para cada localização registada e no sistema de armazenamento	5.1.2				
DMAG_DSE_131	Workflows de sincronização	5.1.2.1				
DMAG_DSE_132	Procedimentos de sincronização	5.1.2.1				
DMAG_DSE_133	Emprego das normas da família ISO 27000	5.2.1; 5.2.2; 5.2.3; 5.2.4				
DMAG_DSE_134	Lista de controlo do sistema	5.2.2				
DMAG_DSE_135	Plano de continuidade	5.2.4			Feito	
DMAG_DSE_136	Identificação e Avaliação de Formatos				Feito	
DMAG_DSE_137	Identificação de Sistemas de Informação				Feito	

	Segurança Informação
	Preservação e Segurança Informação
	Preservação Informação

Anexo 3: Instrumentos normativos (Gestão de documentos de arquivo)

Acrónimo - Nome	Entidade Responsável	Descrição
ISO 15489-1 - Information and documentation – Records Management: Part 1: General [versão portuguesa NP 4438-1:2005] normativa que incide especificamente sobre a gestão de arquivos correntes, não negligenciando aspetos fundamentais da conservação a longo prazo dos documentos eletrónicos; Part 2: Guidelines [versão portuguesa NP 4438-2:2005];	ISO	A norma ISO 15489-1 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. Fornece orientação sobre gestão de registos em apoio a uma estrutura de processo de qualidade em conformidade com as normas ISO 9001 e ISO 14001; Fornece 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 23081-1:2004 - Information and documentation – Records management processes - Metadata for records, que complementa a ISO 15489 ao nível da metainformação: Part 1: Principles; Part 2 : Conceptual and implementation issues Part 3 : Self-assessment method;	ISO/TS	ISO 23081-1:2004 abrange os princípios que sustentam e governam a metainformação da gestão de registos. Estes princípios aplicam-se ao longo do tempo para: Registos e sua metainformação; Todos os processos que lhes dizem respeito; Qualquer sistema em que residem; Qualquer organização que é responsável pela sua gestão.
ISO 14721:2003 - Space data and information transfer systems. Open archival information system (OAIS). Reference model.	ISO	A normativa ISO 14721:2003 especifica um modelo de referência para um sistema de informação de arquivo aberto (OAIS). O objetivo desta é estabelecer um sistema de

Acrónimo - Nome	Entidade Responsável	Descrição
		arquivo de informação, tanto digitalizada como física, com um esquema organizacional composto por pessoas que aceitam a responsabilidade de preservar a informação e disponibilizá-la para uma comunidade designada. Este modelo de referência aborda uma gama completa de funções de arquivo de preservação da informação, incluindo ingestão, armazenamento de arquivo, gestão de dados, acesso e disseminação. Também aborda 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	ISO/TR	Esta norma descreve a metodologia de implementação e operação de Sistemas de Gestão da Informação 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 investigado, desde a sua criação e/ou captura, até à sua eventual destruição.
ISO 16363:2012 – Space data and information transfer systems – Audit and certification of trustworthy digital repositories.	ISO	Define um Guia de práticas recomendadas para fundamentar um processo de certificação e de auditoria para avaliar a confiabilidade de um repositório digital, no âmbito da preservação em meio digital
ISO/TR 18492:2005 - Long-term preservation of electronic document-based information.	ISO/TR	A norma ISO / TR 18492:2005 fornece orientações metodológicas práticas para a preservação a longo prazo e recuperação de documentos eletrónicos com base de informação, autênticos, baseada em, quando o período de retenção excede a expectativa de vida da tecnologia (*hardware* e *software*) utilizada para criar e manter a informação. Esta norma também reconhece que garantir a

Acrónimo - Nome	Entidade Responsável	Descrição
		preservação a longo prazo e recuperação de documentos eletrónicos, com base de informação, autênticos, deve envolver especialistas de TI, gestores de documentos, gestores de registos e arquivistas
ISO/TR 13028:2010 - Information and documentation: Implementation guidelines for digitization of records.	ISO/TR	Estabelece diretrizes para a criação e manutenção de registos em formato digital apenas, onde o papel original ou outro registro de origem não-digital, foi copiado por digitalização; estabelece as diretrizes de boas práticas para a digitalização para garantir a confiabilidade e confiabilidade dos registos e permitir a consideração da eliminação dos registos de origem não-digitais; estabelece diretrizes de boas práticas para a confiabilidade dos registos digitalizados que podem ter impacto sobre a admissibilidade legal e peso probatório de tais registos; estabelece diretrizes de boas práticas para a acessibilidade de registos digitalizados para enquanto eles são necessários; especifica as estratégias para ajudar na criação de registos digitalizados aptos para retenção a longo prazo, e estabelece as diretrizes de boas práticas para a gestão de registos de origem não-digitais seguindo a digitalização.
ISO/IEC 27001:2005 - Information technology. Security techniques. Information security management systems. Requirements.	ISO/IEC	Esta norma aborda os requisitos para um SGSI, sendo através desta que se consegue 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.
MoReq2010 - Modular Requirements	DLM Forum	A especificação descreve um Modelo de

Acrónimo - Nome	Entidade Responsável	Descrição
for Records Systems	Foundation	Requisitos para a Gestão de Arquivos Eletrónicos. Este modelo destaca, sobretudo, os requisitos funcionais para a gestão de documentos de arquivo eletrónicos através de um Sistema de Gestão de Arquivos Eletrónicos (SGAE).

Anexo 4: Documentos de Suporte à Especificação

Documento de Suporte à Especificação: Declaração de Missão

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma Declaração de Missão, para a elaboração do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

Documento de Suporte à Especificação: Declaração de Missão

3. RESPONSABILIDADES

Actividade / Função	DM	DD	CD	SEC	QC
Recepção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Recepção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Declaração de Missão

Os Arquivos Metropolitanos de Londres existem para coletar documentos do rico passado histórico de Londres e para encontrar e coletar documentos da presente, vibrante e diversificada Londres, que são selecionados, catalogados, armazenados e permanentemente preservados para o uso e benefício das gerações presentes e futuras. A Política de Preservação Digital foi criada para apoiar o uso a longo prazo e preservação de documentos em meio digital.

Os The National Archives (TNA) têm como objetivo preservar qualquer tipo de registo digital que é:

- *Criado usando qualquer tipo de aplicação;*
- *Criado em qualquer plataforma de computação;*
- *Entregues em qualquer suporte digital;*
- *A partir de qualquer organização da Commonwealth;*
- *Proporcionar a descoberta e o acesso para as gerações atuais e futuras.*

Sob a Lei de Arquivos de 1983, os The National Archives são responsáveis pela preservação de documentos da Commonwealth que formam os recursos arquivísticos da Commonwealth. Estes incluem documentos nado-digitais e cópias principais de preservação digital dos documentos originais analógicos.

Os Arquivos só aceitam documentos de entidades governamentais que tenham sido "condenados" a "Manter como Arquivo Nacional" (isto é, para a retenção permanente) sob uma autoridade registos. ("Condenação" é um processo de utilização de uma autoridade de documentos ou outro instrumento para decidir sobre a manutenção, destruir ou transferir um registo.) Em circunstâncias excecionais, os Arquivos aceitarão registos cujo valor não foi identificado, por exemplo, os registos que estão em risco ou são considerados um recurso significativo.

Os Arquivos não preservam os meios utilizados para criar, gerir ou apresentar documentos digitais, por exemplo, software de gestão de registos. Os Arquivos aceitam a exportação de documentos digitais e a respetiva metainformação de sistemas, e não as exportações dos próprios sistemas.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Director de Departamento
DM	- Director Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Acções de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Repositório Confiável: Declaração de Missão

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma Declaração de Missão para o Repositório Digital Confiável da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Declaração de Missão do Repositório

Para esta declaração de missão é apresentado o exemplo do primeiro repositório digital a ser certificado através das indicações da norma ISO 16363:2012, o projeto Portico:

O repositório digital está comprometido com a preservação das publicações digitais, como revistas eletrónicas, e-books e outros conteúdos digitais. A participação neste repositório digital, fornece um seguro que protege a sua biblioteca de perda de acesso a e-conteúdo licenciado diretamente pelas editoras. Quando o conteúdo preservado no vasto repositório se tornar indisponível a partir de outras fontes, o Portico irá continuar a fornecer o acesso direto a esse mesmo conteúdo, a todas as instituições participantes. Na maioria dos casos, o repositório também pode fornecer acesso a materiais tornados indisponíveis após uma anulação de licença.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Plano de Preservação

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma estrutura base, para a construção do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

R - Responsável; E - Envolvido

4. DESCRIÇÃO

Estrutura base para a construção do Plano de Preservação

1. **Considerar:**
    a) Políticas de preservação;
    b) Obrigações legais;
    c) Constrangimentos organizacionais;
    d) Condicionalismos técnicos;
    e) Necessidades dos utilizadores;
    f) Objetivos de preservação
    g) Tipos de preservação
        1. Preservação a longo prazo - o acesso contínuo a materiais digitais, ou pelo menos, à informação contida neles, por tempo indeterminado.
        2. Preservação a médio prazo – o acesso contínuo a materiais digitais, para além das mudanças na tecnologia, por um período definido de tempo, mas não indefinidamente.
        3. Preservação de curto prazo - O acesso a materiais digitais por um período de tempo definido durante a utilização encontra-se previsto embora não seja para extensão num futuro próximo e / ou até que se torne inacessíveis devido a mudanças na tecnologia.
2. **Descrever:**
    a. O contexto de preservação;
    b. As estratégias de preservação avaliadas (como a migração, conversão e emulação) (Ver DMAG_Anexo_DSE_Plano_preservação_01).
    c. E a decisão resultante para uma estratégia, incluindo a fundamentação da decisão.
3. **Definir:**
    a. Série de ações de preservação a serem tomadas pela instituição responsável, devido a um risco identificado para um determinado conjunto de objetos digitais ou registos (chamados de coleção).

b. Um procedimento bem documentado de ações para garantir o acesso e a utilização da coleção a longo prazo.
   I. Contexto de preservação;
   II. Estratégia de preservação selecionada;
   III. Os resultados da avaliação de diferentes alternativas de preservação e a decisão (Ver DMAG_Anexo_DSE_Plano_preservação_03);
   IV. Papéis e responsabilidades para o plano de preservação e para a sua monitorização;
   V. Acionadores que iniciam a execução do plano;
      - Custo (estimado) de realizar o plano de preservação:
        - O custo para a elaboração do plano de preservação;
        - O custo para a execução do plano de preservação.

Tabela 1 - Custos típicos de eventos

Atividades	Custo dos eventos
Atividades de criação e gestão do sistema	Criação de infraestrutura organizacional Criação de arquitetura do repositório Administração do arquivo Operação do Repositório Manutenção Atualizações
Atividades do ciclo de vida/fluxo de trabalho de material digital	Seleção Aquisição Validação Criação de coleções digitais, Conversão do material depositado Negociação e gestão de direitos Descrição de Recursos, por exemplo, catalogação Criação de metainformação e metainformação de preservação Armazenamento Avaliação e revisão Eliminação
Atividades específicas de preservação	Atividades de planeamento, tais como Visão Tecnológica Estratégias de longo prazo, por exemplo, migração e emulação
Atividades específicas de acesso	O acesso aos objetos Acesso aos catálogos Suporte ao utilizador

Tabela 2 - Custos típicos de fontes

Tipo de Custo	Fontes de custo
Objeto digital / aquisição de dados	Preço de compra / Custo licenciamento
Trabalho	Pessoal vai incluir uma equipa dedicada, bem como proporções variáveis de alta gestão, supervisor, equipa de TI, etc.
Tecnologia	*Hardware* *Software* Nível dos requisitos (por exemplo, velocidade, disponibilidade e desempenho)
Custos operacionais não-laborais	Instalações e espaço (por exemplo, rendas e eletricidade) Materiais e Equipamentos Comunicações Seguros Custos legais

4. **Garantir que os registos digitais são, pelo menos:**
    a. Pesquisáveis e disponíveis para acesso de forma atempada;
    b. Interpretáveis (usabilidade, apresentação, representação, vista, criptografia);
    c. Recuperáveis, incluindo a metainformação apropriada;
    d. Protegidos contra a perda de direitos, tais como propriedade intelectual, confidencialidade e direitos de autor;
    e. Disponíveis para acesso por tanto tempo quanto necessário, pelas pessoas autorizadas a aceder ao registo;
    f. Monitorizados para a qualidade da prestação de acesso (disponibilidade, pontualidade, entrega, histórico).

5. **Cobrir todas as atividades** (desde o planeamento inicial, às atividades de preservação, monitoramento e revisões em curso)
    a. Definir âmbito e estrutura do Plano
        I. Incluir os processos e procedimentos que vão ser usados para a preservação, os quais devem assegurar a retenção das características essenciais da informação a preservar e características adicionais relativas aos processos de preservação, abarcando (Ver DMAG_Anexo_DSE_Plano_preservação_02):

            i. A determinação de que os documentos devem ser mantidos em formato digital;
            ii. A implementação de horários de disposição;
            iii. A identificação de formatos e plataformas de armazenamento (por exemplo, ótica, magnética) para os documentos digitais;
            iv. A gestão de requisitos de metainformação adicional para os documentos digitais;

v. A implementação de ações de preservação necessárias para garantir a confiabilidade e a autenticidade dos documentos digitais;
vi. Cumprimento dos requisitos legais e regulamentares, específicos para os documentos digitais em cada jurisdição;
vii. A identificação e gestão dos riscos associados à obsolescência tecnológica;
viii. A capacidade de demonstrar a autenticidade, confiabilidade e facilidade de uso de um documento digital;
ix. Revisões regulares e requisitos de auditoria

b. Que informação vai ser abrangida:
   I. Identificar tipos de informação digital produzida (Ver DMAG_Anexo_DSE_Plano_preservação_04).
   II. Tipos de sistema:
      1. Sistemas que criam, mantêm e gerem documentos digitais;
      2. Sistemas que criam, mantêm e gerem documentos digitais podem criar e capturar os registos e a metainformação (informações sobre registos), ou gerir metainformação, apenas enquanto os registos são mantidos noutro lugar.
      3. Exemplos de sistemas incluem:
         a. Sistema de Gestão de Documentos e Registos Eletrónicos
         b. Sistemas de *email*
         c. Sistemas financeiros
         d. Sistemas de pessoal
         e. Sistemas de workflow
         f. Sistemas de negócios essenciais, tais como sistemas de gestão de caso ou sistemas de correspondência ministeriais
   III. Avaliar risco de perda (Ver DMAG_Anexo_DSE_Plano_preservação_02);
   IV. Identificar período de retenção/conservação permanente;
   V. Determinar o período de vida do *software* e *hardware* da plataforma / suporte em que estão armazenados.
c. Definir a articulação com as políticas e estratégias gerais de gestão da informação (incluindo tabelas de retenção)
d. Quem é responsável pelo plano?
   I. Gestor Informação
   II. Gestor TI
   III. Outros atores que devem integrar a equipa de implementação (ao nível da conversão/migração), representantes de:
      1. Gestão organizacional (para aprovar o orçamento e recursos);
      2. Tecnologia da informação (TI) (para implementar os processos);
      3. Gestão de registos (para garantir que os registros permanecem autênticos);

4. Utilizadores (para garantir que os registos convertidos / migrados são acessíveis);
5. Auditores (para garantir que os processos são auditados uma vez concluídos).

e. Quais os requisitos técnicos a cumprir? Incluir aspetos relacionados com:
   I. Obsolescência da plataforma/suportes;
   II. Obsolescência do formato de ficheiro;
   III. Obsolescência de *software*;
   IV. Obsolescência de *hardware*.
f. Que metainformação criar?
g. Que período de retenção e requisitos de acesso considerar?
h. Que requisitos não técnicos considerar (ao nível da …)?
   I. Logística
   II. Gestão
   III. Monitorização
   IV. Autenticidade
i. Quais as situações mais críticas?
   I. Migração do sistema de TI para novas plataformas de *software*/*hardware*;
   II. A introdução de novos tipos de plataformas de armazenamento;
   III. A introdução de novos formatos de ficheiro de armazenamento.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Figura 1 - Relações entre os diversos elementos do contexto de Gestão no seio de uma instituição (DPC, p.85)

Estratégias de preservação					
Designação	**Descrição**	**Vantagens**	**Desvantagens**	**Requisitos**	**Estratégias Relacionadas**
Migração	Um meio de superar a obsolescência tecnológica através da transferência de recursos digitais de uma geração de hardware / software para a próxima. O objetivo da migração é preservar o conteúdo intelectual dos objetos digitais e para manter a capacidade de os clientes o poderem recuperar, exibir, e de outra maneira usá-los em face da tecnologia em constante mudança.	Procedimentos para uma fácil migração estão bem estabelecidos. É atualmente a estratégia preferida para a maioria dos arquivos digitais. Pode tornar-se mais simples, com os avanços da tecnologia e a diminuição da variedade de plataformas.	Custo - requer programa especial a ser escrito para migrações complexas. Pode consumir muito tempo e ser demasiado complexo. Propensos a perder algumas funcionalidades e aparência dos originais. Podem comprometer a integridade dos originais, a menos que estejam implementados procedimentos de controlo de qualidade rigorosos para garantir a autenticidade. Recursos digitais mais complexos podem ser migrados com perda significativa de funcionalidade. Precisa de ocorrer em intervalos regulares ao longo da vida do recurso.	Políticas e orientações escritas, incluindo a política de seleção para materiais a serem migrados. Procedimentos de controlo de qualidade. Documentação rigorosa do processo de migração. Metainformação de preservação e documentação. Migrar dados sempre que houver uma atualização do software ou uma nova aplicação de software seja instalada. Assegurar resultados de migração com pouca ou nenhuma perda de conteúdo ou contexto. Empregar procedimentos rigorosos controlo de qualidade que podem incluir testes do programa de migração com uma amostra de registos ou bit / byte ou comparações de checksum de dados migrados e originais. Reter cópias do recurso digital no seu formato original, de forma a prevenir eventuais perdas ou modificações da informação no momento da migração.	Armazenamento e manutenção. Compatibilidade com versões anteriores. Identificador Permanente. Procedimentos de validação. Conversão de formatos padrão.
Emulação	Um meio de superar a obsolescência tecnológica de hardware e software através do desenvolvimento de técnicas para imitar sistemas obsoletos nas futuras gerações de computadores.	Recria a funcionalidade e aparência do original. Evita custos repetidos associados à migração. Pode oferecer as melhores perspetivas para recursos digitais mais complexos.	Ainda está em fase de investigação e requer mais testes práticos Só pode ser capaz de emular parte da funcionalidade e aparência do original. É provável que seja muito caro, a menos que se tenha economias de escala. Os novos emuladores precisam de ser construídos para grandes mudanças de paradigma computacional. É possível que esses custos possam até mesmo ultrapassar as economias de custos de migração repetidas. Questões de direitos de autor de software precisam de ser abordadas, o que pode ser extremamente complexo. Deve haver uma documentação rigorosa de requisitos de hardware e software. Estes têm sido raramente documentados para este nível de detalhe no passado e exigiria esforços e recursos concertados.	Procedimentos de armazenamento e manutenção adequados Políticas e orientações gerais documentadas. Metainformação de preservação Documentação detalhada sobre as especificações de hardware e software.	Armazenamento e manutenção. Encapsulamento. Identificadores permanentes
Preservação da Tecnologia	Um meio de superar a obsolescência tecnológica, retendo o hardware e o software usado para aceder ao recurso digital. Note-se que a atual definição dessa estratégia envolve instituições individuais que necessitam de manter o hardware e o software para todos os materiais que eles criam e / ou adquiram.	Armazenamento retém a funcionalidade e aparência do original. Armazenamento atrasa o momento em que são necessárias outras estratégias de preservação. Armazenamento pode ser a estratégia intercalar mais prático para recursos digitais complexos.	Só pode ser utilizado como uma estratégia de curto e médio prazo. Não é viável a longo prazo O suporte técnico irá inevitavelmente desaparecer dentro de um prazo relativamente curto. Facilitar o acesso tornar-se-á cada vez mais problemático ao longo do tempo.	Políticas e diretrizes referentes ao acesso. Documentação de hardware e software mantidos. Metainformação necessária para manter o hardware e software	Armazenamento e manutenção. Conversão de formatos padrão. Compatibilidade com versões anteriores. A adesão a padrões.
Adesão a padrões	Aderir a padrões abertos estáveis e amplamente adotados na criação e arquivamento dos recursos digitais. Estes não estão vinculados a plataformas de hardware / software específico e, portanto, pode adiar a inacessibilidade de recurso digital, devido à obsolescência tecnológica.	Usando padrões abertos estáveis irá atrasar o momento em que são necessárias estratégias mais dispendiosas. A utilização de padrões estáveis irá reduzir a complexidade e, portanto, os custos, de estratégias de preservação a longo prazo. Pode simplificar a migração e obter economias de escala na migração de itens semelhantes. Pode beneficiar criadores, bem como a preservação a longo prazo. Ajuda a distribuir alguns dos esforços ao longo do ciclo de vida dos recursos.	Dependente dos criadores serem capazes e / ou dispostos a cumprir a conversão posterior pelo arquivamento. Padrões estáveis não estão disponíveis para alguns formatos. Mesmo quando existem normas estáveis, estas estão sujeitas a mudanças inevitáveis à medida que evoluem para novas versões. Extensões proprietárias são relativamente comuns, mas geralmente, não tão bem documentado como o próprio padrão.	Conhecimento de todas as normas pertinentes para todas as categorias de recursos digitais adquiridos pela instituição. Orientações escritas sobre as normas preferenciais e aceitáveis. Estratégias institucionais de divulgação, colaboração, padrões e melhores práticas. Verificação de Tecnologia em atividades de normalização.	A adesão a normas facilitará todas as outras estratégias de preservação digital.
Compatibilidade com versões anteriores	Ser capaz de manter a acessibilidade a um recurso digital seguinte, após atualização para um novo software e / ou sistemas operativos.	Adia por um período a necessidade de estratégias de preservação primárias. Está a ser oferecida por um número crescente de fornecedores.	Não é oferecido rotineiramente por todos os fornecedores. Só tem aplicação/valor de curto a médio prazo. Mesmo quando ela existe, não se pode esperar que dure indefinidamente. A sua contínua disponibilidade é dependente das forças de mercado que são notoriamente voláteis. Ela pode, portanto, deixar de estar disponível, com pouco ou nenhum aviso.		Armazenamento e manutenção.
Encapsulamento	Agrupando um recurso digital e tudo o que é necessário para manter o seu acesso. Pode incluir metainformação, visualizadores de software e arquivos discretos que formam o recurso digital.	Garante todas as informações de suporte necessárias para que o acesso seja mantido como uma entidade. Pode potencialmente superar algumas das principais desvantagens das estratégias alternativas. Fornece um meio útil de concentrar a atenção sobre os elementos que são necessários para o acesso.	Pode produzir arquivos muito grandes com duplicação em toda a coleção a menos que esses links sejam mantidos. Software encapsulado ainda está aberto à rápida obsolescência tecnológica.		Emulação
Identificadores Permanentes	Um meio de localização de um objeto digital, mesmo quando sua localização muda. Exemplos são Universal Resource Names (URN); Digital Object Identifiers (DOI)	Criticamente importante para ajudar a estabelecer a autenticidade de um recurso. Fornece acesso a um recurso mesmo que a sua localização mude. Ultrapassa os problemas provocados pela natureza impermanente de URL's. Permite a interoperabilidade entre coleções.	Não existe um sistema único aceite por todos. Os custos de criação ou utilização de um serviço de resolução. É dependente de manutenção contínua do sistema de identificador permanente.		Todas, com exceção da Conversão para formatos analógicos.
Conversão para o formato analógico estável	Convertendo determinados recursos digitais valiosas para um meio analógico estável como papel permanente ou preservação de microfilme ou, mais recentemente, o disco de níquel legíveis por microscópio eletrônico. Isso não pode ser recomendado como mais do que uma estratégia provisória pragmática para uma pequena categoria de materiais digitais, enquanto se aguarda o desenvolvimento de estratégias de preservação digital mais apropriadas.	Não é mais vulnerável à obsolescência tecnológica assumindo que são usados microfilme de qualidade ou papel permanente para preservação. Seria essencialmente um custo "único" para a conversão. Irá garantir a acessibilidade por centenas de anos, desde que seja convertido num padrão de arquivo e armazenada em condições de arquivamento. Pode ser uma estratégia pragmática interina enquanto se aguarda o desenvolvimento de infraestruturas para as estratégias de preservação digital mais apropriadas.	Perde funcionalidade do recurso digital original. Só pode sensatamente ser considerada como uma opção para os recursos digitais que não utilizam ou necessitam de todas as funcionalidades da tecnologia digital. Já causou dificuldades mesmo quando usado para emails de texto simples Não pode ser considerado para recursos digitais mais complexos, onde a perda de funcionalidade diminui, ou pé mesmo destruída, a utilidade e a integridade do recurso. Perde as vantagens da tecnologia digital, por exemplo, a conveniência de uso, e uso eficiente do espaço. Custos de conversão para padrão de arquivo e armazenamento em condições de arquivamento (o último custo será recorrente e o custo acumulado será significativo ao longo do tempo).	Políticas e diretrizes claramente documentadas para adoção de estratégia e categoria de recursos que podem ser utilizados.	Nenhuma, esta não é uma estratégia de preservação digital, mas um mecanismo para preservar o conteúdo de informação de determinados recursos digitais.
Arqueologia digital	Resgatar recursos digitais que se tornaram inacessíveis, como resultado de obsolescência tecnológica e / ou degradação do suporte. Não tanto uma estratégia em si como um substituto para um quando materiais digitais caíram fora de um programa de preservação sistemática.	Há um número crescente de serviços de entidades especializadas que oferecem este serviço. Tem sido demonstrado ser tecnicamente possível recuperar uma vasta gama de informações a partir de meios danificados ou obsoletos (embora não necessariamente da mesma forma).	Muito mais caro a longo prazo do que as estratégias de preservação digital convencionais. É pouco provável que seja rentável para algo diferente dos recursos digitais mais valorizados. Materiais potencialmente úteis que não justificam os custos envolvidos serão perdidos. Risco de alguns materiais digitais poderem não ser esgatados com sucesso. Má gestão de investimento inicial.		

Procedimentos para preparar documentos para armazenamento e preservação							
Numeração Única	**Marcação e rotulagem preferencial**	**Manuseando as matrizes**	**Validação**	**Reformatação de formatos de arquivo**	**Reformatação de suportes de armazenamento**	**Cópia**	**Segurança**
Cada recurso de dados acondicionado por uma instituição deve ser alocado um identificador exclusivo. Este número irá identificar o recurso no catálogo da instituição e ser usado para localizar ou identificar suporte físico e documentação. No caso de um recurso que está sendo descondicionado por qualquer motivo, este número único não deve ser realocado.	No mínimo todos os meios físicos e documentação em papel deverá ser marcada com o número único atribuído ao recurso, e qualquer informação adicional exigida pela instituição identificar facilmente os conteúdos e formatos	O manuseio de diretrizes para acondicionamento dos funcionários deve ser desenvolvida refletindo os conselhos de armazenamento e preservação para os funcionários sobre as melhores práticas para os diferentes suportes	Verificações de validação devem ser realizadas pela instituição na transferência do, suporte, conteúdo e a estrutura de recursos de dados depositados, e em qualquer documentação que o acompanha. Procedimentos de validação podem ser adaptados à luz do volume de material e recursos disponíveis na seção de aquisições. Pode ser possível automatizar alguns dos procedimentos de validação mas os outros só podem ser realizadas manualmente. Essas verificações podem incluir: • Verificação de vírus de computador. • Verificar se os suportes e os arquivos podem ser lidos. • Verificar a integridade e exatidão de papel com base ou documentação digital. • Verificar descrição e conteúdo intelectual do recurso. • Verificar estrutura e formatação do recurso. • Procedimentos para que documenta as verificações de validação e de quaisquer discrepâncias encontradas. • Procedimentos para verificação e, se possível, resolver as discrepâncias com o fornecedor.	Onde os formatos de arquivos usados para transferir os recursos não são adequados para a preservação a longo prazo, a Instituição pode voltar a formatar o recurso em seus formatos de arquivo preferenciais. Além de formatos de arquivo, as versões em outros formatos adequados para a entrega aos utilizadores também pode ser produzido a partir do original	Onde o suporte de armazenamento usado para transferir os recursos não são adequados para a preservação a longo prazo, a instituição pode voltar a formatar os recursos nos seus suportes preferidos.	Várias cópias de backup de um item podem ser geradas durante o acondicionamento como parte de armazenamento e da política de preservação das instituições e para permitir os procedimentos de recuperação de desastres.	Políticas e procedimentos do sistema e de segurança física devem estar no local para garantir o cuidado e a integridade dos itens durante o acondicionamento. Estes devem ser desenvolvidos a partir e refletir as políticas e procedimentos institucionais sobre segurança.

Checklist de Avaliação das digitalizações		
Checklist		**Problemas em preservar substitutos digitais**
1	Avaliação da necessidade de digitalização	O material já foi digitalizado? Se assim for, é para um padrão adequado e de fácil acesso?
2	Encontrar fundos para o projeto	Quais as políticas de arquivamento que existem, ambas, da organização financiadora (se financiado externamente) e da instituição com a responsabilidade primordial para o projeto?
3	Planeamento do projeto e atribuição de recursos	Necessidade de reservar fundos recorrentes para a manutenção das cópias digitais bem como fundos para a conversão. Assegurar que todas as partes interessadas estão cientes do projeto (por exemplo, se uma outra parte da organização ou uma organização externa é esperada para manter o recurso, eles terão de ser incluídos nas discussões neste momento, se não antes)
4	Seleção de materiais	Direitos de autor. Necessidade de assegurar que a permissão é dada tanto para digitalizar o original e para fazer cópias da cópia digital para efeitos de preservação. Condição e integridade dos originais. É capaz de ser verificado novamente em uma data posterior se a cópia digital é perdida?
5	Decidir como o conteúdo da informação precisa de ser organizado (por exemplo, bases de dados de texto pesquisáveis e / ou imagens das páginas de documentos)	Seleção de formatos de arquivos apropriados e suportes de armazenamento para ambas as cópias, principal/arquivo e derivados.
6	Decidir o método de digitalização apropriado para originais analógicos e objetivos do projeto	Detalhes do método de digitalização precisam de ser documentados e anexados ao registo de metainformação para permitir a gestão futura.
7	Preparar originais para a digitalização	Documentação.Serão os originais mantidos? A questão principal, então, será ou não se o original é muito frágil para ser verificado novamente numa data posterior se a cópia digital for perdida. Em qualquer caso, se a cópia digital se tornar o principal meio de acesso, ela estará sujeita aos mesmos requisitos que o material nascido em meio digital
8	Conversão	Documentação das características técnicas. Algoritmo de compressão (se for usado); profundidade de bits necessários; resolução da digitalização etc. Criar cópias de backup, logo que a conversão é realizada.
9	Controlos de garantia da qualidade	Substituto Digital precisa ser de uma qualidade aceitável de preservação. Se utilizar serviços de terceiros, precisa de se certificar que a documentação clarifica responsabilidade pela garantia de qualidade.
10	Indexação e catalogação final	Metainformação para a descoberta de recursos e para a gestão e preservação da cópia digital.
11	Carregamento de dados em sistemas computacionais	Requisitos de armazenamento de documentos para acesso e preservação cópias (se diferente). Fazer cópias de backup, conforme apropriado.
12	Implementar estratégias de arquivamento e preservação ou transferir para uma organização de preservação	Normas requeridas para formatos, suportes de armazenamento, documentação e procedimentos de transferência. Armazenamento de cópias mestres e de backup. Estratégias para atualização de suportes e mudanças no ambiente tecnológico.

Variedade de registos digitais que podem ser gerados por diferentes organizações diariamente			
Documentos criados usando aplicações Office	**Registos em ambientes on-line e baseados na web**	**Registos gerados pelos sistemas de informação de negócios**	**Sistemas de comunicação digitais**
Documentos de processamento de texto	Intranets	Bases de dados	Email
Folhas de cálculo	Extranets	Sistemas de dados geoespaciais	SMS (serviço de mensagens curtas)
Apresentações	Sites públicos	Sistemas de recursos humanos	MMS (serviço de mensagens multimédia)
Documentos publicados no desktop	Registos de transacções online	Sistemas financeiros	EDI (intercâmbio electrónico de dados)
		Sistemas de workflow	Intercâmbio electrónico de documentos (fax eletrónico)
		Sistemas de gestão de cliente	Correio de voz
		Sistemas de gestão de relacionamento com clientes	Mensagens instantâneas
		Sistemas desenvolvidos internamente	Comunicações multimédia (por exemplo, videoconferência e teleconferência)
		Sistemas de gestão de conteúdo	

Documento de Suporte à Especificação: Ata de Reunião

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma Ata de reunião, para a elaboração do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e

Documento de Suporte à Especificação: Ata de Reunião

respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

ATA DE REUNIÃO

Assunto:		**Data:**	
		Local:	
Unidade(s) Orgânica(s):			
Ordem de Trabalhos:			
Presentes:			

Próxima reunião	**Local:**	**Data/ hora:**	

Documento de Suporte à Especificação: Ata de Reunião

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Plano de Contingência

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Plano de contingência, para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Plano de Contingência

Propósito

Esta orientação interina fornece instruções para ações que serão tomadas no caso de o Governo não providenciar as dotações regulares ou uma resolução contínua, resultando numa interrupção do financiamento para as funções apropriadas do arquivo.

Resumo das atividades NARA em caso de lapso de verbas:

a) No caso de um lapso de dotações, a instituição deverá suspender imediatamente todas as atividades apropriadas. Salvo conforme autorizado por este plano de contingência, nenhuma atividade que requeira a intervenção ou a presença no local de um Governo ou o contratante empregado ou de outra forma requer a obrigação de dotações anuais serão permitidas;

b) Todas as instalações de arquivo devem ser fechadas, nomeadamente aos funcionários, público em geral e ocupantes não-federais e será assegurado para a duração de um lapso de financiamento.

c) A maioria dos funcionários deve ser dispensada temporariamente. Exceto para os funcionários identificados como "exceção" no âmbito deste plano de contingência e funcionários pagos a partir de fontes diferentes de uma dotação anual;

d) Alguns empregados podem ser chamados ao serviço em casos de emergência. Em caso de uma emergência que ocorre durante um lapso de dotações anuais, os funcionários que foram inicialmente designados como "não-isentos" podem ser temporariamente chamados da licença para executar funções de emergência.

e) A maioria dos contratos deve ser suspensa. Contratos isentos (como contratos de serviços públicos e de serviços de telecomunicações) vão manter o nível "mínimo" de contrato de serviço necessário para proteger a vida e a propriedade.

f) Listagens de emergência serão mantidas vigentes. As organizações deverão rever periodicamente estas listas de emergência, para garantir que as mesmas são atuais.

Documento de Suporte à Especificação: Plano de Contingência

É de seguida apresentado, um quadro geral para responder a um lapso temporário de dotações. Apesar de "temporário" é definido como 30 dias consecutivos ou menos para ações adversas de funcionários, nesta parte, significa apenas o período relativamente curto, muitas vezes apenas alguns dias ou menos, normalmente exigidos para o Congresso fornecer fundos. Se um lapso for alargado ou uma atividade for finalizada, serão emitidas instruções adicionais.

a) *A menos que sejam notificados no sentido contrário, todos os funcionários devem comparecer ao trabalho no primeiro dia útil de um lapso temporário. Uma vez que todos os funcionários são dispensados do serviço, exceto aqueles necessários para funções excecionais.*
b) *Os funcionários que realizam atividades excecionais devem-se apresentar ao serviço, conforme indicado durante todo o período temporário. Durante um lapso de dotações, os funcionários considerados excecionais ainda estão num estatuto de remunerados, embora as suas remunerações sejam adiadas, isto é, eles não estão a prestar serviços gratuitos, devendo, por isso, comparecer ao trabalho.*
c) *No primeiro dia útil após o lapso de dotações, os funcionários considerados não-excecionais serão avisados de dispensa temporária, instruções adicionais e serão dispensados do serviço, o mais tardar às 12:00h desse dia.*
d) *Pessoas em viagem oficial, aquando do lapso de fundos, serão tratadas caso a caso. Os viajantes que desempenhem funções de exceção, ou apoiados por fundos não afetados pelo lapso, permanecem em serviço. Os viajantes com funções não-excecionais são colocados em licença temporária.*
e) *Todas as instalações de arquivo e de bibliotecas serão fechados e seguros durante o período do lapso de financiamento.*
f) *O website público permanecerá online, mas deverá conter uma faixa que indica que o Arquivo Nacional se encontra fechado. O site pode ser atualizado para indicar que os eventos foram cancelados, de acordo com a duração do encerramento.*
g) *Bens e serviços não podem ser adquiridos durante um lapso de dotações, exceto quando necessário para apoiar certas atividades ou quando adquiridos com os fundos que estão isentos de um lapso de dotações.*

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador

Documento de Suporte à Especificação: Plano de Contingência

RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Acordo de custódia

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Acordo de custódia, para a elaboração do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

PROPOSTA DE ACEITAÇÃO DE DOAÇÃO – MINUTA

F. propôs por escrito a doação, a favor da Câmara Municipal do Porto e para custódia do Departamento Municipal de Cultura, de ....[1].

A doação ficará condicionada, conforme acordado com o proponente doador, ao cumprimento dos seguintes requisitos por parte do mesmo:

-
-

A doação em causa ficará ainda condicionada, conforme acordado com o proponente doador, ao cumprimento dos seguintes requisitos por parte do Município:

-
-

Considerando[2]:

-
-
-

Propõe-se a aceitação da doação, nas condições aqui expressas.

[1] Identificação do documento ou conjunto documental.
[2] Justificação(ões) proposta(s) para a aceitação do depósito.

Documento de Suporte à Especificação: Acordo de custódia

Porto, ...[3]

.....[4]

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

[3] Data.
[4] Assinatura e cargo do proponente a reunião de Câmara.

Documento de Suporte à Especificação: Política de Preservação

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma Política de preservação da informação em meio digital, para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

R - Responsável; E - Envolvido

4. DESCRIÇÃO

Política de Preservação

Para haver de facto um documento sobre a Política de Preservação, foram identificados vários campos aplicáveis que servem de base para uma correta e eficaz constituição de um documento desta importância, a saber:

Declaração de Visão / Declaração da Política

Serve para demonstrar o alcance da Política de Preservação.

Fundamentação

A forma como se irá preservar e gerir os objetos digitais.

Âmbito

Qual a área de atuação da política, ou seja, aquilo que a política cobre.

Objetivos

Finalidades da Política de Preservação Digital

Formatos de ficheiros de dados / Formatos de preservação

Especificação dos formatos de preservação dos ficheiros.

Características dos objetos digitais

Enumeração dos atributos e propriedades dos objetos digitais

Abordagem à Preservação Digital

A abordagem efetuada relativamente aos objetos digitais, como os processos utilizados (migração, normalização, etc.).

Documento de Suporte à Especificação: Política de Preservação

Armazenamento digital

Definição do sistema tecnológico que irá permitir a preservação dos objetos digitais.

Responsabilidades

Indica as responsabilidades e funções dos elementos da equipa, de forma a responder aos requisitos presentes na ISO 16363:2012.

Normas, Orientação e Organizações

Indicação dos padrões, normas e referenciais que servem de base à política de preservação.

Cooperação/ colaboração

Comprometimento com outros organismos na promoção de ferramentas de preservação digital; estabelecimento de parcerias.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Estratégia de Preservação

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para uma definição de uma Estratégia de preservação da informação, para a elaboração do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade	Função	DM	DD	CD	SEC	QC
Receção / identificação de documento					R	
Registo de um novo documento					R	R
Encaminhamento				R	E	R
Receção por parte do Gestor						R
Encerramento		R	R	R	E	

R - Responsável; E - Envolvido

4. DESCRIÇÃO

COMO DEFINIR UMA ESTRATÉGIA DE PRESERVAÇÃO A LONGO TERMO

ISO/TR 18492:2005 - Long-term preservation of electronic document-based information.	ISO 16363:2012 – Space data and information transfer systems – Audit and certification of trustworthy digital repositories.	ISO/IEC 27001:2005 - Information technology. Security techniques. Information security management systems. Requirements.
Esta Norma, fornece orientação metodológica e prática para a preservação a longo prazo e recuperação de informação autêntica baseada em documentos eletrónicos, quando o período de retenção excede a expectativa de vida da tecnologia (hardware e software) utilizado para criar e manter a informação. Esta leva em conta o papel da tecnologia de padrões de tecnologia de informação neutro no apoio ao acesso de longo prazo. Esta orientação também reconhece que garantir a preservação a longo prazo e recuperação de informação autêntica baseada em documentos eletrónicos deve envolver especialistas de TI, gestores de documentos, de registos e arquivistas. Não abrange os processos	Esta Norma define uma prática recomendada para avaliar a confiabilidade dos repositórios digitais. É aplicável a uma vasta série de repositórios digitais. Pode ser utilizada como uma base para a certificação.	Esta Norma abrange todo o tipo de organizações (empresas comerciais, por exemplo, agências governamentais, organizações sem fins lucrativos). Esta Norma especifica os requisitos para estabelecer, implementar, operar, monitorar, rever, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. É responsável pela especificação requisitos para a implementação de controlos de segurança personalizados para as necessidades de cada organização ou suas partes. O SGSI é projetado para assegurar a seleção de controlos de segurança adequados e proporcionais que protegem os ativos de informação e dar confiança

para a criação, captura e classificação de informação autêntica baseada em documentos eletrónicos. Este Relatório Técnico aplica-se a todas as formas de informações criadas pelos sistemas de informação e guardadas como prova de transações e atividades empresariais.		às partes interessadas.

Objetivos (6):
- Informação legível baseada em documentos eletrónicos
- Informação inteligível baseada em documentos eletrónicos
- Informações identificáveis baseada em documentos eletrónicos
- Informação recuperável baseada em documentos
- Informação compreensível baseada em documentos
- Informação autêntica baseada em documentos eletrónicos

Elementos na estratégia:
- Renovação da plataforma
- Metainformação
- Migração da informação baseada em documentos eletrónicos
    - Dependência de *software*
    - Atualizações de *software* e instalação de novo *software*
    - A migração para formatos padrão
    - Migração do legado do sistema de informação da informação baseada em documentos eletrónicos.
        - Etapas de migração
            - Analisar legado do sistema de informação (Parte 1)
            - Decompor o legado da estrutura do sistema de informação (Parte 2)
            - Projetar as interfaces alvo (Parte 3)
            - Projetar os aplicativos de destino (Parte 4)
            - Projetar as bases de dados de destino (Parte 5)
            - Instalar e testar totalmente o ambiente de destino (Parte 6)
            - Criar e instalar os *gateways* necessários (parte 7)
            - Migrar o legado das bases de dados (Parte 8)
            - Migrar o legado das aplicações (Parte 9)
            - Migrar o legado das interfaces (Parte 10)

O desenvolvimento de uma estratégia de preservação a longo prazo
- A política de preservação a longo prazo (indicar elementos a considerar):
- Uma seção afirmando que o fornecimento de preservação a longo prazo da informação baseada em documento, autêntica e processável, é um objetivo do repositório de armazenamento e a identificação de outros objetivos e responsabilidades do repositório;
- Uma descrição do tipo de guarda que o repositório de armazenamento compromete a informação baseada em documento eletrónico, por exemplo, jurídica ou física;

- Uma descrição das melhores práticas de gestão da informação baseada em documentos eletrónicos para quais o repositório de armazenamento adere;
- Identificação das circunstâncias sob quais as atividades de migração serão realizadas e os métodos e fundamentos de tais atividades;
- Uma explicação dos tipos de auditoria de conformidade, que terá lugar;
- Clarificação dos papéis do pessoal do repositório de armazenamento e uma descrição de quaisquer responsabilidades que são terceirizados.

- Controlo de qualidade

Informação baseada em documentos eletrónicos preservados em conformidade com as normas e procedimentos estabelecidos, é considerada, geralmente, como tendo melhor autenticidade e, finalmente, melhor credibilidade em processos judiciais.

Portanto, repositórios confiáveis de terceiros devem implementar políticas e "melhores práticas" para cada uma das suas atividades.

Evidências sobre como a informação baseada em documentos eletrónicos foi gerida podem ser extremamente importantes num processo judicial e, portanto, deve ser mantida com o mesmo cuidado e preocupação. Esta evidência deve incluir todas as políticas relevantes e procedimentos, documentação de qualquer perda de dados durante a migração, e os resultados das auditorias de controlo de qualidade periodicamente que foram realizadas para assegurar a conformidade com as políticas e procedimentos.

- Segurança

Procedimentos de segurança rigorosos irão:

a) Assegurar a conformidade com os requisitos legais e regulamentares;
b) Proteger os recursos digitais de alterações inadvertidas ou deliberadas;
c) Fornecer um registo de auditoria para satisfazer as exigências de prestação de contas;
d) Agir como um impedimento para potenciais falhas de segurança interna;
e) Proteger a autenticidade dos recursos digitais;
f) Proteger contra roubo ou perda.

Os requisitos de segurança envolvem:

- Estabelecer plano de recuperação de desastres
- Controlar o acesso às instalações de armazenamento e áreas de processamento. Armazenar em área preferencialmente bloqueável separada.
- Assegurar que não há acesso não autorizado.
- Características de projeto de auditoria em sistemas de armazenamento em massa e controlos computadorizados de acesso físico. Realizar verificações aleatórias regulares se as auditorias automatizadas não forem viáveis.
- Estabelecer procedimentos para garantir que não haja mudanças deliberadas ou inadvertidas
- Assegurar que todos os requisitos legais estão reunidos.
- Estabelecer procedimentos para garantir a autenticidade.

- Usar senhas (*passwords*) e Identificadores (*ID's*) de utilizador e outros procedimentos de segurança de rede.
- Definir privilégios de sistema e acesso à área para o pessoal.
- Atribuir responsabilidades específicas ao pessoal para instalações de segurança e armazenamento de dados.

Repositórios de armazenamento devem desenvolver procedimentos de segurança por escrito que descrevam:

- Medidas de segurança utilizadas durante a transferência de informação com base em documentos eletrónicos para o repositório de armazenamento;
- Procedimentos de controlo de acesso e monitorização desses procedimentos;
- O posicionamento do local de armazenamento para que o perigo de perda devido a desastres naturais seja minimizada;
- Um plano para a recuperação de desastres;
- Aderência aos padrões reconhecidos relativa ao manuseamento dos suportes de armazenamento;
- Provisão para uma instalação de armazenamento secundário para cópias de segurança dos suportes de armazenamento e procedimentos de recuperação de desastres.

- Controlo de acesso de aplicação / *software*

Os repositórios de armazenamento devem utilizar os seguintes procedimentos automatizados para controlar a modificação e / ou eliminação da informação com base eletrónica.

Qualquer informação baseada em documentos eletrónicos que é modificado / eliminado deve ser automaticamente registado pelo aplicativo / *software*, juntamente com o nome da pessoa e o motivo para a modificação / eliminação.

Ao contrário do espaço de armazenamento para as coleções físicas, o armazenamento em computador significa a redução no custo e aumento da capacidade de todo o tempo. Os recursos digitais podem ser gerados de uma forma relativamente fácil, e as perspetivas de espaço de armazenamento podem se tornar confusos com várias versões de documentos e outros recursos digitais podem ter valores bastante elevados.

Estas decisões terão de ser bem documentadas e compreendidas por todas as partes interessadas dentro da instituição.

- Políticas para a manutenção de documentos no servidor ficheiros central
- Estratégias para migrar para um servidor de ficheiros maior antes da sua capacidade total ser atingido.
- Políticas para identificar quais os recursos digitais que devem ser armazenadas *online*.
- As políticas de retenção para determinar em que fase (ou nunca) de armazenamento *online* de recursos digitais serão reavaliados.

- Controlo de acesso físico

Repositórios de armazenamento devem utilizar as seguintes medidas, a fim de controlar o acesso físico aos sistemas de informação baseados em documentos eletrónicos:

- Apenas ao pessoal autorizado deve ser permitido o acesso ao local de armazenamento;
- Um sinal no log in/out deve ser mantida a data, hora e identidade de cada pessoa que entra no local seguro de armazenamento;
- Um registo deve ser gerado quando o pessoal autorizado remover o suporte de armazenamento. O registo deve incluir a data e a hora e ainda uma breve declaração explicando o motivo da sua remoção;
- Quadros superiores com responsabilidade de supervisão devem analisar os registos periodicamente para verificar o cumprimento do pessoal, e o próprio log in/out deve ser mantido como prova do cumprimento do repositório com as suas próprias políticas.

- Proteção contra perda

Repositórios de armazenamento devem utilizar as seguintes medidas a fim de proteger a informação baseada em documentos eletrónicos de perda:

- O local de armazenagem deve ser localizado onde a ameaça de desastre natural, por exemplo, inundação, incêndio, terremoto ou meteoro é mínima;
- O local de armazenagem deve incluir sistemas de supressão e deteção de incêndio;
- Um plano de recuperação de desastres em larga escala deve estar no local, que inclui a categorização de informações com base em documento eletrónicos para que o resgate e a recuperação de plataformas de armazenamento possam ser priorizados.
- Um repositório de armazenamento usando suportes magnéticos deverá localizar o seu local de armazenagem longe de motores blindados pesados elétricos por exemplo, sistemas de ar condicionado, geradores, transformadores e linhas de energia elétrica que transportem cargas elevadas.

O desenvolvimento e o uso de um plano de recuperação de desastres com base em princípios sólidos, endossado pela alta administração, e capaz de ser ativado por pessoal treinado irá reduzir muito a gravidade do impacto de possíveis desastres e incidentes.

- Desenvolver plano contra desastres para funcionar em caso de catástrofes naturais ou provocadas pelo homem.
- Garantir que todos os funcionários relevantes são treinados em procedimentos de desastres
- Criar cópias de arquivos de recursos de dados, no momento da sua transferência para a instituição.
- Armazenar cópias de arquivo em fita digital padrão ou em outros suportes contemporâneos aprovados.
- Armazenar cópias de arquivo dentro e fora do local, isto é, as cópias fora do local devem ser armazenadas a uma distância segura das cópias no local para garantir que estas não são afetadas por qualquer desastre natural ou causado pelo homem que possam danificar as cópias no local.

- Controlo e monitorização ambientais

A relativa fragilidade dos suportes de armazenamento eletrónico coloca a sua longevidade e a capacidade de leitura em risco. Como tal, repositórios de armazenamento devem implementar um programa de controlo e de monitoramento ambiental. Tal programa deve usar as seguintes medidas:

- Fornecer um ambiente de armazenamento onde a temperatura e a humidade relativa são controladas dentro de um intervalo adequado, conforme especificado por normas e/ou estudos de autoridade estabelecidos;
- Fornecer um sistema de filtragem de ar concebido para remover partículas de poeira do ar e gases poluentes a partir do ambiente de armazenamento;
- Proibição do consumo de alimentos e bebidas e fumar no ambiente de armazenamento;
- Implementação de um programa para ler anualmente uma amostra estatística da informação com base em documentos eletrónicos para identificar a perda atual ou iminente de informações.

As condições ambientais adequadas irão aumentar a longevidade dos meios de armazenamento digital e ajudar a evitar danos acidentais para um recurso de dados ou a sua documentação (DCP, p. 108).

Device	Operating	Non-Operating	Long term storage
Magnetic tape cassettes 12.7mm	18 to 24°C 45 to 55% RH	5 to 32°C 5 to 80% RH	18 to 22°C 35 to 45% RH
Magnetic tape cartridges	10 to 45°C 20 to 80% RH	5 to 45°C 20 to 80% RH	18 to 22°C 35 to 45% RH
Magnetic tape 4 & 8mm helical scan	5 to 45°C 20 to 80% RH	5 to 45°C 20 to 80% RH	5 to 32°C 20 to 60% RH
CD-ROM	10 to 50°C 10 to 80% RH	-10 to 50°C 5 to 90% RH	18 to 22°C 35 to 45% RH

Figura 1 - Condições ambientais para o armazenamento da plataforma de dados

Desta forma, são especificados alguns requisitos necessários para que exista um controlo de ambiente eficaz e eficiente por parte da organização, a saber:

- Estabelecer orientações e procedimentos para aclimatizar fita magnética caso estejam em movimento entre variações significativas de temperatura (por exemplo, as fitas que se deslocam de condições externas muito frias não devem ser utilizadas antes de serem ambientadas a condições internas mais quentes);
- Estabelecer procedimentos para a monitorização das condições ambientais;

- Minimizar os riscos de danos causados por poeira e outros poluentes atmosféricos;
- Proibir fumar e comer na área de armazenamento;
- Armazenar o mais afastado possível da luz solar direta;
- Fornecer proteção adicional na forma de invólucros para suportes;
- Fornecer instalações de armazenamento que minimizam a ameaça de desastres naturais, como incêndios, inundações ou para meios de armazenamento magnético de campos magnéticos;
- Assegurar que qualquer material de acompanhamentos não digitais (por exemplo, livros de códigos, instruções operacionais) também é armazenado em condições ambientais adequadas.

- Suporte

Em baixo são apresentadas algumas recomendações, de acordo com a DPC a nível de suportes de armazenamento:

- Mantenha o acesso às áreas livres de fumo, poeira, lixo e outros contaminantes.
- Guarde os suportes magnéticos longe de campos magnéticos fortes.
- Transporte meios magnéticos em gabinetes com folgas espaço de 50 mm.
- Armazene num ambiente fresco, seco, estável e seguro (consulte Armazenamento e Preservação).
- Aclimatizar o suporte antes da sua utilização.
- Usar suportes e dispositivos de alta qualidade.
- Mantenha os dispositivos de acesso bem conservado e limpo.
- Não coloque etiquetas em discos e / ou marca de ótica usando uma caneta ou lápis.
- Seguir as recomendações dos fabricantes.
- Minimizar o manuseio e o uso dos suportes de arquivamento e / ou número recorde de acessos / usar e implementar refrescante apropriado.
- Escrever cópias de arquivo a partir de diferentes dispositivos e *software*.
- Faça cópias de arquivo para suportes de armazenamento comparáveis adquiridos de diferentes fornecedores.

- Formatos de ficheiro

- Utilizar formatos "abertos" não-proprietários, formatos de arquivos bem documentados, sempre que possível.
- Em alternativa utilizar os formatos de ficheiro que são bem desenvolvidos, têm sido amplamente adotado e são normas de facto no mercado.
- Identificar os formatos aceitáveis para efeitos de transferência, armazenamento e distribuição de utilizadores (estes podem ser distintos).
- Minimizar o número de formatos de ficheiro a ser gerido, tanto quanto for possível / desejável.
- Não utilizar criptografia ou compressão para ficheiros de arquivos, se possível.

- Monitorização da Tecnologia

- Realizar um levantamento retrospetivo de participações digitais, uma avaliação de risco e plano de ação.
- Implementar um processo de vigilância tecnológica e / ou implementar procedimentos para a padronização e as mudanças na tecnologia na sua estratégia de SI.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

29-07-2014

MATRIZ DE COMPETÊNCIAS / LEVANTAMENTO DE NECESSIDADES FORMATIVAS

UO - Nuclear

Matriz de Competências & Funções

Matriz de Competências & Funções

Estrutura	Nuclear
Serviço	Estrutura Nuclear -
Atribuições	

Trabalhador / Competências Técnicas e Profissionais

N.º Mecanográfico																	
Postos de trabalho (cargos/carreiras/categorias)																	
Atribuições	Origem (SIADAP ou outras)	Competências														Média Competencial na UO	Iniciativas Formativas
Média Competencial do Trabalhador																	

Legenda:

Nível de Competências	Valor
Excelente (Domínio absoluto / Autonomia prática de aplicação / Supervisão de terceiros)	5
Relevante (Domínio alargado / Autonomia e prática de aplicação)	4
Adequado (Domínio mínimo necessário para o desempenho autónomo de funções)	3
Inadequado (Domínio elementar / Desempenho de funções apenas com supervisão)	2
Totalmente Inadequado (Domínio inexistente / incapacidade para o desempenho de funções)	1
Não Aplicável (ainda não desempenha funções)	0

Prioridades de desenvolvimento

Importante desenvolver a curto prazo (1 ano)

Importante desenvolver a médio prazo (2/3 anos)

Nota: Em casos de dúvida no processo de selecção de formandos, será dada prioridade aos que possuirem um maior défice de competências (média das competências).

Instrução de aplicação

1º - Classificar competências (q.v. escala 0 a 5)

2º - Identificar prioridades (q.v. código cores)

Documento de Suporte à Especificação: Plano de Formação

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Plano de Formação, para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de

Documento de Suporte à Especificação: Plano de Formação

Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Plano de Formação CMP 2012/2013

Dando continuidade ao Projeto Formativo Institucional, a DMRH vem divulgar o Ciclo de 2013 do Plano de Formação CMP referente ao biénio 2012/2013, constituído por um conjunto de iniciativas formativas diretamente resultantes da participação das diferentes UO no processo de Diagnóstico de Necessidades Formativas, através do instrumento estratégico Matriz de Competências & Funções.

A aposta formativa prevista para 2013 reparte-se por um conjunto de 44 cursos (que se estendem por um total de 74 edições), a desenvolver entre maio e dezembro, associados a diferentes áreas de formação e com forte ligação aos diversos eixos de priorização estratégica definidos no âmbito das vertentes de capacitação: jurídica, técnica específica, uso de ferramentas informáticas, articulação com o cliente, desenvolvimento de uma linha de conduta ética e organizacional (transversal) - vd. Referencial de Formação.

Destaca-se, ainda, a aposta da DMRH em modalidades inovadoras de formação contínua (designadamente, as assentes em bLearning e eLearning), materializada na inclusão, neste ciclo formativo, de 9 cursos (20,5% do total de cursos previstos) a realizar nas modalidades de ensino / aprendizagem referidas.

O Ciclo de 2013, que envolverá participações de trabalhadores afetos à totalidade das UO, conta com iniciativas associadas às seguintes Áreas de Educação e Formação:

- *Língua e Literatura Materna*
- *Ciências Sociais e do Comportamento*
- *Biblioteconomia, Arquivo e Documentação (BAD)*
- *Comércio*
- *Enquadramento na Organização / Empresa*
- *Direito*

- *Informática na ótica do Utilizador*
- *Eletricidade e Energia*
- *Arquitetura e Urbanismo*
- *Floricultura e Jardinagem*
- *Turismo e Lazer*
- *Proteção de Pessoas e Bens*
- *Segurança e Higiene no Trabalho*
- *Desenvolvimento Pessoal*

***Inscrição**:*

- *Os processos de seleção e inscrição de formandos nos cursos ora divulgados serão assegurados pela DMRH e resultam das priorizações definidas por cada uma das UO em sede da respetiva Matriz de Competências & Funções.*

Direção Municipal de Recursos Humanos
Departamento Municipal de Recursos Humanos
Divisão Municipal de Formação e Avaliação do Desempenho

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Formação Externa

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma evidência de Formação externa (ficha de inscrição), para a elaboração do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e

respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

FICHA DE INSCRIÇÃO - FORMAÇÃO EXTERNA

I – Identificação da Ação de Formação

Designação do Curso _____

Entidade Formadora _____

Local _____

Data _____

Horário _____

Custos (se aplicável) _____

II – Identificação do Participante

Nome _____ **N.º Mec.** _____

Habilitações Literárias _____ **Categoria Profissional** _____

Data _____ **Assinatura do Interessado** _____

III – Identificação do Serviço

Direção **Departamento** **Divisão/Unidade**

Documento de Suporte à Especificação: Formação Externa

Telefone/Extensão	E-mail

IV – Fundamentação

Razões funcionais e/ou de pertinência para o serviço em causa que estão associadas à potencial participação em Formação Externa.	
Validação - Chefe de Divisão	**Validação - Diretor de Departamento**
Data:	**Data:**
Validação - Diretor Municipal (obrigatória)	**Validação - Membro do Executivo Responsável *(obrigatória)***
Data:	**Data:**

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria

Documento de Suporte à Especificação: **Formação Externa**	
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Registo de Eliminação

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de 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 Câmara Municipal do Porto.

2. ÂMBITO

Documento de Suporte à Especificação: Registo de Eliminação

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Auto de Eliminação de Documentos

DIVISÃO MUNICIPAL DE _____

AUTO DE ELIMINAÇÃO N.º_____

Aos _____ dias do mês de _____ de _____ , no Arquivo Geral da Câmara Municipal do Porto, na presença dos abaixo assinados, procedeu-se à inutilização por trituração, de acordo com os artigos 6º e 7º da Portaria n.º 412/2001, de 17 de Abril e disposições da tabela de seleção, anexo nº 1, alterada pela Portaria n.º 1253/2009, de 14 de Outubro, dos documentos a seguir identificados:

Serviço Produtor: _____

N.º ordem	N.ºRef. tabela *	Título da Série ou Sub-série	N.º / Tipo unidades de instalação	Forma de Suporte	Datas Extremas	N.º Guia Entrega	Metra-gem	Local

Documento de Suporte à Especificação: Registo de Eliminação

TOTAL m.l.:

Responsável pelo Serviço Produtor

_____

Responsável pela DMAG

_____

Representante da Autarquia Local

_____

*** - H: referência homóloga de acordo com o n.º 4 do Artigo 2,º da Portaria 412/2001.**

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Procedimento de Trabalho

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Procedimento de trabalho, para o Plano de Preservação da Informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e

respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

PROCEDIMENTO DE TRABALHO

1. OBJETIVO

2. ÂMBITO

3. MODO DE PROCEDER - FLUXOGRAMA (OPCIONAL)

4. DESCRIÇÃO

Nº ou Fase	Descrição	Responsável	Documentos
1.		↙	↙
		↙	↙
		↙	↙

5. PLANO DE CONTROLO - MONITORIZAÇÃO DA EXECUÇÃO DO SERVIÇO (OPCIONAL)

Nº ou Fase	Descrição	Método	Frequência	Responsável	Registo
1.	↙			↙	↙
	↙			↙	↙
	↙			↙	↙

Documento de Suporte à Especificação: Procedimento de Trabalho

SIGLAS E DEFINIÇÕES	
Sigla	**DESCRIÇÃO**

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Instrução de Trabalho

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma Instrução de trabalho para o Plano de preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de

Documento de Suporte à Especificação: Instrução de Trabalho

Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

INSTRUÇÃO DE TRABALHO

1. OBJETIVO

2. ÂMBITO

3. MODO DE PROCEDER - FLUXOGRAMA (OPCIONAL)

4. DESCRIÇÃO

Nº ou Fase	Descrição	Responsável	Documentos
1.		↙	↙
		↙	↙
		↙	↙

SIGLAS E DEFINIÇÕES

Sigla	DESCRIÇÃO

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Política de *Backups*

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma Política de *Backups* para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Política de *Backups*

Esta Política define o conjunto de procedimentos a levar a cabo para se salvaguardar os Sistemas de Informação da CMP através da realização de *backups*.

Diariamente é realizada uma verificação dos eventos gerados pela aplicação de *backups* e aos e-mails que a aplicação de *backups* gera em caso de falhas. Ocorrendo falhas, são analisadas as causas e realizados *backups* adicionais, se tal for possível.

Caso o problema com a realização de *backup* não seja resolvido, é informada a Chefia da DMTC para que se definam ações que permitam resolver o problema. O processo é encerrado quando o problema é resolvido.

São também definidas as regras de *backups*, explicitando os casos em que estes garantem a segurança dos sistemas, assim como, a proteção antivírus que se encontra instalada em todos os computadores, sendo o programa atualizado remotamente de forma automática.

Desta forma, os *backups* garantem a segurança nos seguintes casos:

i. Informação existente nos servidores.

ii. Informação produzida pelo colaborador e guardada nas seguintes localizações:
   - ➥ Área pessoal de cada utilizador criada em servidor (diretoria h:).
   - ➥ Área de Serviço, pasta partilhada em servidor, atribuída a cada serviço.
   - ➥ Área em *roaming profiles* da Microsoft.

A capacidade de fazer réplicas de igual qualidade (digital para digital) significa que é possível, e recomendável, armazenar cópias de objetos digitais num ambiente diferente das armazenadas para acesso frequente. Estas cópias terão a mesma qualidade da cópia ou original arquivado, e estes só serão necessários para inspeções, para fazer novas cópias, ou para efetuar a migração para novos formatos.

Documento de Suporte à Especificação: Política de *Backups*

Segundo a DGARQ (2011), as cópias digitais de arquivo devem também ser guardadas em locais diferentes das cópias de acesso frequente, a fim de prevenir perdas de informação por desastres, roubo ou mau manuseamento.

Cópia Arquivada – uso limitado (*backup*/réplica)	**Cópia de acesso frequente – uso múltiplo** (armazenamento)
1. Armazenar num ambiente controlado e separado, se possível, da cópia de acesso frequente; 2. Armazenar em condições ambientais recomendadas para armazenamento de arquivo.	1. Armazenar para fácil acesso; 2. Verificar, visualmente, se o disco foi alvo de algum dano após a utilização; 3. Armazenar em condições ambientais similares às condições de utilização.

De acordo com a DGARQ (2011), as unidades de suporte para backups mais aconselhadas são:

- ***Tapes (magnéticas):*** *são um suporte de acesso sequencial, pelo que, mesmo que os tempos de acesso sejam baixos, a velocidade de escrita ou leitura contínua de dados é rápida. São, desde há muito tempo, o suporte mais utilizado para armazenamento, cópias de segurança, arquivo e transmissão. Existe uma variedade de formatos, muitos dos quais proprietários ou específicos de alguns nichos de mercado, como é o caso das mainframes ou de uma marca de computadores específica.*
- ***Discos rígidos:*** *podem ser ligados localmente através de interfaces SCSI, USB ou Firewire, ou através de tecnologias de maior distância, tais como Ethernet (Rede), SCSI ou Canais de Fibra. As suas principais vantagens são: tempos de acesso baixos, disponibilidade, capacidade e facilidade de uso. A relação capacidade/preço dos discos rígidos tem vindo a melhorar ao longo dos anos.*
- ***Cópia de Segurança Remota:*** *são feitas através Internet para um local remoto e permitem proteger os dados contra alguns dos maiores perigos, como o fogo, inundações, sismos ou detonação nuclear. À medida que as ligações de Internet de banda larga se tornam cada vez mais disseminadas, os serviços de cópia de segurança remota são cada vez mais utilizados. Um dos aspetos menos positivos desta solução, prende-se com o facto da velocidade da ligação de Internet ser normalmente mais baixa do que a velocidade de transmissão dos sistemas de armazenamento de dados locais. Este facto pode ser problemático quando se lida com grandes volumes de dados. Adicionalmente, é necessário ter em conta os perigos associados à subcontratação (outsourcing) de terceiros para armazenarem dados considerados sensíveis ou pessoais.*

As menos aconselhadas são:

- ***Discos Óticos:*** *podem ser utilizados como suporte de cópias de segurança. Uma das vantagens do CD e do DVD é poderem ser restaurados em qualquer máquina com um leitor. Muitos formatos de disco ótico são WORM, o que faz com que sejam tradicionalmente utilizados para arquivo, visto os dados não poderem ser alterados.*

Outros formatos regraváveis podem também ser utilizados, como os CDRW ou DVD-RAM. Os novos discos HD-DVD e BluRay aumentaram de forma significativa a quantidade de dados que podem ser armazenados num único disco ótico. No entanto é preciso ter em consideração a inexistência de estudos sobre a real perdurabilidade de suportes óticos.

- ***Disquetes:*** *muito utilizadas durante a década de 80 e inícios de 90 e associadas às cópias de segurança. Hoje em dia, a capacidade das disquetes tornaram esta solução obsoleta.*
- ***Dispositivos de memória:*** *também conhecidos por memórias flash, Pen-drives, cartões de memória, cartões digitais, etc., estes suportes são relativamente caros em comparação com a sua baixa capacidade, mas são bastante portáteis e fáceis de utilizar.*

Nos casos em que os organismos produzam e/ou giram pequenos volumes de dados (< 10 GB) não compensa investir em grandes sistemas de armazenamento e de segurança de dados, mais vocacionados para o armazenamento de grandes volumes de dados. Nesse sentido, e tendo em conta as características específicas e limitações derivadas das ameaças, esses organismos poderão utilizar, após análise cuidada de cada uma das hipóteses de suportes de armazenamento e decisão bem justificada relativa à sua utilização como sistema de armazenamento e/ou réplica de segurança, Discos Rígidos Portáteis e/ou Discos Óticos DVD-R e DVD+R (DGARQ, 2011).

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Plano de recuperação de desastre

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de Plano de Recuperação de desastres para o Plano de Preservação de informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e

respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Plano de Recuperação de Desastre

O planeamento eficaz de desastres é essencial para garantir a segurança dos funcionários e para a sustentabilidade do conteúdo e serviços digitais. Este plano também está em linha com a missão do Arquivo para fornecer suporte em todo o ciclo de vida da informação. O objetivo deste plano é garantir o acesso contínuo aos bens e serviços digitais prestados pelo Arquivo, com o mínimo de interrupção.

Este plano é destinado a comunicar os procedimentos de preparação de desastres, continuidade e recuperação do arquivo de dados para o pessoal, os depositantes, utilizadores e financiadores, bem como facilitar a promulgação da preparação de desastres no Arquivo.

Um Plano de Recuperação de Desastres pode ser dividido em três seções principais:

- ***Mitigação;***
- ***Continuidade;***
- ***Recuperação.***

*A **Mitigação** descreve as atividades que o Arquivo se compromete para assegurar a preparação de emergências e da proteção dos seus ativos. Essas atividades incluem a avaliação de risco, um inventário de bens e equipamentos, apoiar as políticas e procedimentos, normas, formação e manutenção deste plano.*

Mitigação de desastres e prevenção são as atividades realizadas para reduzir o impacto dos perigos. Essas atividades são executadas através de um ciclo contínuo de planeamento, treino e equipamento, exercitando, avaliando e tomando ações para corrigir deficiências e reduzir vulnerabilidades.

*A fase da **Continuidade** diz respeito às atividades do Arquivo comprometendo-se a garantir o acesso contínuo aos seus produtos e serviços com o mínimo de interrupção em caso de uma emergência.*

Documento de Suporte à Especificação: Plano de recuperação de desastre

Recuperação *detalha as etapas que o Arquivo vai empreender para restaurar o arquivo para a funcionalidade completa depois de uma emergência. Esta secção inclui orientações sobre a recuperação e a utilização das aplicações e tecnologias-chave.*

Mitigação

Normas e Procedimentos de ativos essenciais

Conjuntos de dados:

- *Tipos de dados;*
- *Confidencialidade;*
- *Aquisições;*
- *Formatos;*
- *Acesso;*
- *Localização;*
- *Volume;*
- *Políticas de apoio;*
- *Plano de Sucessão.*

Website e Catálogo:

- *Tipos de arquivos e formatos;*
- *Localização;*
- *Volume;*
- *Políticas de apoio;*
- *Rede informática;*
- *Material Analógico;*
- *Pessoal.*

Inventário do Equipamento

A seguinte tabela fornece uma possível lista de equipamentos e sistemas, dentro de um Arquivo. No caso de um grande desastre, esta lista irá fornecer ao Arquivo, uma ferramenta com a qual começar a avaliar os danos e documentar o custo de recuperação.

Documento de Suporte à Especificação: Plano de recuperação de desastre

Tabela 1 – Estrutura exemplo de um inventário de bens de um arquivo

Data	Item	Condição (boa, danificado, destruído)	Custo	Observações
mês/dia/ano	Computador: tipo			
mês/dia/ano	Impressora: tipo			
mês/dia/ano	Scanner: tipo			
mês/dia/ano	Secretária: grande			
mês/dia/ano	Secretária: média			
mês/dia/ano	Secretária: pequena			
mês/dia/ano	Estantes rolantes			
mês/dia/ano	Unidades de Armazenamento			
mês/dia/ano	Cacifos			
mês/dia/ano	Quadros			
mês/dia/ano	Cadeiras adicionais			
mês/dia/ano	Mesa de conferência			
mês/dia/ano	Cadeiras de secretária			
mês/dia/ano	Iluminação			

mês/dia/ano	Aquecimento e Arrefecimento			

Formação (Treino)

Os planos de recuperação de desastres não são úteis se permanecerem na prateleira; devem ser elaborados e serem dados a conhecer a todos os funcionários, para que estes se familiarizem com o seu conteúdo. Os funcionários vão precisar de saber onde encontrar informações essenciais e quais são suas responsabilidades, antes, durante e depois de uma emergência.

Formação (Treino) de recuperação

Periodicamente, o Arquivo irá realizar exercícios e simulações de cenários de desastres de vários níveis para assegurar que cada membro da equipa é capaz de realizar as principais atividades de recuperação necessárias para que o arquivo continue a funcionar de maneira eficiente.

Como parte deste processo, os seguintes papéis de recuperação devem ser atribuídos:

- *O programador informático será responsável por inserir atualizações do website, e garantir que os sistemas técnicos essenciais se encontram operacionais (online).*
- *O profissional de gestão da informação irá avaliar o inventário, interagir com outros colaboradores, e gerir as necessidades e expectativas dos clientes.*
- *O profissional de informação vai dirigir as operações de continuidade e recuperação.*
- *O profissional de gestão da informação irá ficar a par dos mais recentes desenvolvimentos e tecnologias para a recuperação de desastres que são colocadas em prática em instituições com missões semelhantes.*

Continuidade

Procedimentos de emergência em caso de desastre

Em primeiro lugar a equipa do arquivo deve-se reger pelas normas existentes a nível do edifício onde se encontrem estabelecidos e da cidade a que pertencem.

Dentro do arquivo, o arquivista irá supervisionar todos os procedimentos de emergência e de interface com a universidade e departamento de pessoal em relação a resposta de emergência. O arquivista também irá emitir relatórios de estado para os clientes relativas a danos para o Arquivo e o tempo de recuperação necessário para restaurar a funcionalidade.

Comunicação

Comunicação eficiente é fundamental para garantir a segurança do pessoal e do público, bem como para se manter conectado com os utilizadores em caso de uma crise.

O pessoal do Arquivo deve entrar em contato com os restantes colaboradores por telefone, email ou qualquer outro meio disponível para comunicar a sua situação e qualquer informação relativa à continuidade e recuperação do arquivo.

Documento de Suporte à Especificação: Plano de recuperação de desastre

Será de responsabilidade do arquivista entrar em contato com os utilizadores e informá-los dos danos, bem como os esforços de recuperação e estado. Principal ponto de contato com os seus utilizadores do arquivo é o seu website, pois este é o lugar onde os esforços de comunicação serão o alvo. Atualizações informativas durante a resposta aos desastres e de recuperação incluem o seguinte:

- *Data e hora da atualização;*
- *Breve resumo da situação;*
- *Declaração de estado e ações;*
- *Tempo esperado resolução;*

Continuidade de serviços

O arquivo deve ser capaz de continuar os seus serviços mesmo sem um local físico (Ver DMAG_DSE_Plano_de_continuidade).

O acesso e utilização de conjuntos de dados podem ser restaurados e preservados, desde que a conectividade de rede seja estabelecida. Se isso não acontecer deve-se tentar estabelecer um contacto com outra rede para as opções de armazenamento em nuvem, o que reduzirá a dependência do arquivo de uma rede particular.

Embora o acesso a conjuntos de dados possa continuar sem muita dificuldade, pode-se perder alguns dos serviços centrados no cliente. Nestes casos, o arquivo deve oferecer suporte de pesquisa e análise.

Recuperação

Recuperação a partir de um local remoto

O Arquivo não requer necessariamente um local físico para cumprir sua missão de preservar e disponibilizar acesso a dados de pesquisa.

Usando os procedimentos de recuperação descritas neste documento, a equipa de arquivo pode conseguir restaurar a preservação e a funcionalidade de acesso a partir de uma localização remota, desde que possam aceder aos servidores, que se encontram noutra localização. Uma vez que o arquivo começar a tirar proveito de opções de armazenamento em nuvem, a dependência de uma infraestrutura física torna-se desnecessária no caso de uma emergência.

Se o profissional de informação é incapaz de entrar no escritório físico, ela ou ele vai coordenar com o programador e qualquer outro pessoal, por telefone ou outros meios para determinar a melhor forma de manter o arquivo em funcionamento enquanto o local físico é restaurado/recuperado.

Recuperação no escritório

Embora o arquivo possa sobreviver por um período de tempo sem um local físico, um este fornece ao arquivo formas mais eficientes de se conectar a utilizadores, doadores e outros contatos.

Uma vez que seja capaz de voltar a entrar no escritório, o profissional de informação deve realizar um inventário completo de todos os equipamentos recuperáveis, juntamente com estimativas sobre quando estará pronto para utilização.

Este deve ser liberal na sua estimativa do tempo necessário para reparar ou substituir um recurso danificado incluindo a encomenda, o transporte, instalação e tempo de teste. O inventário deve observar se os ativos estão desaparecidos, destruídos ou recuperáveis. Além de avaliar os ativos e equipamentos, o profissional de informação pode querer avaliar danos à estrutura elétrica, ar condicionado e rede, se este ainda não tiver sido realizado.

Recuperação de pessoal

É possível que o pessoal necessite de tempo para garantir o seu bem-estar, mas regressar ao trabalho é importante para a própria recuperação das pessoas que sofreram desastres. O Arquivo deve incentivar alimentação adequada, descanso e lazer para acelerar a recuperação física e emocional de sua equipa. O arquivo também deve ter uma política de porta aberta que facilita a procura de cuidados, quando necessário.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Plano de Continuidade

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Plano de continuidade para a elaboração do Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Plano de Continuidade

O Plano de Continuidade Digital, baseado em seis princípios da Continuidade Digital irá ajudar as organizações a alcançar benefícios de negócios, incluindo a eficiência e minimização de riscos.

Princípios de Continuidade Digital:

1. *O valor da informação digital como um negócio, probatório e recursos da comunidade é entendida e as informações são geridas em conformidade.*
2. *A administração da informação digital é integrada com a governança da organização, com papéis e responsabilidades claramente definidas e alocadas.*
3. *Informação digital é autêntica e confiável.*
4. *Informação digital é visível, acessível e utilizável.*
5. *Informação digital é gerida digitalmente.*
6. *Informação digital é gerida, protegida e preservada por tanto tempo quanto necessário e, em seguida, eliminada de forma adequada.*

O Plano de Continuidade Digital:

- *Identifica os resultados práticos que surgem a partir dos Princípios de Continuidade digitais e sugere ações-chave para alcançar estes resultados*
- *Auxilia todas as agências na gestão contínua de informações digitais, permitindo-lhes atender às exigências específicas da agência e otimizar os benefícios*
- *Detalha a realização de cada ação e identifica ferramentas úteis, se for caso disso.*

Ações-chave

Essas ações compõem o Plano de Continuidade Digital e são destinadas a ajudar as organizações para alcançar os resultados de continuidade digitais. As ações não pretendem ser um processo passo-a-passo ou como uma solução "única". As organizações devem desenvolver os seus próprios planos atendendo às especificidades, de forma a alcançar a continuidade digital.

Foco no negócio

Resultado: benefícios da informação digital para o seu negócio, o governo e a comunidade são otimizados.

- *Analise a sua informação para entender a informação que a sua organização cria, utiliza e mantém e identifique responsabilidades, oportunidades, obrigações de conformidade, custo, valor e riscos.*
  - *Desenvolver planos de ação para enfrentar as maiores questões prioritárias levantadas pela análise de informações.*
  - *Regularmente atualizar e avaliar as informações recolhidas na revisão.*

Foco em pessoas, processos e tecnologia

Resultado: pessoas, processos e tecnologia estão alinhados para oferecer suporte a uma gestão da informação eficaz.

- *Estabelecer uma framework de gestão para a informação digital, que está alinhada e integrada com a administração da organização.*
- *Definir, atribuir recursos e papéis de gestão da informação digital a determinados responsáveis, incluindo a gestão de topo.*
- *Informar, formar e apoiar os utilizadores de informação.*
- *Fornecer processos, sistemas e ferramentas que possam apoiar a gestão eficaz e uso da informação.*
- *Acompanhar e analisar gestão contínua de informações digitais em relação aos objetivos da organização.*

Foco na informação

Resultado: a informação está apta à sua finalidade ao longo de sua vida.

- *Definir, atribuir e gerir metainformação apropriada.*
- *Fornecer informação digital num formato que seja acessível e utilizável.*
- *Assegurar que a informação digital pode ser trocada entre os sistemas e órgãos, e com a comunidade.*
- *Estabelecer um sistema de verificação em curso para garantir que a informação digital permanece utilizável.*
- *Se a informação já está num formato digital, continuar a geri-la num formato digital.*
- *Planear e implementar um programa permanente de disponibilização de informação de acordo com legislação vigente.*

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo

Documento de Suporte à Especificação: Plano de Continuidade	
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Documento de Suporte à Especificação: Identificação e Avaliação de Formatos

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de uma identificação e avaliação a nível de formatos de ficheiros para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de

Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

Identificação / Diagnóstico dos Sistemas de Informação (*hardware e software*)

A preservação em meio digital envolve o que se designa por planeamento sistemático que decorre desde a avaliação de necessidades e potencialidades até à construção, e posteriores atualizações do plano de preservação.

Entre os **fatores mais influentes** encontram-se os especificados por Becker, et al (2009), que se enunciam no esquema abaixo, nos quais é destacada em primeiro ligar a tecnologia.

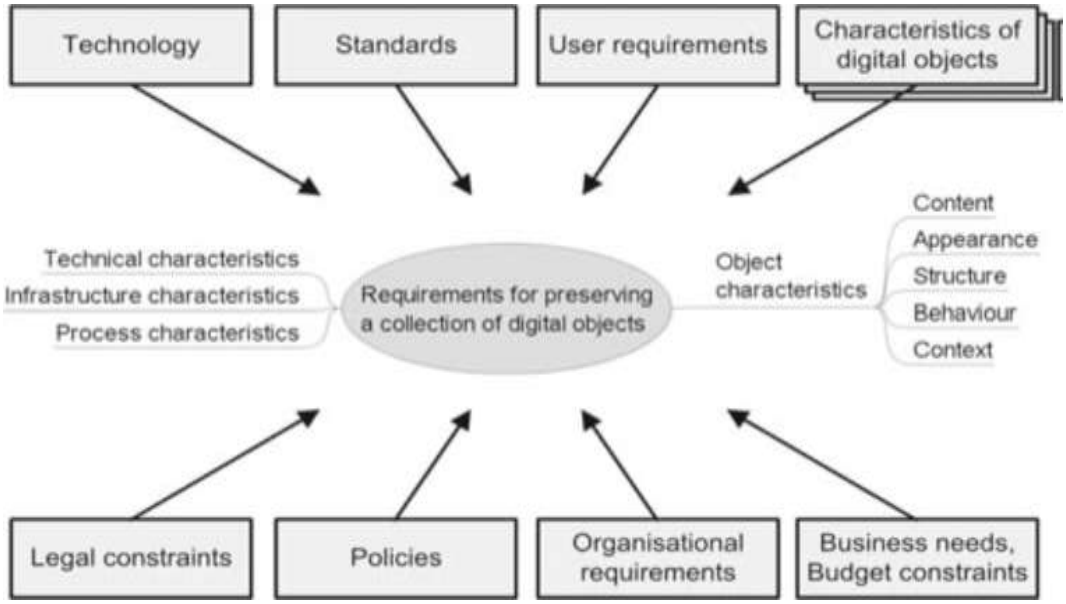


Figura 1 - Fatores de Influência (BECKER et al.,2009)

Acresce que, os elementos constituintes de um plano de preservação[1] consistem em:

- Identificação
- Estado e *Triggers*
- Descrição do ambiente institucional
- Descrição da coleção
- Requisitos para a preservação
- Evidência de decisão para uma estratégia de preservação
- Custos
- Funções e responsabilidades
- Plano de Ação de Preservação

Entre esses elementos encontra-se a identificação dos **estados de desenvolvimento do plano e as situações que despoletam as necessidades e determinam as ações de preservação.**

Assim, no planeamento da preservação foram identificadas na tabela abaixo, proposta por Becker, et al. (2009)[2] o **estado de elaboração do plano** e **as situações críticas** a considerar quer na **definição inicial do plano**, quer nas sucessivas **atualizações**, entre as quais se encontra a **monitorização tecnológica**, quer ao nível das **mudanças ambientais**, quer ao nível das **mudanças de objetivos** envolvendo:

Mudança Ambiental

[1] BECKER, Christoph, et al. (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans)

[2] BECKER, Christoph, et al. (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans)

Monitorizar a Tecnologia

- Alteração nos resultados da avaliação dos objetivos de um plano de preservação existente, por exemplo, alterações de preços ou avaliação de risco alterada;
- Novas estratégias de preservação disponíveis de que constituem por exemplo, novas versões de ferramentas e serviços;
- Iminente obsolescência da tecnologia utilizada, por exemplo, quando um formato de destino usado num plano de preservação baseado em migração está a tornar-se obsoleto.

Mudanças de Objetivos

Monitorizar a Tecnologia

- Novas normas que devem ser adotadas.
- Monitorizar a comunidade designada
- Mudança na plataforma computacional ou nas tecnologias de comunicação utilizadas.

Alert	Triggered by OAIS functional entity	Event (examples)
New collection	Administration	Agreement for a new collection
	Monitor Designated Community	New object type in use
		Frequent submissions of unanticipated formats
Changed collection profile	Monitor Designated Community	Use of a new version of an object format in the designated community
		Frequent submission of unanticipated formats or new versions of an object format, or objects with new functionality/characteristics
	Manage System Configuration (in Administration)	Collection grows faster than initially foreseen and specified in the existing preservation plan
Changed environment	Monitor Technology	Change in the results of the evaluation of objectives of an existing preservation plan, for example price changes or changed risk assessment
		New available preservation strategies, for example new versions of tools and services
		Impending obsolescence of used technology, for example when a target format used in a migration-based preservation plan is becoming obsolete
	Monitor Designated Community	Change of software available at user sites (e.g. indicated by reports about problems with DIPs)
Changed objective	Monitor Technology	New standards that have to be adopted
	Monitor Designated Community	Change in computer platform or communication technologies used
	Manage System Configuration (in Administration)	Change in designated community of consumers or producer community
		Change of institutional policies
Periodic review	Develop Packaging Design and Migration Plans	Raised on a scheduled basis defined in the institutional policy or in the preservation plan

Figura 2 - Alertas, Triggers e Eventos

Assim, encontramos como um dos objetivos **identificar os formatos produzidos e usados** na organização.

FORMATOS

Documento de Suporte à Especificação: Identificação e Avaliação de Formatos

No que respeita ao formato, a maioria das instituições terá de desenvolver procedimentos e documentos para apoiar a correta transferência de recursos digitais dos fornecedores das suas coleções. A tabela abaixo suporta a avaliação das opções existentes para os formatos de ficheiros e plataformas de armazenamento[3]. As decisões sobre formatos de ficheiro e plataformas de armazenamento vão apoiar e ser interdependentes com este processo.

Tabela 1 – Avaliação das opções existentes para os formatos de ficheiros e plataformas de armazenamento

Opções	Questão	Requisitos
		Política de formatos de armazenamento. Visão Tecnológica sobre a evolução formatos de armazenamento. (todas as opções)
Limitar série de formatos de arquivos recebidos Limitar série de plataformas recebidos (opção a longo prazo mais rentável)	Simplifica a gestão e reduz os custos gerais. O Depositante pode não ter recursos ou conhecimento para cumprir. Grande variedade de formatos de arquivos usados e extensões proprietárias com padrões abertos. A plataforma utilizada para a transferência pode, potencialmente, ser usada para o armazenamento a longo prazo.	Diretrizes sobre formatos preferenciais. Grau de influência sobre o depósito. Estratégias de divulgação e colaboração para atingir os resultados desejados. Diretrizes sobre as plataformas de transferência preferenciais e procedimentos de transferência.
Aceitar como recebido, mas converter para o formato de arquivo padrão Aceitar como recebido, mas converter para o formato de plataforma de armazenamento padrão	Simplifica a gestão e reduz os custos de longo prazo. Pode não ser tecnicamente viável para converter para o formato padrão. Será necessário verificar se a perda acidental de dados não ocorreu.	Permissões de direitos de autor ou direitos legais de preservação. Recursos e capacidades técnicas da instituição de acolhimento. Eleição dos formatos preferidos. Documentação de formatos nativos para permitir a conversão. A integridade verifica o processo de conversão.

[3] (DPC, p.97)

Aceitar e armazenar como recebido (opção menos rentável a longo prazo, apesar da redução de custos iniciais)	Complica a gestão e aumenta os custos de gestão dos recursos ao longo do tempo. Opção de alto risco, especialmente se um grande número de recursos digitais estão a ser recolhidos. A escolha de formatos de arquivos pode estar disponível. O que se encontra depositado pode não ser o mais adequado para a preservação. Plataforma de armazenamento pode ser de qualidade e adequação desconhecida para preservação a longo prazo. Os formatos podem estar obsoletos ou não são suportados dentro da instituição.	Prioridades claramente definidas para a preservação tanto a curto como a longo prazo. Habilidade para tratar de questões como a criptografia, *software* proprietário, em itens recebidos. Habilidade de assegurar o acesso futuro à informação contida no item.

Tal como acontece com os suportes de armazenamento, há uma grande variedade de formatos (por exemplo, Word, TIFF) de uso comum.

Os formatos de ficheiros estão sujeitos a uma rápida evolução, assim como obsolescência. O processo de seleção e avaliação de opções para a preservação é largamente de redução de riscos.

O uso de formatos de ficheiros que tenham sido bem documentados, submetidos a testes rigorosos e que sejam não-proprietário e utilizáveis em diferentes plataformas de *hardware* e *software* minimiza a frequência de migração e reduz o risco e os custos da sua preservação.

Da mesma forma, utilizando formatos que têm sido amplamente adotados minimiza o risco, pois é mais provável que os caminhos de migração sejam fornecidos pelos fabricantes e que haja um grau de "retro compatibilidade" que esteja disponível entre as versões do formato de arquivo conforme evolução.

É aconselhável para as instituições, sempre que possível identificar formatos de ficheiro que são preferidos para armazenamento de arquivos e para procurar depósitos nessa forma, sempre que exista uma escolha de formatos.

Algumas instituições têm identificado e distinguido os formatos preferidos, aceitáveis e não aceitáveis para transferência para a instituição, para o armazenamento de arquivo, assim como os formatos que possam ser fornecidos aos utilizadores.

Desta forma, são apresentadas as seguintes recomendações[4] no que aos formatos de ficheiros diz respeito:

- Usar formatos de ficheiros "abertos", não-proprietários e bem documentados, sempre que possível.
- Alternativamente utilizar formatos de ficheiro que são bem desenvolvidos, têm sido amplamente adotado e que de facto são normas no mercado.
- Identificar formatos aceitáveis para fins de transferência, armazenamento e distribuição para os utilizadores (que podem ser distintos).
- Minimize o número de formatos de ficheiro a ser gerido, tanto quanto for possível / desejável.
- Não usar criptografia ou compressão para ficheiros de arquivamento, se possível.

Tabela da DGARQ[5]

Categoria	Características
1. Dados Tabulares (Data Set)	Dados alfanuméricos existentes numa vasta variedade de aplicações de processamento de dados; Dados geridos em ficheiro linear (flatfile), em rede, hierárquica; Bases de dados relacionais e orientadas a objetos.
2. Texto estruturado/ documentos do Office	Dados alfanuméricos; Dados de marcação (markup); Etiquetas para outros tipos de dados (imagens vetoriais e mapas de bits [raster]) existentes em processadores de texto/programas para escritório e digitalização de documentos/sistemas aplicacionais de gestão de documentos eletrónicos, bases de dados relacionais, e outros ambientes de tipos de documentos de aplicações específicas.
3. Dados de Desenho [design data]	Imagens vetoriais e de mapa de bits e dados alfanuméricos em sistemas de CAD e conversão orientada a objetos para bases de dados normalizadas.
4. Apresentações	Dados alfanuméricos em imagens empresariais, clipart [formação de imagens], vídeo, e multimédia de treino/ensino. Diagramas para a gestão de informações, de conhecimento e de capital intelectual; para a compreensão e solução de problemas.
5. Imagens	Imagens de mapas de bit e dados alfanuméricos existentes no *software* de captura/edição de imagens, bases de dados orientadas a objetos, relacionais ou

[4] DPC

[5] Barbedo, F.; Corujo, L.; Sant'ana, M. (2010). Recomendações para a produção de planos de preservação digital. Lisboa: DGARQ. Consultado em Outubro 30, 2013, em http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf>

	simples de livrarias de fotos, coleções digitais de belas-artes, coleções de imagens médicas.
6. Documentos de som e voz	Dados de som em processamento de voz, bases de dados relacionais ou simples (flat) de registos áudio em coleções de música e repositórios similares.
7. Documentos de Vídeo	Vídeo Digital, ecrã total (*fullscreen*) / vídeo (em movimento) em fotogramas de vídeo digital armazenadas em ficheiros de mapas de bit e som armazenadas em bases de dados relacionais ou simples (flat) em coleções de música e repositórios similares
8. Dados geográficos/cartográficos	Imagens vetoriais e de mapa de bits e dados alfanuméricos em sistemas de informação geográfica (SIG) e *software* de cartografia. Dados armazenados orientados em bases de dados relacionais orientadas a objetos.
9. Publicações Multimédia Interativas	Dados de som e vídeo, imagens em movimento, imagens vetoriais e de mapa de bits e dados alfanuméricos armazenados em *software* de criação e edição em ambientes de publicação eletrónica.
10. Dados Científicos e Financeiros	Dados específicos de carácter científico e financeiro.

Desta forma, segundo Barbedo et al. (2010), recomenda-se que não se utilize formatos proprietários para armazenamento e preservação digital a longo prazo, por vários motivos, nomeadamente a obsolescência dos formatos, devendo ser necessário identificar, à partida, quais os formatos que, por serem normalizados e/ou não proprietários e de fácil preservação a longo prazo, se poderão utilizar alternativamente.

Quando não existem formatos normalizados para cada uma das categorias de formatos identificados, há que manter o formato original sujeito a monitorização regular até ser desenvolvido um formato normalizado aplicável ao formato original em questão.

Deve ser produzida uma tabela que permita definir quais os formatos de preservação que a organização pretende utilizar.

Para isso, foi criada uma tabela[6] com uma lista dos critérios de apoio/suporte à avaliação de formatos.

Segundo, os colaboradores da "London Metropolitan Archives and Guildhall Library Manuscripts" os objetos devem ser preservados, sempre que possível, em formato aberto, dado que é de mais fácil compreensão e torna-se mais fácil o desenvolvimento de software que possa ler este tipo de formato. Podem ser também admitidos os formatos mais amplamente utilizados.

Para os "The National Archives" a formatação original do documento deve ser preservada, para evitar a degradação de cópias, através de técnicas, como migração, encapsulamento, etc. Deve-se, por isso, evitar objetos com patentes, direitos de propriedade

[6] Anexo DMAG_DSE_Identificação_Avaliação_de_Formatos

intelectual ou outros direitos, pois necessitam de licenciamento para o desenvolvimento de software que possam ler estes objetos.

De acordo com a "Sheffield Archives and Sheffield Local Studies Library", todos os objetos devem ser revistos periodicamente para evitar a obsolescência tecnológica. Sempre que possível serão utilizados padrões abertos (ou seja, não proprietários) para cópias principais e de acesso. Além disso, são utilizadas para cópias de acesso Adobe Portable Document Format (PDF) e os formatos do MS Office (Word, Excel, Access e PowerPoint).

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto
DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

Nome do critério	Descrição
Quota de Mercado	Se o formato é amplamente aceite ou simplesmente um formato de nicho. A quota de mercado também é conhecida como grau de "adoção". A "adoção" refere-se ao grau de utilização do formato por parte dos criadores primários, disseminadores, e/ou utilizadores dos recursos de informação. Um elevado nível de adoção é considerado favorável para fins de preservação.
Nível de Suporte técnico	O nível de suporte técnico dado pelo criador oficial do formato. Um elevado nível de suporte é preferível num contexto de preservação
Normalizado (standard)	Se o formato foi publicado por uma organização oficial de normalização. Formatos normalizados são preferíveis aos não normalizados.
Especificação Aberta	Se a especificação do formato pode ser inspecionada/verificada de forma independente. O uso de formatos abertos é fortemente recomendado em contextos de preservação
Suporta Compressão	Se o formato suporta qualquer tipo de compressão. Formatos não comprimidos são geralmente defendidos pela comunidade.
Apenas suporta Compressão com Perda	Se o formato suporta exclusivamente um tipo de compressão que provoca perda de informação ou deterioração do objeto original. Os esquemas de compressão com perda são geralmente desaconselhados.
Suporta Transparência	Se o formato oferece funcionalidades de tranparência. Este critério é relativamente específico de certo tipo de formatos (p. ex. imagens de mapa de bits). Se o formato de origem contém funcionalidades de transparência, o formato de destino deve ter também suporte para essa propriedade.
Metainformação Embebida	Se o formato contém metainformação embebida. O formato de destino deve ter capacidade de incluir/acomodar a metainformação embebida do formato de partida.
***Royalties* (taxas de utilização)**	Se a utilização ou produção do formato requer o pagamento de *royalties* ou taxas de utilização. Existe preferência por formatos livres de *Royalties*
Código Aberto	Se existem aplicações cujo código pode ser inspecionado/verificado de forma independente. A existência de aplicações de código aberto é grandemente recomendada.
Retrocompatibilidade	Se as revisões aos formatos incluem suporte para as versões anteriores. A Retrocompatibilidade é uma caracteristica desejável.
Nível de Documentação	Se as especificações do formato estão bem documentadas. Favorece-se a existência de formatos bem documentados
Formatos Concorrentes	Se existem formatos concorrentes ou similares. A existência de formatos concorrentes torna um formato mais atrativo para preservação, uma vez que a informação poderá ser mais facilmente convertida.
Suporte a Gestão de Direitos Digitais	Se é possível a utilização de Gestão de Direitos Digitais (DRM), encriptação ou assinaturas digitais. Desaconselha-se a existência de qualquer tipo de funcionalidade que possa constituir obstáculo no acesso à informação.
Frequência de Atualização	Qual a frequência de revisão de um formato desde a sua publicação inicial. Este critério é defenido de acordo com a seguinte fórmula: número de revisões / (ano atual - ano de disponibilização). Os formatos estáveis são preferenciais. Se a frequência de revisões é muito grande, o arquivo poderá ter dificuldade em acompanhar o ritmo das mesmas.
Suporte para extensões	Se o formato permite a inclusão de esxtensões, tais como seções executáveis ou caracteristicas marginalmente suportadas. Desaconselha-se a utilização de formatos que suportam tais funcionalidades
Longevidade	Quantos anos passaram desde que o formato foi disponibilizado oficialmente. Os formatos de longa duração têm geralmente preferência sobre formatos novos e pouco estabelecidos
Interpretação/descodificação transparente	Complexidade inerente à codificação: legibilidade por parte de um ser humano recorrendo a um editor de texto simples. Têm preferência os formatos que podem ser facilmente inspecionados e/ou interpretados.
Vários produtores de aplicações de leitura	Se existem várias entidades que produzem leitores/visualizadores. Para finalidades de preservação, não se deve apostar apenas em leitores produzidos somente por uma única entidade.
Várias aplicações de leitura	Se o formato pode ser lido/interpretado por diversas aplicações informáticas. Para finalidades da preservação, não se deve apostar em formatos que apenas podem ser lidos/visualizados por uma aplicação específica.
Aplicações de leitura em código aberto	Se o código fonte da aplicação de leitura pode ser inspecionada/verificada de forma independente. A existência de leitores/visualizadores em código aberto é uma caracteristica altamente desejável.
Leitor/Visualizador Multiplataforma	Se a aplicação de leitura/visualização pode ser executada, ou tem versões para várias outras plataformas (p. ex. sistemas operativos ou hardware). A existência de aplicações executáveis em plataformas concorrentes é uma caracteristica altamente desejável num contexto de preservação.

Documento de Suporte à Especificação: Diagnóstico dos Sistemas Tecnológicos e Informacionais da CMP

	Responsável	*Data*	*Assinatura*
Elaborado por	Equipa da		_____
Verificado por	Chefe de Divisão		_____
Aprovado por	Diretor Municipal		_____

Revisão	*Data da Aprovação*	*Descrição das Alterações*
0	/ /	1ª Elaboração do documento

Detentores de Cópias Controladas:

1. OBJETIVO

Este documento tem como principal objetivo servir de guia para a definição de um Diagnóstico dos sistemas tecnológicos e informacionais para o Plano de Preservação da informação em meio digital da Câmara Municipal do Porto.

2. ÂMBITO

Este Documento de Suporte à Especificação aplica-se ao Plano de Preservação da Informação, tendo por base as Políticas de Preservação de Informação e as Políticas de Segurança de Informação, alicerçadas por uma Política de Gestão da Informação e TI, e respetivo Plano, sob a monitorização de uma Comissão de Gestão da Informação e TI no âmbito da implementação do Arquivo Digital Certificado da Câmara Municipal do Porto.

3. RESPONSABILIDADES

Atividade / Função	DM	DD	CD	SEC	QC
Receção / identificação de documento				R	
Registo de um novo documento				R	R
Encaminhamento			R	E	R
Receção por parte do Gestor					R
Encerramento	R	R	R	E	

4. DESCRIÇÃO

IDENTIFICAÇÃO/ DIAGNÓSTICO DOS SISTEMAS TECNOLÓGICOS E DE INFORMAÇÃO (*hardware e software*)

A preservação em meio digital envolve o que se designa por planeamento sistemático que decorre desde a avaliação de necessidades e potencialidades até à construção, e posteriores atualizações do plano de preservação.

Entre os **fatores mais influentes** encontram-se os especificados por Becker, et al (2009), que se enunciam no esquema abaixo, nos quais é destacada em primeiro lugar a tecnologia.

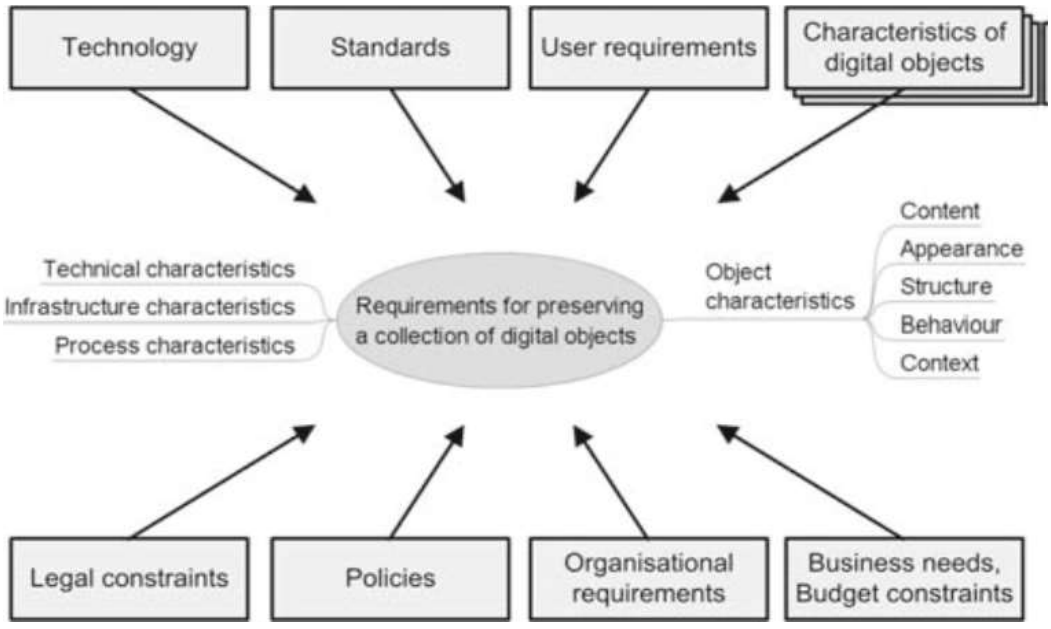


Figura 1 - Fatores de Influência (BECKER et al., 2009)

Acresce que, os elementos constituintes de um plano de preservação[1] consistem em:

- Identificação
- Estado e *Triggers*
- Descrição do ambiente institucional
- Descrição da coleção
- Requisitos para a preservação
- Evidência de decisão para uma estratégia de preservação
- Custos
- Funções e responsabilidades
- Plano de Ação de Preservação

Entre esses elementos encontra-se a identificação dos **estados de desenvolvimento do plano e as situações que despoletam as necessidades e determinam as ações de preservação.**

Assim, no planeamento da preservação foram identificadas na tabela abaixo, proposta por Becker, et al. (2009)[2], o **estado de elaboração do plano** e **as situações críticas** a considerar quer na **definição inicial do plano**, quer nas sucessivas **atualizações**, entre as quais se encontra a **monitorização tecnológica**, quer ao nível das **mudanças ambientais**, quer ao nível das **mudanças de objetivos** envolvendo:

Mudança Ambiental

- **Monitorizar a Tecnologia**
  - Alteração nos resultados da avaliação dos objetivos de um plano de preservação existente, por exemplo, alterações de preços ou avaliação de risco alterada;
  - Novas estratégias de preservação disponíveis, por exemplo, novas versões de ferramentas e serviços;
  - Iminente obsolescência da tecnologia utilizada, por exemplo, quando um formato de destino usado num plano de preservação baseado em migração está a tornar-se obsoleto.

Mudanças de Objetivos

- **Monitorizar a Tecnologia**
  - Novas normas que devem ser adotadas.
- **Monitorizar a comunidade designada**
  - Mudança na plataforma computacional ou nas tecnologias de comunicação utilizadas.

[1] BECKER, Christoph, et al. (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans).
[2] BECKER, Christoph, et al. (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans).

Alert	Triggered by OAIS functional entity	Event (examples)
New collection	Administration	Agreement for a new collection
	Monitor Designated Community	New object type in use
		Frequent submissions of unanticipated formats
Changed collection profile	Monitor Designated Community	Use of a new version of an object format in the designated community
		Frequent submission of unanticipated formats or new versions of an object format, or objects with new functionality/characteristics
	Manage System Configuration (in Administration)	Collection grows faster than initially foreseen and specified in the existing preservation plan
Changed environment	Monitor Technology	Change in the results of the evaluation of objectives of an existing preservation plan, for example price changes or changed risk assessment
		New available preservation strategies, for example new versions of tools and services
		Impending obsolescence of used technology, for example when a target format used in a migration-based preservation plan is becoming obsolete
	Monitor Designated Community	Change of software available at user sites (e.g. indicated by reports about problems with DIPs)
Changed objective	Monitor Technology	New standards that have to be adopted
	Monitor Designated Community	Change in computer platform or communication technologies used
	Manage System Configuration (in Administration)	Change in designated community of consumers or producer community
		Change of institutional policies
Periodic review	Develop Packaging Design and Migration Plans	Raised on a scheduled basis defined in the institutional policy or in the preservation plan

Figura 2 - Alertas, *Triggers* e Eventos

Assim, encontramos como um dos objetivos **identificar todos os sistemas de informação, designação assumida na aceção tecnológica (*hardware* e *software*)** existentes na organização.

Está em causa a produção e ou armazenamento de dados e informação, diretamente relacionada com as atividades desempenhadas pela organização.

Neste sentido o seu desempenho terá impacto nos processos a utilizar para preservar essa informação.

Entre as possibilidades de FRD[3] a utilizar para a análise e tratamento dos dados encontram-se nas figuras apresentadas abaixo (mod. DGARQ, 2011) que por sua vez permitirá, obter uma descrição das características do sistema tecnológico[4], bem como o conhecimento necessário sobre a informação que se pretende preservar no âmbito do Plano de Preservação Digital.

5. DEFINIÇÕES E ABREVIATURAS

CD	- Chefe de Divisão
CMP	- Câmara Municipal do Porto

[3] Ver Anexo DMAG_Anexo_DSE_Identificação_Sistemas_Informação
[4] Ver Anexo DMAG_Anexo_DSE_Identificação_Sistemas_Informação

DD	- Diretor de Departamento
DM	- Diretor Municipal
F	- Formulário
GP	- Gestor do Processo
I	- Instrução
NC	- Não Conformidade
P	- Procedimento
QC	- Qualquer Colaborador
RAM	- Responsável Ações de Melhoria
SEC	- Colaborador a exercer Funções na Secretaria

6. ANEXOS

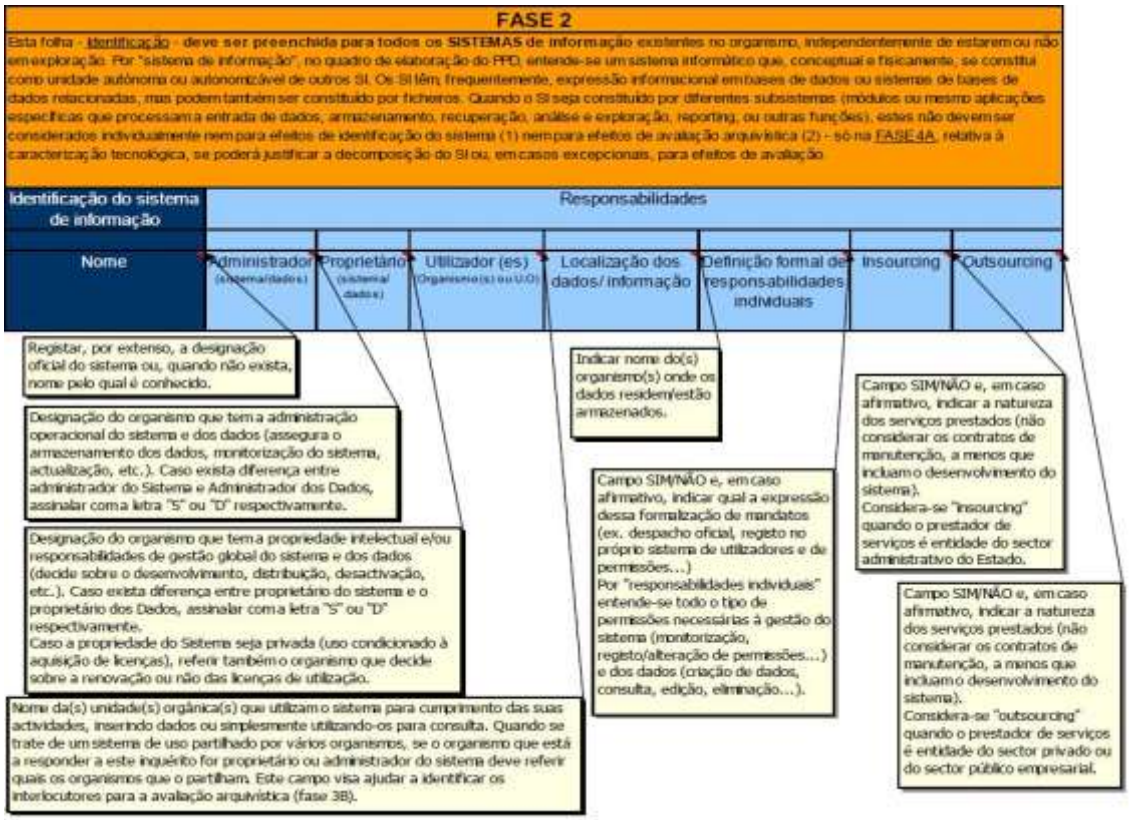


Figura 3 – Identificação de Sistemas de Informação

Documento de Suporte à Especificação: Diagnóstico dos Sistemas Tecnológicos e Informacionais da CMP

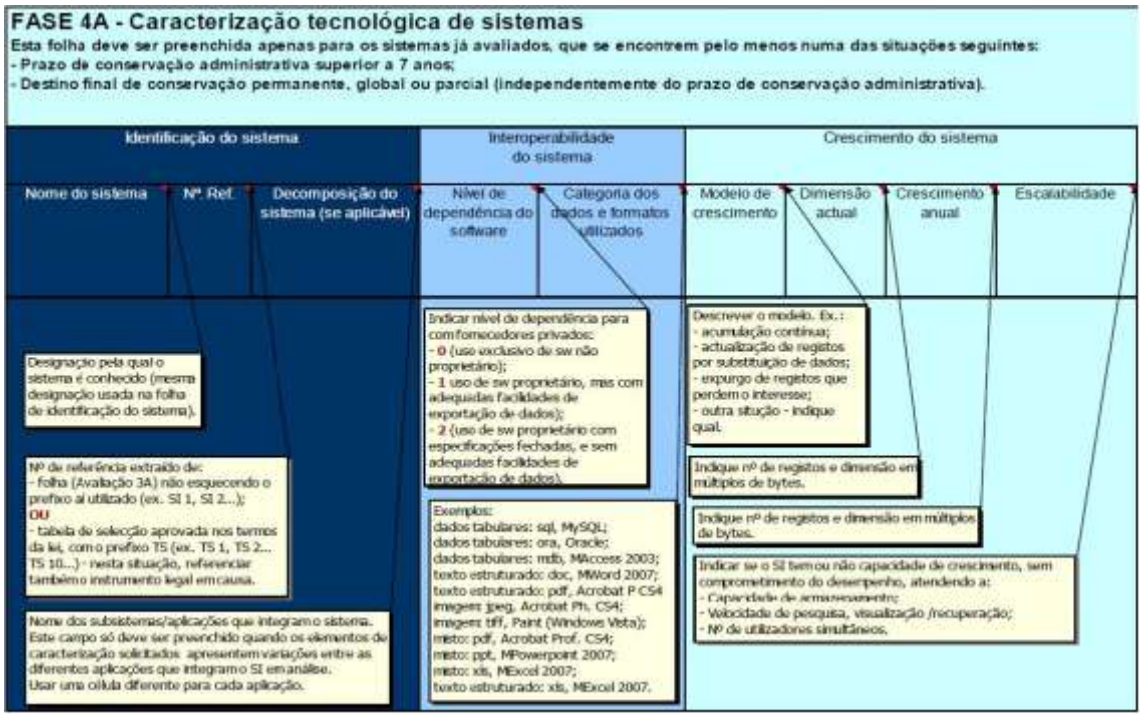


Figura 4 - Caracterização de Sistemas de Informação/TI (1)

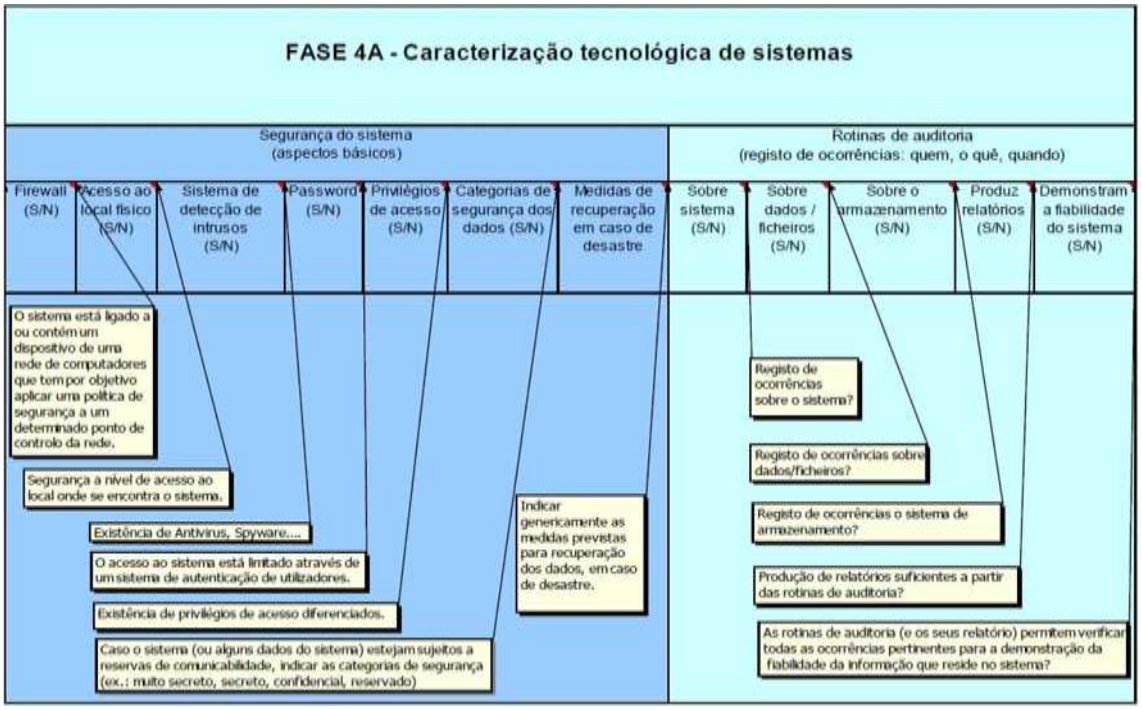


Figura 5 - Caracterização de Sistemas de Informação/TI (2)

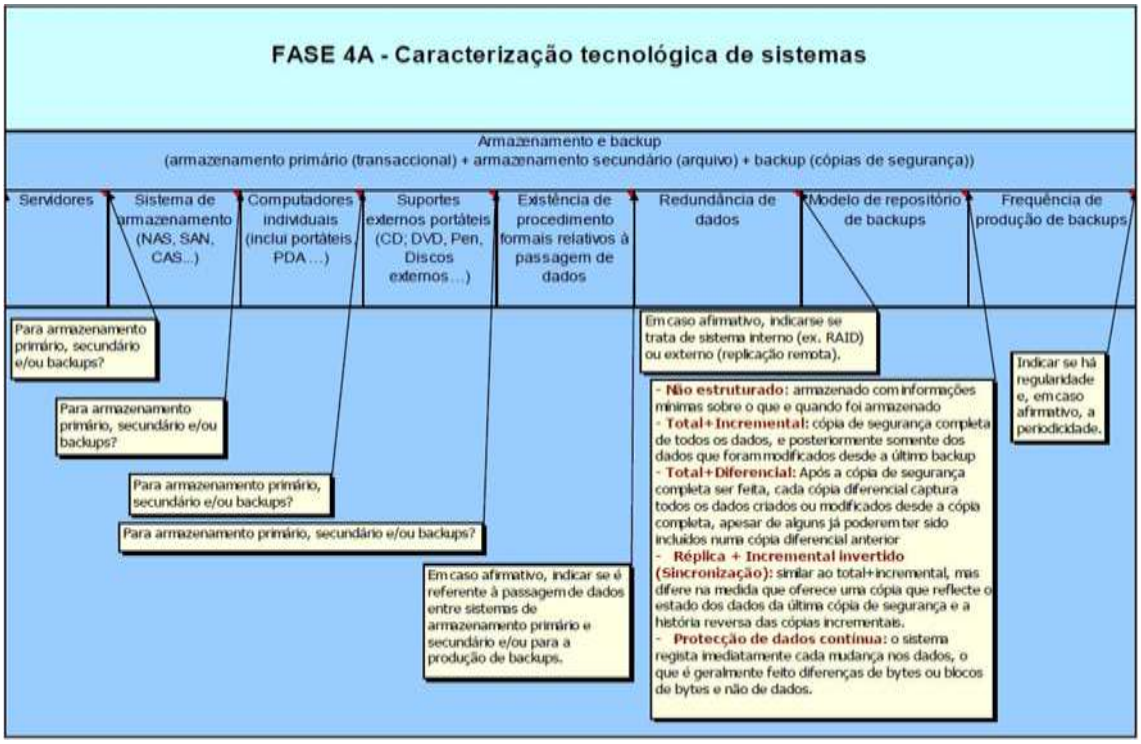


Figura 6 – Caracterização de Sistemas de Informação (3)

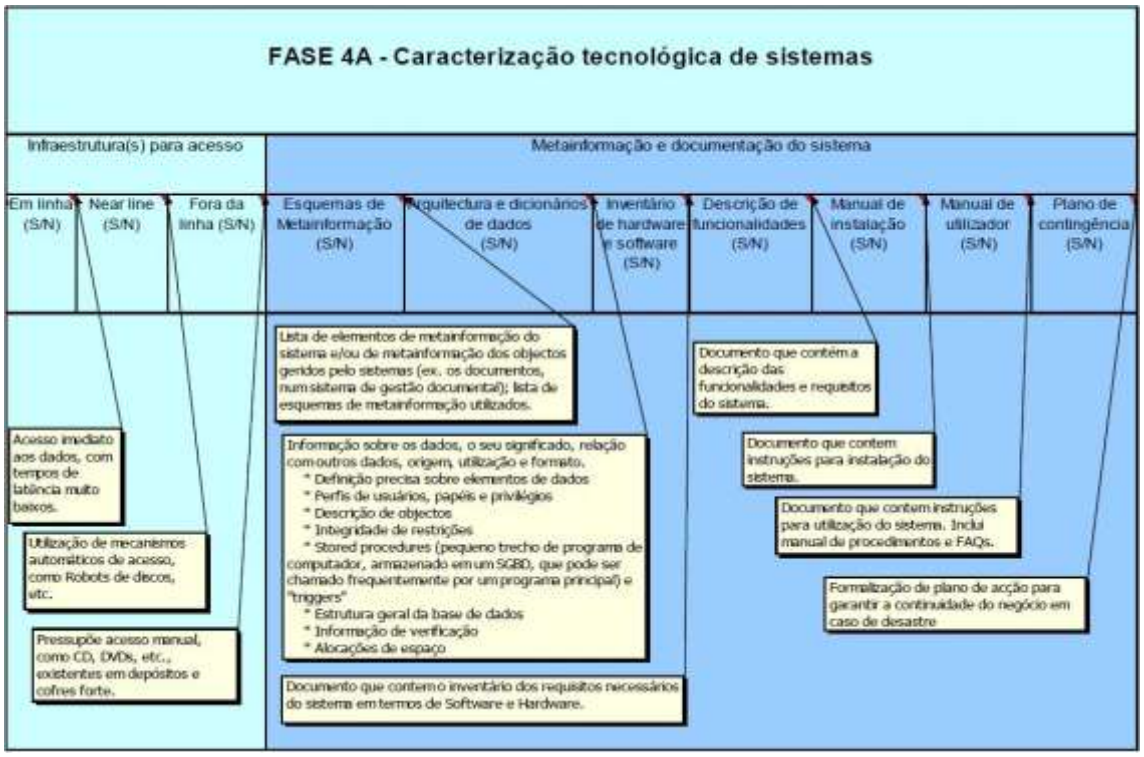


Figura 7 - Caracterização de Sistemas de Informação/TI (4)

Anexo 5: Documento de Especificação de Requisitos – Repositório Digital Confiável

Arquivo Digital Confiável

Documento de Especificação de Requisitos

ISO/IEC 16363:2012

Sumário

1. Introdução

1.1. Propósito do documento

Este documento tem como propósito especificar um conjunto de requisitos de implementação e inovação para o *Arquivo Digital* da Câmara Municipal do Porto, com vista à definição de para uma futura certificação normativa (ISO 16363:2012 – *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*).

Para tal, foi necessário aplicar todos os requisitos compreendidos na norma ISO 16363:2012 ao qual se seguiu uma comparação de correspondência com a tabela de certificação de requisitos do projeto Portico. Na última coluna apresenta-se a conformidade de documentos que foram criados no âmbito deste projeto de dissertação para que possam ser submetidos a avaliação aquando de uma futura auditoria para a certificação do repositório digital.

1.2. Âmbito do repositório

A normativa ISO 16363:2012 é relevante por consistir numa revisão da *checklist* do TRAC - *Trustworthy Repositories Audit & Certification: Criteria and Checklist*. De acordo com os seus critérios, torna-se 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 sua missão de preservação digital.

Um repositório digital confiável não deve deixar de parte a implementação de ações e de uma estratégia consciente, e entender os riscos e ameaças a que os sistemas estão sujeitos. A Norma também faz uma ressalva quanto ao estado de confiança que o repositório alcança, pois não se trata de uma realização única, dado que pressupõe auditorias regulares para que se possa averiguar a conformidade do mesmo.

Esta norma "reúne um conjunto de requisitos que vão desde a gestão organizacional, às infraestruturas de suporte, e que são considerados vitais no estabelecimento de um clima de confiança em torno de um repositório digital". Um repositório digital deve atender a estes critérios para que seja considerado um repositório confiável.

Há um conjunto de requisitos fundamentais que devem ser observados para que os

repositórios consigam obter a certificação, destacando-se, assim, alguns deles:

- O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, a preservação a longo prazo, a gestão e acesso à informação digital.
- O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório terá no apoio a longo prazo da sua missão.
- O repositório deve 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.
- O repositório deve comprometer-se aos 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.
- O repositório deve ter e manter contratos ou acordos de depósito apropriados para materiais digitais que gere, preserva e/ou aos quais fornece acesso.
- O repositório deve ter mecanismos em vigor para controlar o seu ambiente de preservação.
- O repositório deve identificar e gerir os riscos das suas operações de preservação e os objetivos associados à infraestrutura do sistema.
- O repositório deve manter uma análise sistemática dos fatores de risco de segurança associado a dados, sistemas, pessoal e instalações físicas.

1.3. Visão Geral do documento

Neste documento de especificação de requisitos para a implementação do *Arquivo Digital Confiável da CMP*, é apresentada uma primeira secção de descrição geral do próprio repositório, como a sua perspetiva, as suas funções e características. Posteriormente segue-se uma secção de descrição dos respetivos requisitos a serem tidos em conta no processo de certificação do repositório digital e no final encontram-se os prossupostos e dependências que existem na implementação deste repositório.

2. Descrição Geral

2.1. Perspetiva do repositório

A CMP, como uma qualquer outra organização que pretenda construir um Arquivo Digital Certificado, terá que aceitar em primeiro lugar que a materialização do sistema de gestão de informação capaz de suportar o Arquivo Digital Certificado passa, obrigatoriamente, pela criação de um Sistema [Integral] de Informação – Ativa e Permanente (**SI-AP**). Este terá que garantir o controlo do processo em tramitação dos documentos, assegurar a aplicação de técnicas de autenticação e certificação digital, a captura de metainformação (administrativa, descritiva, técnica, estrutural e de preservação) adequada, a produção/ agregação de documentos em formatos específicos de preservação mas que não limitem as atividades diárias, a avaliação sistemática e automatizada da informação finda a sua tramitação, a definição da sua inclusão ou não, no repositório digital/preservação.

Na perspetiva da gestão do sistema de informação, Pinto e Silva (2005) apontam precisamente para a ideia de que as organizações necessitam 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"[1]. É com base neste pressuposto que se configura este modelo sistémico – o SI-AP, indispensável para que se contemple todo o ciclo de vida da informação, a pluridimensionalidade e a interoperabilidade.

[1] Pinto, M. M.; Silva, A. M. (2005). Um Modelo Sistémico e Integral de Gestão da Informação nas Organizações. 2º Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação, São Paulo, Brasil, 2005. Actas de Conferência Internacional. Consultado em Fevereiro 25, 2014, em http://repositorio-aberto.up.pt/bitstream/10216/13461/2/modelo000071239.pdf>

Sistema [Integral] de Informação Ativo e Permanente

Como foi referido, este modelo deve plasmar as várias componentes do ciclo de gestão: a conceção da plataforma tecnológica (*hardware* e *software*), a produção, circulação, avaliação, armazenamento, disponibilização e preservação da informação, os processos de negócio da organização, o *software* aplicacional, as tecnologias e sistemas de armazenamento da informação (ex.: *data warehouse*), as ferramentas de *data mining,* abarcando as muitas vezes separadas áreas de *Gestão de Documentos*, de *Gestão de Conteúdos e de Gestão de Arquivos*.

Daqui se depreende que não só cada organização deve ter o seu próprio Modelo de Gestão, como a informação *digital* e *analógica* a gerir não é apenas a que está arquivada, mas toda aquela que ainda se encontra em tramitação.

Por outro lado é importante lembrar que gerir informação compreende o garantir que este ativo organizacional mantenha durante todo o seu ciclo de vida, características vitais para a organização: **autenticidade**, **fidedignidade**, **integridade**, **inteligibilidade**, **usabilidade, confidencialidade e disponibilidade.**

2.2. Funções do repositório

Há um conjunto de requisitos fundamentais que devem ser observados para que os repositórios consigam obter a certificação, destacando-se, assim, alguns deles:

- O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, a preservação a longo prazo, a gestão e acesso à informação digital.
- O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório terá no apoio a longo prazo da sua missão.
- O repositório deve 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.
- O repositório deve comprometer-se aos 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.
- O repositório deve ter e manter contratos ou acordos de depósito apropriados para materiais digitais que gere, preserva e/ou aos quais fornece acesso.
- O repositório deve ter mecanismos em vigor para controlar o seu ambiente de preservação.
- O repositório deve identificar e gerir os riscos das suas operações de preservação e os objetivos associados à infraestrutura do sistema.
- O repositório deve manter uma análise sistemática dos fatores de risco de segurança associado a dados, sistemas, pessoal e instalações físicas.

Deve contemplar, igualmente, a criação progressiva de um *Sistema de Gestão [Integrado] de Informação Ativa e Permanente* na CMP**,** capaz de:

- Manter e preservar informação Ativa e Permanente, gerida de forma integrada, independentemente do seu suporte. Implica a existência de uma gestão contínua e integral do ciclo de vida da informação que, desta forma, acompanha a componente orgânica que a usa e/ou cria, sendo, simultaneamente, o reflexo da interatividade informacional da organização. Este sistema permite que a informação esteja sempre acessível, independentemente do seu suporte; inclui igualmente o processo de avaliação da informação, ao longo da sua tramitação; mecanismos e técnicas de controlo do processo de tramitação dos documentos, passando pelas técnicas de autenticação e certificação digital, captura de metainformação (técnica, descritiva, estrutural e de preservação) e a conceção da plataforma tecnológica.

- Fazer face às necessidades de armazenamento seguro, acesso controlado e preservação da informação (documentos digitalizados e nado-digitais) no longo termo.
- Eliminar, progressivamente, situações de caos informacional nos serviços administrativos, associado a situações de:
    - Desconhecimento das normas de organização dos processos, independentemente do suporte dos mesmos [digital e papel], isto é: ordenar, numerar, anexar, apensar, etc.;
    - Deficiente manutenção da informação em tramitação administrativa [digital e papel]: organização, identificação, acondicionamento, etc.;
    - Menor possibilidade de eliminação de documentos, com a mistura de documentos de conservação definitiva com outra de menor importância;
    - Acumulação de massas documentais amorfas e dispersas por vários locais;
    - Falta de espaço crónica sem solução à vista;
    - Desqualificação do processo informacional, por falta de precisão, arrastamento e bloqueio;
    - Dificuldades de pesquisa e acesso (localização) dos documentos [digital e papel];
    - Ignorância dos princípios de comunicabilidade;
    - Eliminações abusivas;
    - Tentativa de transferências descontroladas, despejos ou mero abandono dos documentos [em ambiente digital, não utilização das plataformas definidas ou não cumprimento das boas práticas];
    - Uma administração pouco confiante, que não consegue controlar a informação e que por isso recorre à multiplicação de cópias, cópias de ficheiros, fotocópias, etc.
- Permitir melhorar a **eficiência** ao:
    - Evitar produção de documentos não essenciais (menos volume de papel, menos confusão, menos espaço físico e/ou em servidor);

- Aumentar a utilidade e possibilidades de uso dos documentos (maior densidade informativa);
- Criar a possibilidade de resolver vários assuntos do mesmo processo, em simultâneo, dado o acesso multidirecional;
- Acesso descentralizado à informação;
- Reforçar a segurança ao acesso/comunicabilidade, pela definição de perfis de utilizadores;
- Promover a "desmaterialização" controlada;
- Facilitar o recurso à informática e à digitalização;
- Melhorar o acesso à informação;
- Eliminar o caos informacional;
- Diminuir o tempo gasto no registo;
- Diminuir o tempo gasto na pesquisa e na recuperação da informação;
- Promover a profilaxia da informação, separar documentos de conservação definitiva da outra de menor importância;
- Confiança no sistema, eliminação das duplicações para controlo interno.

2.3. Características do repositório

Infraestrutura tecnológica (*storage*)

Relativamente aos recursos tecnológicos, contempla-se a existência de um *data warehouse*, com a diferenciação de dois repositórios e a adição de *tapes*:

- Repositório transacional – armazenamento da informação que se encontra em tramitação;
- Repositório definitivo – armazenamento da informação arquivada e de conservação definitiva;
- Tapes WORM – possibilitam a reposição da totalidade da informação dos repositórios.

Deverão ainda ser contempladas as aplicações informáticas de controlo dos documentos, como a aplicação de gestão documental e aplicações utilizadas para gestão de documentos arquivados. No caso da CMP, serão o DocInPorto e o GISA, respetivamente. Deverá estar prevista a interoperabilidade entre os vários aplicativos.

No caso da CMP, a plataforma tecnológica assentará no FEDORA, uma vez já ter sido adotada pelo aplicativo GISA, em utilização.

Por sua vez, a estrutura do repositório digital necessitará, de forma global, da criação de alguns mecanismos que contemplam a segurança e preservação da informação, garantindo as suas propriedades (confidencialidade, integridade e disponibilidade):

- Servidor de *masters* (documentos digitais);
- Servidor Web;
- SGBD (Sistema de Gestão de Base de Dados);
- Ligação à Internet;
- *Firewall* para controlo de acessos;
- Largura de banda de acesso à Internet, de forma a garantir o desempenho do sistema;
- *Backup* do sistema, dos *masters* e dos documentos digitais (já comprimidos);
- Cópias de segurança do *backup* do sistema

A Unidade de Arquivo deverá incorporar:

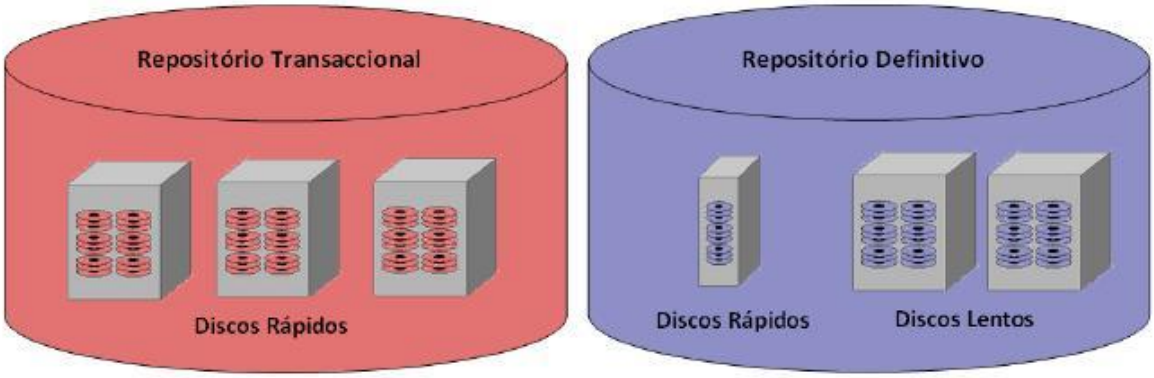
- Três níveis de velocidades de acesso, sendo a mais lenta *tapes* tipo WORM (*Write Once Read Many*), com o objetivo de preservar os ficheiros;
- *Software* de gestão da *storage* para administrar a unidade de arquivo;
- Interfaces com as aplicações através de sistema de ficheiros e/ou API's;
- Os suportes de armazenamento deverão estar distribuídos geograficamente para garantir a disponibilidade da informação em situações de contingência.

Em resumo, os recursos tecnológicos irão englobar:

- Um Data Warehouse;
- As aplicações informáticas: DocInPorto e GISA;

- Aplicativos workflow;
- Aplicativos para captura de metainformação para controlo das digitalizações descentralizadas;
- Aplicativos para captura de metainformação para documentos nado-digitais.

No que diz respeito ao **armazenamento**, e tendo em conta a existência de dois repositórios (transacional e definitivo), a CMP irá utilizar uma arquitetura de *storage* híbrida, constituída por um *Storage Area Network* **(SAN)** e um *Network Attached Storage* **(NAS)**.



Solução de Armazenamento do Repositório Digital da CMP

Um SAN, ou rede de área de armazenamento, "é um tipo de rede de área local (LAN) projetado para lidar com grandes transferências de dados", suportando o seu armazenamento, recuperação e replicação.[2]

Por sua vez, um NAS, "permite que arquivos sejam armazenados e recuperados através de uma rede de computadores", tentando "reduzir o custo associado com os servidores de ficheiros tradicionais".[3]

A diferença entre estes dois tipos de armazenamento, é que, "enquanto os SAN"s tradicionalmente empregam protocolos de rede de baixo nível para transferir blocos de disco, um dispositivo NAS normalmente trabalha através de TCP/IP e pode ser integrado facilmente em redes de computadores domésticos".

[2] Fonte: Compnetworking - http://compnetworking.about.com/od/networkstorage/g/storage_san.htm
[3] Fonte: Compnetworking - http://compnetworking.about.com/od/itinformationtechnology/l/bldef_nas.htm

A opção por uma solução deste tipo prende-se com a necessidade de ter um sistema com discos rápidos para processar a informação em tramitação (no repositório transacional) e para facilitar o acesso à documentação arquivada (no repositório definitivo). Esta terá características de uma solução de tipo SAN.

Para armazenar a informação arquivada, cujo acesso é mais esporádico e sem necessidade de disponibilização imediata, pensa-se vir a utilizar uma solução com discos mais lentos do tipo NAS.

Para além destes está prevista existência de Tapes WORM que possibilitam, em caso de desastre, a reposição da totalidade da informação dos repositórios.

A solução híbrida implementa os *pontos fortes* dos dois sistemas:

- Vários níveis de armazenamento;
- Interoperabilidade;
- Capacidade de expansão;
- Baixo custo relativo;
- Elevado desempenho;
- Elevada disponibilidade.

Este sistema de armazenamento híbrido deverá ter os seguintes componentes:

- Servidor de masters (documentos digitais);
- *Backup* do sistema, dos masters e dos documentos digitais;
- Cópias de segurança do Backup do sistema;
- Três níveis de velocidade de acesso, sendo a mais lenta tapes tipo WORM (Write Once Read Many), com objectivo de preservar os ficheiros;
- software de gestão da *storage* para administrar a unidade de armazenamento;
- interfaces com as aplicações através de sistema de ficheiros e/ou API´s;

O sistema de armazenamento será controlado por uma solução de *hardware*/*software* com as seguintes características:

- Métodos eficientes de integridade dos dados;

- Redução da complexidade dos *backups* e administração dos sistemas de armazenamento;
- Alta performance na pesquisa e na captura de ficheiros;
- Um formato de dados aberto que permita o acesso aos dados ao longo de diferentes evoluções tecnológicas;
- Escalabilidade - possibilitar a expansão da capacidade ao longo do tempo;
- Alto desempenho global;
- Normalizado de acordo com as normas internacionais;
- Independente da plataforma aplicacional;
- Custos de armazenamento comportáveis

2.4. Características dos utilizadores

Os utilizadores finais do sistema são do tipo:

- Administradores;
- Utilizadores (munícipes).

Os Administradores têm acesso total as funcionalidades do *arquivo*, enquanto os Utilizadores não terão acesso às configurações da administração do mesmo.

Os munícipes deverão de ser acompanhados e informados para realizarem a pesquisa no repositório, através do aplicativo próprio, sendo por isso importante que estes tenham conhecimentos básicos a nível de informática.

2.5. Restrições Gerais

O repositório não deve permitir a manipulação de objetos digitais por parte de utilizadores e pessoal não autorizado, limitando-se a função de gestão e alteração dos objetos digitais aos intervenientes envolvidos na sua implementação.

3. Requisitos Específicos

Para a realização da seguinte tabela foi necessário aplicar todos os requisitos compreendidos na norma ISO 16363:2012 ao qual se seguiu uma comparação de correspondência com a tabela de certificação de requisitos do projeto Portico, que foi o primeiro repositório digital certificado por esta normativa, encontrando-se assim as evidências (documentos) que foram avaliados para a certificação deste repositório, assinalados a "azul". Por último foi efetuada uma conformidade relativamente aos Documentos de Suporte à Especificação (DSE) criados no âmbito desta dissertação, permitindo desta forma uma visão mais holística e sistémica de quais os requisitos que o arquivo digital confiável da CMP necessita de cumprir ou elaborar para que possa ser corretamente certificado internacionalmente.

Desta forma, os DSE criados servem como guias de referência para que se estabeleçam os documentos finais para assim se atingir o objetivo da certificação do arquivo digital do município do Porto.

Para uma leitura e compreensão mais inteligível os requisitos foram dispostos conforme se encontram na norma, ou seja, estruturados em 3 grandes secções: **Infraestrutura Organizacional**, **Gestão de Objetos Digitais** e **Infraestrutura e Gestão de Riscos de Segurança,** que por sua vez se encontram subdivididos nos vários aspetos relativos à sua secção.

3.1. Infraestrutura Organizacional

Secção	**3. Infraestrutura Organizacional**	
Aspeto	**3.1 Governança e Viabilidade Organizacional**	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
3.1.1. O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, a retenção a longo prazo, a gestão e acesso à informação em meio digital.	Declaração de missão.	Ver. Mod. DMAG_DSE_RC_Declaração_de_missão
3.1.2. O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório desenvolverá no apoio à sua missão a longo prazo.	Plano Estratégico de Preservação; atas de reuniões.	Ver. Mod. DMAG_DSE_Plano_preservação ou DMAG_DSE_Atas_de_reunião
3.1.2.1. O repositório deve ter um plano de sucessão adequado, planos de contingência, e/ou acordos de custódia, no caso de o repositório deixar de funcionar ou da instituição governamental ou financiadora mudar substancialmente o seu âmbito de atuação.	Plano de Sucessão; Planos de Contingência; Planos de Atividades; Acordos de Custódia; documentos que explicitem a intenção de garantir a continuidade do repositório.	Ver. Mod. DMAG_DSE_Acordo_de_custódia ou DMAG_Plano_de_contingência
3.1.2.2. O repositório deve monitorizar o ambiente organizacional para determinar quando deve acionar o plano de sucessão, os planos de contingência e/ou acordos de custódia.	Políticas, planos, protocolos e documentos de análise financeira; procedimentos de monitorização.	
3.1.3. O repositório deve ter uma Política de Gestão do Acervo ou outro documento que especifique o tipo de informação que irá preservar, manter, gerir e prover o acesso.	Política de Gestão da Coleção; Política de Preservação; missão, visão e objetivos do repositório.	Ver. Mod. DMAG_DSE_Política_de_preservação

Secção	3. Infraestrutura Organizacional	
Aspeto	3.2 Estrutura Organizacional e de Pessoal	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
3.2.1. O repositório deve ter identificado e estabelecido as tarefas/atribuições que precisa executar e deve ter nomeado funcionários com competências e experiência adequadas para as efetivar.	Matriz de funções, competências e responsabilidades dos funcionários; descrições de cada cargo; organograma.	Ver. Mod. DMAG_DSE_Matriz_de_conpetências_e_funções
3.2.1.1. O repositório deve ter identificado e estabelecido as tarefas que precisa realizar.	Plano de recursos humanos; matriz de funções, competências e responsabilidades dos funcionários; descrições de cada cargo.	Ver. Mod. DMAG_DSE_Matriz_de_conpetências_e_funções
3.2.1.2. O repositório deve ter o número adequado de funcionários para apoiar todas as funções e serviços.	Organograma; matriz de funções, competências e responsabilidades dos funcionários.	Ver. Mod. DMAG_DSE_Matriz_de_conpetências_e_funções
3.2.1.3. O repositório deve dispor de um programa de desenvolvimento profissional ativo que providencie pessoal com competências e com oportunidades de desenvolvimento de competências.	Plano de formação; evidências de formações internas e/ou externas; documentação das despesas da formação; cópias dos certificados de formação e acreditação.	Ver. Mod. DMAG_DSE_Plano_de_formação ou DMAG_DSE_Formação_externa

Secção	3. Infraestrutura Organizacional		
Aspeto	**3.3 Responsabilidade Processual e *Framework* de Política de Preservação**		
Requisito		**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
3.3.1. O repositório deve ter definida a sua *comunidade-alvo* e base(s) de conhecimento associada, bem como ter estas definições devidamente acessíveis.		Definição da comunidade-alvo; declaração da missão; acordos de nível de serviço (SLA's) e condições de acesso dos utilizadores/permissões.	Ver. Mod. DMAG_DSE_RC_Declaração_de_missão
3.3.2. O repositório deve ter estabelecidas as Políticas de Preservação para garantir que o seu Plano Estratégico de Preservação será cumprido.		Políticas de Preservação; Declaração de missão.	Ver. Mod. DMAG_DSE_Política_de_preservação ou DMAG_DSE_RC_Declaração_de_missão
3.3.2.1. O repositório deve ter mecanismos de revisão, atualização e desenvolvimento contínuo das Políticas de Preservação, por forma a acompanhar o crescimento do repositório e a evolução da tecnologia e das práticas da comunidade.		Políticas de Segurança; Política de Preservação; Plano Estratégico de Preservação; definição do ciclo de revisão da documentação; procedimentos de monitorização.	
3.3.3. O repositório deve ter documentado o histórico das mudanças nas suas operações, procedimentos, *software* e *hardware*.		Contratos de serviços; documentação de aquisição, implementação, atualização e eliminação de *software* e *hardware*; documentos atuais e obsoletos (versões anteriores) de políticas e procedimentos.	
3.3.4. O repositório deve comprometer-se com os princípios de transparência e prestação de contas em todas as ações de suporte à operação e gestão do repositório que afetam a preservação dos conteúdos digitais ao longo do tempo.		Relatórios de auditorias e certificações técnicas e financeiras; documentação referente aos procedimentos de contratação pública; contratos com outras entidades.	

3.3.5. O repositório deve definir, recolher, controlar e prover, de forma adequada, as medições da integridade da informação.	Procedimentos de monitorização; definição de medidas de integridade do repositório; documentação dos procedimentos e mecanismos para monitorar as medidas de integridade e para responder a resultados de medidas de integridade que indicam que os conteúdos digitais estão em risco.	
3.3.6. O repositório deve comprometer-se com um regular agendamento de autoavaliação e da certificação externa.	Checklists de autoavaliação; preparação para auditoria.	

Secção	**3. Infraestrutura Organizacional**	
Aspeto	**3.4 Sustentabilidade Financeira**	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
3.4.1. O repositório deve ter em vigor processos de planeamento de negócio, de curto e longo prazo, para sustentar o repositório ao longo do tempo.	Relatórios financeiros; orçamentos; procedimentos de auditoria; planos de contingência.	Ver. Mod. DMAG_DSE_Plano_de_contingência
3.4.2. O repositório deve ter práticas e procedimentos financeiros transparentes e compatíveis com relevantes normas e práticas contabilísticas, e auditados por terceiros, de acordo com os requisitos legais territoriais.	Relatórios financeiros; auditoria financeira anual e relatório.	

3.4.3. O repositório deve ter um compromisso contínuo para analisar e informar sobre riscos financeiros, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).	Política de Gestão do Risco; análise de custo-benefício; procedimentos de revisão e monitorização.	

Secção	**3. Infraestrutura Organizacional**
Aspeto	**3.5 Contratos, Licenças e Passivos**

Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
3.5.1. O repositório deve ter e manter contratos ou acordos de depósito adequados aos materiais digitais que gere, preserva, e/ou aos quais fornece acesso.	Acordos de licença ou de depósito; procedimentos de revisão dos contratos.	
3.5.1.1. O repositório deve ter contratos ou acordos de depósito que especificam e transferem todos os direitos de preservação necessários, devendo ser documentados os direitos transferidos.	Acordos de licença ou de depósito; especificação de direitos transferidos para diferentes tipos de conteúdo digital (se aplicável).	
3.5.1.2. O repositório deve ter especificados todos os aspetos relevantes relativos à aquisição, manutenção, acesso e revogação de acordos escritos com os depositantes e outras partes interessadas.	Acordos de licença ou de depósito.	
3.5.1.3. O repositório deve ter políticas que indicam quando aceita a responsabilidade de preservação de conteúdos de cada conjunto de objetos de dados submetidos.	Acordos de licença ou de depósito; recibos de confirmação enviados para o produtor/ depositante.	
3.5.1.4. O repositório deve ter em vigor políticas para abordar a responsabilidade e os desafios em termos de propriedade/direitos.	Políticas e procedimentos de acordo com os requisitos legais; definição de direitos e permissões de produtores e colaboradores.	

3.5.2. O repositório deve controlar e gerir os direitos de propriedade intelectual e restrições ao uso de conteúdos do repositório, como exigido pelo acordo de depósito, contrato ou licença.	Políticas e procedimentos de acordo com os requisitos legais.	

3.2. Gestão de Objetos Digitais

Secção	**4. Gestão de Objetos Digitais**	
Aspeto	**4.1 Ingestão: Aquisição [Entrada, Incorporação] de Conteúdos**	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
4.1.1. O repositório deve identificar o Conteúdo Informacional e as Propriedades da Informação que irá preservar.	Declaração de missão; procedimentos de ingestão de objetos digitais.	Ver. Mod. DMAG_DSE_RC_Declaração_de_missão
4.1.1.1. O repositório deve ter um procedimento(s) para a identificação das Propriedades da Informação que irá preservar.	Política de Preservação; procedimentos de ingestão de objetos digitais.	Ver. Mod. DMAG_DSE_Política_de_preservação
4.1.1.2. O repositório deve ter um registo do Conteúdo Informacional e das Propriedades da Informação que irá preservar.	Política de Preservação; registos do tipo de objetos digitais.	Ver. Mod. DMAG_DSE_Política_de_preservação
4.1.2. O repositório deve especificar claramente a informação que precisa ser associada a conteúdo informacional específico, aquando do seu depósito.	Requisitos de transferência; esquemas de metainformação.	
4.1.3. O repositório deverá ter especificações adequadas e que permitam o reconhecimento e a análise dos SIP (*Submission Information Package*).	Pacote de Informação para os SIP; especificações de formatos de ficheiros; esquemas de metainformação.	

4.1.4. O repositório deve ter mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais.	Registos de procedimentos e autenticações.	
4.1.5. O repositório deve ter um processo de ingestão que verifique a completude e exatidão de cada SIP.	Ficheiros de registo do sistema responsável pelo procedimento de ingestão; procedimentos detalhados.	
4.1.6. O repositório deve obter controlo suficiente sobre os objetos digitais para preservá-los.	Documentos que mostram o nível de controlo físico do repositório e a metainformação associada.	
4.1.7. Durante os processos de ingestão, e em pontos acordados, o repositório deve fornecer respostas adequadas ao produtor/depositante.	Relatórios anuais; fluxos de trabalho.	
4.1.8. O repositório deve ter registos atualizados de ações e processos administrativos que são relevantes para a aquisição de conteúdos.	Conjunto de metainformação ligada aos objetos digitais; registos de decisões e de medidas tomadas.	

Secção	**4. Gestão de Objetos Digitais**	
Aspeto	**4.2 Ingestão: Criação do AIP (*Archival Information Package*)**	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
4.2.1. O repositório deve ter para cada AIP ou classe de AIPs preservada pelo repositório, uma definição associada que é adequada para analisar o AIP e se enquadre nas necessidades de preservação a longo prazo.	Documentação que identifica claramente cada classe de AIP (definição) e a sua implementação no repositório.	
4.2.1.1. O repositório deve ser capaz de identificar qual a definição que se aplica a cada AIP.	Documentação que identifica claramente cada classe de AIP (definição) e a sua implementação no repositório.	

4.2.1.2. O repositório deve ter uma definição de cada AIP que é adequada para a preservação a longo prazo, permitindo a identificação e análise de todos os componentes necessários, dentro desse AIP.	Demonstração da utilização das definições, para extrair informação.	
4.2.2. O repositório deve ter uma descrição de como os AIPs são construídos a partir dos SIPs.	Descrição dos processos; documentação da relação SIP-AIP; documentação clara de como os AIP's são derivados dos SIP.	
4.2.3. O repositório deve documentar a avaliação/eliminação final de todos os SIPs (incluindo 4.2.3.1.).	Registos de eliminação; documentos de descrição do processo; documentação da relação de um SIP com um AIP; documentação clara de como os AIP's são derivados dos SIP.	Ver. Mod. DMAG_DSE_Registo_de_eliminação
4.2.3.1. O repositório deve seguir os procedimentos documentados se um SIP não for incorporado num AIP ou eliminado e deve indicar a razão pela qual o SIP não foi incorporado ou eliminado.		
4.2.4. O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIP (incluindo 4.2.4.1.; 4.2.4.1.1.; 4.2.4.1.2.; 4.2.4.1.3.; 4.2.4.1.4. e 4.2.4.1.5.).	Documentação da nomenclatura e evidência física da sua aplicação (registos).	
4.2.4.1. O repositório deve identificar cada AIP de forma única dentro do repositório.		
4.2.4.1.1. O repositório deve ter identificadores únicos.		
4.2.4.1.2. O repositório deve atribuir e manter identificadores persistentes dos AIP e seus componentes, de modo a ser único dentro do contexto do repositório.		
4.2.4.1.3. A documentação deve descrever todos os processos utilizados para alterações nesses identificadores.		
4.2.4.1.4. O repositório deve ser capaz de fornecer uma lista completa desses identificadores e fazer verificações pontuais para duplicações.		

4.2.4.1.5. O sistema de identificadores deve ser adequado para atender às atuais e previsíveis futuras exigências do repositório, como, por exemplo, número de objetos.		
4.2.4.2. O repositório deve ter um sistema confiável de serviços de ligação/resolução, a fim de encontrar o objeto identificado de forma exclusiva [identificador único e persistente], independentemente da sua localização física.		
4.2.5. O repositório deverá ter acesso a ferramentas e recursos necessários para fornecer Informação de Representação para todos os objetos digitais que contém (incluindo 4.2.5.1.; 4.2.5.2.; 4.2.5.3 e 4.2.5.4.).	Registos de Informação de Representação (incluindo registos de formatos); registos que incluem Informação de Representação e identificadores persistentes para objetos digitais relevantes.	
4.2.5.1. O repositório deverá ter também ferramentas ou métodos para identificar o tipo de ficheiro de todos os Objetos de Dados submetidos.		
4.2.5.2. O repositório deve ter ferramentas ou métodos para determinar que Informação de Representação é necessária para fazer com que cada Objeto de Dados seja compreensível para a *comunidade-alvo*.		
4.2.5.3. O repositório deve ter acesso à Informação de Representação necessária.		
4.2.5.4. O repositório deve ter ferramentas ou métodos para assegurar que a Informação de Representação necessária é persistentemente associada aos Objetos de Dados relevantes.		
4.2.6. O repositório deve ter processos documentados para a aquisição de Informação de Descrição de Preservação (IDP/PDI) para o Conteúdo Informacional associado e adquirir a IDP em conformidade com os processos documentados (incluindo 4.2.6.1.; 4.2.6.2. e 4.2.6.3.).	Definição da ingestão de objetos digitais; documentação sobre a forma como o repositório adquire e gere a Informação de Descrição de Preservação.	
4.2.6.1. O repositório deve ter processos documentados para a aquisição da IDP.		

4.2.6.2. O repositório deve executar os processos documentados para a aquisição da IDP.		
4.2.6.3. O repositório deve assegurar que a IDP é persistentemente associada ao Conteúdo Informacional relevante.		
4.2.7. O repositório deve garantir que o Conteúdo Informacional dos AIP é compreensível para a sua *comunidade-alvo*, no momento da criação do AIP (incluindo 4.2.7.1.; 4.2.7.2. e 4.2.7.3.).	Procedimentos de testes de acesso aos objetos digitais para verificação dos requisitos de acessibilidade, integridade, autenticidade e inteligibilidade.	
4.2.7.1. O repositório deve ter um processo documentado para testar, na sua criação, a inteligibilidade do Conteúdo Informacional dos AIP pela sua *comunidade-alvo*.		
4.2.7.2. O repositório deve executar o processo de teste para cada classe de Conteúdo Informacional dos AIP.		
4.2.7.3. Se falhar o teste de compreensibilidade, o repositório deve trazer o Conteúdo Informacional do AIP ao nível necessário de inteligibilidade.		
4.2.8. O repositório deve verificar a completude e exatidão de cada AIP no momento em que é criado.		
4.2.9. O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção/conteúdo do repositório.	Verificações de integridade dos dados; documentação que identifica claramente cada classe de objetos digitais.	
4.2.10. O repositório deve ter registos atualizados de ações e processos administrativos que são relevantes para a criação do AIP.	Registo da metainformação de preservação, armazenada e ligada aos objetos digitais; documentação sobre as decisões e ações tomadas.	

Secção	4. Gestão de Objetos Digitais	
Aspeto	4.3 Planeamento de Preservação	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
4.3.1 O repositório deve ter documentadas estratégias de preservação relevantes para a sua coleção/conteúdo.	Estratégias de Preservação de objetos digitais.	
4.3.2. O repositório deve ter implementados mecanismos para controlar o seu ambiente de preservação.	Inquéritos à comunidade-alvo.	
4.3.2.1. O repositório deve ter mecanismos de monitorização e notificação quando a Informação de Representação é inadequada para a *comunidade-alvo* entender a informação armazenada.	Serviço de registo da Informação de Representação.	
4.3.3. O repositório deve ter mecanismos para alterar os seus planos de preservação, em resultado das atividades de monitorização desenvolvidas.	Atualização das Políticas e Planos de Preservação; definição do período de atualização (não superior a 5 anos).	
4.3.3.1. O repositório deve ter mecanismos para criar, identificar ou recolher qualquer Informação de Representação adicional que seja necessária.	Planos de Preservação; serviço de registo de formatos.	Ver. Mod. DMAG_DSE_Plano_de_preservação
4.3.4. O repositório deve fornecer evidências da eficácia das suas atividades de preservação.	Esquemas de metainformação de preservação adequados; prova de usabilidade de objetos digitais selecionados aleatoriamente dentro do sistema.	

Secção	4. Gestão de Objetos Digitais		
Aspeto	4.4 Preservação dos AIPs		
Requisito		**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
4.4.1. O repositório deverá ter especificações de como os AIPs são armazenados até ao nível do bit.		Estratégias de armazenamento de objetos digitais.	
4.4.1.1. O repositório deve preservar o Conteúdo Informacional dos AIPs.		Workflows de preservação; Política de Preservação; estratégias de armazenamento e de migração/conversão dos objetos digitais.	Ver. Mod. DMAG_DSE_Política_de_preservação
4.4.1.2. O repositório deve monitorizar ativamente a integridade dos AIPs.		Verificações de integridade dos dados.	
4.4.2. O repositório deve ter registos atualizados de ações e processos administrativos que são relevantes para o armazenamento e preservação dos AIPs.		Registo da metainformação de preservação, armazenada e ligada aos objetos digitais; documentação sobre as decisões e ações tomadas.	
4.4.2.1. O repositório deve ter procedimentos para todas as ações realizadas nos AIPs.		Documentação sobre as ações que podem ser executadas contra um AIP, erros e anomalias e procedimentos de monitorização.	
4.4.2.2. O repositório deve ser capaz de demonstrar que as ações realizadas nos AIP eram conformes às especificações dessas ações.		Registo da metainformação de preservação, armazenada e ligada aos objetos digitais.	

Secção	4. Gestão de Objetos Digitais	
Aspeto	4.5 Gestão da Informação	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
4.5.1. O repositório deve especificar os requisitos mínimos de informação para permitir que a *comunidade-alvo* possa descobrir e identificar o material de interesse.	Informação Descritiva e metainformação.	
4.5.2. O repositório deve capturar ou criar o mínimo de informação descritiva [metainformação descritiva] e assegurar que está relacionada com o AIP.	Documentação da relação entre o AIP e a sua Informação Descritiva; identificadores persistentes; documentação do sistema e arquitetura técnica; verificações de integridade dos dados; esquemas de metainformação.	
4.5.3. O repositório deve manter uma ligação bidirecional entre cada AIP e a sua Informação Descritiva.	Documentação da relação entre o AIP e a sua Informação Descritiva; identificadores persistentes; documentação do sistema e arquitetura técnica; verificações de integridade dos dados.	
4.5.3.1. O repositório deve manter as associações entre os seus AIPs e a respetiva metainformação descritiva ao longo do tempo.	Documentação da relação entre o AIP e a sua Informação Descritiva; identificadores persistentes; documentação do sistema e arquitetura técnica; verificações de integridade dos dados.	

Secção	4. Gestão de Objetos Digitais	
Aspeto	4.6 Gestão de Acessos	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
4.6.1. O repositório deve cumprir as Políticas de Acesso.	Políticas de Acesso aos objetos digitais; matrizes de autenticação	
4.6.1.1. O repositório deve registar e analisar todas as falhas de gestão de acesso e anomalias.	Registo de falhas de acesso; procedimentos de monitorização; ferramentas de notificação em caso de problemas/anomalias.	
4.6.2. O repositório deve seguir as políticas e procedimentos que permitem a disseminação de objetos digitais que são rastreáveis até aos originais, com provas da sua autenticidade.	Políticas de Acesso aos objetos digitais.	
4.6.2.1. O repositório deve registar e atuar sobre os relatórios de problemas/erros nos dados ou respostas dos utilizadores.	Relatórios de erros e ações tomadas; procedimentos e instruções de trabalho.	

3.3. Infraestrutura e Gestão de Riscos de Segurança

Secção	5. Infraestrutura e Gestão de Riscos de Segurança	
Aspeto	5.1 Gestão de Riscos da Infraestrutura Técnica	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**

5.1.1. O repositório deve identificar e gerir os riscos das suas ações de preservação e os objetivos associados à infraestrutura do sistema.	Procedimentos de avaliação da infraestrutura tecnológica; componente de exportação de registos autênticos para um sistema independente.	
5.1.1.1. O repositório deve utilizar sistemas de notificação de monitorização de tecnologia.	Relatórios de avaliação/monitorização de tecnologia.	
5.1.1.1.1. O repositório deve ter tecnologias de *hardware* apropriadas para os serviços que presta à sua *comunidade-alvo*.	Procedimento de manutenção de *hardware*; manutenção de um inventário de *hardware* atual.	
5.1.1.1.2. O repositório deve ter procedimentos para monitorizar e receber notificações quando se tornam necessárias mudanças tecnológicas ao nível do *hardware*.	Procedimento de monitorização às alterações de *hardware*.	
5.1.1.1.3. O repositório deve dispor de procedimentos para avaliar quando são necessárias mudanças do *hardware* em utilização.	Procedimentos de avaliação do *hardware*.	
5.1.1.1.4. O repositório deve ter procedimentos, compromisso e financiamento para substituir o *hardware* quando a avaliação aponta para a necessidade de o fazer.	Evidência de ativos financeiros em curso reservados para aquisição de *hardware*; demonstração de redução de custos através de custo amortizado de um novo sistema.	
5.1.1.1.5. O repositório deverá ter tecnologias de *software* apropriadas para os serviços que fornece à *comunidade-alvo*.	Procedimento de manutenção de *software*; manutenção de um inventário de *software* atual.	
5.1.1.1.6. O repositório deve ter procedimentos para monitorizar e receber notificações quando são necessárias alterações de *software*.	Procedimento de monitorização às alterações de *software*.	
5.1.1.1.7. O repositório deve dispor de procedimentos para avaliar quando as mudanças são necessárias para o *software* em atualização.	Procedimentos de avaliação do *software*.	

5.1.1.1.8. O repositório deve ter procedimentos, compromisso e financiamento para substituir *software* quando a avaliação indica a necessidade de o fazer.	Evidência de ativos financeiros em curso reservados para aquisição de *software*; demonstração de redução de custos através de custo amortizado de um novo sistema.	
5.1.1.2. O repositório deve ter um adequado suporte de *hardware* e *software* para funcionalidades de *backup* suficientes para preservar o conteúdo do repositório e controlar as funções do repositório.	Política de backups; planos de recuperação de desastres; testes de backups.	Ver. Mod. DMAG_DSE_Política_backups ou DMAG_DSE_Plano_recuperação_desastres
5.1.1.3. O repositório deve ter mecanismos eficazes para detetar a corrupção ou perda de bits.	Análise de risco; relatórios de erros e incidentes; análise da integridade dos objetos digitais.	
5.1.1.3.1. O repositório deve registar e reportar à respetiva gestão, todos os incidentes de corrupção ou perda de dados, devendo ser tomadas medidas para reparar/ substituir dados corrompidos ou perdidos.	Procedimentos relativos à notificação de incidentes para os administradores; metainformação de preservação (por exemplo, DIP); rastreio de fontes de incidentes.	
5.1.1.4. O repositório deve ter um processo para registar e reagir à disponibilização de novas atualizações de segurança com base numa avaliação de risco-benefício.	Processo de registo de riscos e avaliação de atualizações de *software*; documentação referente às instalações de atualização.	
5.1.1.5. O repositório deve ter definidos processos de substituição de suportes de armazenamento e/ou alteração de *hardware* (por exemplo, refrescamento, migração).	Processos de mudança de suportes de armazenamento e alteração de *hardware*.	
5.1.1.6. O repositório deve ter identificados e documentados processos críticos que afetam a sua capacidade de cumprir com as suas responsabilidades obrigatórias.	Matriz de rastreabilidade entre processos críticos e requisitos obrigatórios.	
5.1.1.6.1. O repositório deve ter documentado um processo de gestão da mudança que identifique nos processos críticos alterações que afetam, potencialmente, a capacidade do repositório cumprir com as suas responsabilidades obrigatórias.	Registo de gestão de alterações na mudança de processos críticos; avaliação de riscos.	

5.1.1.6.2. O repositório deve ter um processo para testar e avaliar o efeito das mudanças nos processos críticos do repositório.	Procedimentos de teste; documentação de resultados anteriores e avaliação/análise do impacto de alterações em processos críticos.	
5.1.2. O repositório deve gerir o número e a localização das cópias de todos os objetos digitais.	Testes de validação da existência do objeto para cada localização registada e no sistema de armazenamento.	
5.1.2.1. O repositório deve ter implementados mecanismos para assegurar que quaisquer/múltiplas cópias de objetos digitais são sincronizadas.	Workflows de sincronização; procedimentos de sincronização.	

Secção	**5. Infraestrutura e Gestão de Riscos de Segurança**	
Aspeto	**5.2 Gestão de Riscos de Segurança**	
Requisito	**Documentos [assinalam-se a azul as evidências (Documentos) PORTICO]**	**Conformidade**
5.2.1. O repositório deve manter uma análise sistemática dos fatores de risco de segurança associados a dados, sistemas, pessoal e instalações físicas.	Análise de risco; emprego das normas da família ISO 27000.	
5.2.2. O repositório deve ter implementados controlos para tratar adequadamente cada um dos riscos de segurança definidos.	Lista de controlos do sistema; análise de risco; emprego das normas da família ISO 27000 (em particular, a ISO 27002 - boas práticas relativas à gestão da segurança da informação).	

5.2.3. A equipa do repositório deve ter bem delimitados os papéis, responsabilidades e autorizações relacionadas com a implementação de mudanças no sistema.	Organograma; emprego das normas da família ISO 27000 (em particular, a ISO 27002).	
5.2.4. O repositório deve ter um adequado plano(s) escrito de preparação e recuperação de desastres incluindo, pelo menos, um *backup off-site* de toda a informação preservada, assim como uma cópia *off-site* do(s) plano(s) de recuperação.	Planos de recuperação em caso de desastre; planos de continuidade; emprego das normas da família ISO 27000 (em particular, a ISO 27002).	Ver. Mod. DMAG_DSE_Plano_recuperação_desastres ou DMAG_DSE_Plano_de_continuidade

4. Apêndice

4.1. Pressupostos e dependências

No que respeita à seleção da Plataforma Tecnológica, a CMP optou por selecionar a plataforma FEDORA.

O FEDORA é uma estrutura conceptual que usa um conjunto de abstrações sobre a informação digital, constituindo a plataforma para sistemas de software de gestão de informação digital. No caso da CMP os aplicativos responsáveis pela gestão dessa informação estarão ambos integrados com esta plataforma.

Desta forma podemos considerar o FEDORA como sendo uma dependência do repositório pois é um *software* flexível que suporta diversos formatos de objetos digitais, que tem a possibilidade de ser utilizado como suporte para outras aplicações.

Podem ocorrer situações em que os documentos, apesar de estarem acessíveis, têm uma comunicabilidade condicionada. Noutros casos, os documentos não tem restrições de comunicabilidade mas a fragilidade do seu suporte físico não permite o acesso ao original.

A criação de um Arquivo Digital facilita e potencia exponencialmente o acesso descentralizado à informação, de forma assíncrona e multidireccionada, quer pela consulta de originais (nado-digitais), quer por cópias (digitalizações), quer ainda pela consulta da metainformação descritiva associada, pelo que a *comunicabilidade* dos documentos deve ser atentamente avaliada.

Desta forma, torna-se necessário conhecer e articular a legislação[4] que regulamenta o *Direito à Informação,* sem negligenciar a Proteção da privacidade e segurança do Estado e das Pessoas (individuais ou coletivas) e os Direitos de Autor. É também importante ter presente as implicações legais, que alteram, entre um documento administrativo no serviço que o produziu e o mesmo documento à guarda do Serviço de

[4] Constituição da República Portuguesa – Administração Pública – Direitos e Garantias dos administrados (art.268ª) Código Civil Português – Direitos de personalidade (75ºa 80º); Código Procedimento Administrativo – Direito à informação (Art.º 61º a 65º); Lei Acesso aos Documentos Administrativos (LADA – Lei 46/2007 de 24.08); Código do Direito de Autor e dos Direitos Conexos (Lei 50/2004, de 24.08); Lei da Proteção de Dados Pessoais (LPDP - Lei 67/98 de 26.10); Regime Geral dos Arquivos e do Património Arquivístico (Lei 16/93 de 23.01).

Arquivo.

4.2. Definições, acrónimos e abreviaturas

CMP	Câmara Municipal do Porto
DSE	Documentos de Suporte à Especificação
FEDORA	Flexible Extensible Digital Object and Repository Architecture
GI	Gestão de Informação
GISA	Gestão Integrada de Sistemas de Arquivo
NAS	Network Attached Storage
SAN	Storage Area Network
SI-AP	Sistema [Integral] de Informação Ativa e Permanente

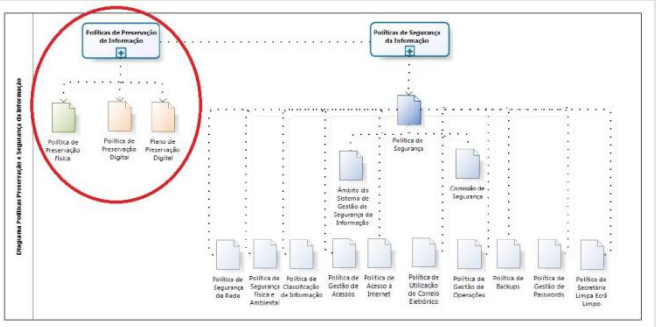
Anexo 6: Poster da dissertação apresentado nas XII Jornadas de Ciência da Informação em 19 de Maio de 2014

A Preservação da Informação: um contributo para a implementação de um Arquivo Digital Certificável no Município do Porto

Dissertação em ambiente empresarial – Câmara Municipal do Porto (CMP)

Contextualização

Este projeto situa-se no âmbito da definição da Estratégia e Políticas de Gestão da Informação, direcionando-se especificamente à Preservação e Segurança da Informação, com especial enfoque no meio digital e na operacionalização do Arquivo Digital Certificado.

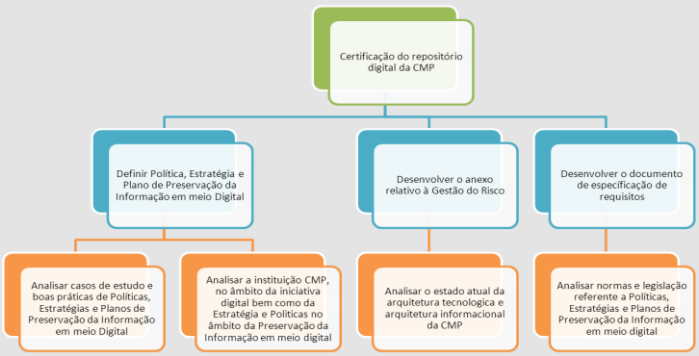


Problema/Necessidade

O problema apresentado situa, este projeto na área de estudos da Gestão da Informação, no âmbito da preservação da informação em meio digital, num contexto de certificação do repositório digital da CMP.

Como referência de investigação suportamo-nos no paradigma cientifico-informacional e os conceitos que o mesmo implica, pelo que partimos da formulação da seguinte questão: **Quais os procedimentos e requisitos a estabelecer tendo em vista a criação de um Repositório Digital Confiável, que garanta os atributos de autenticidade, integridade, inteligibilidade e de preservação da informação no longo prazo?**

Objetivos

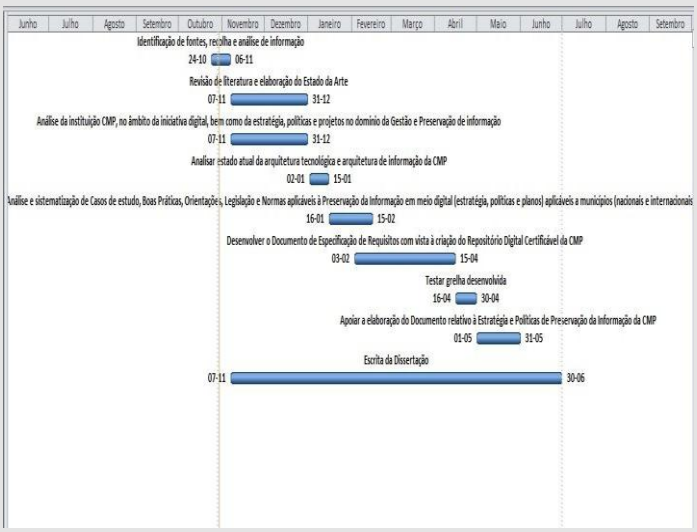


Metodologia

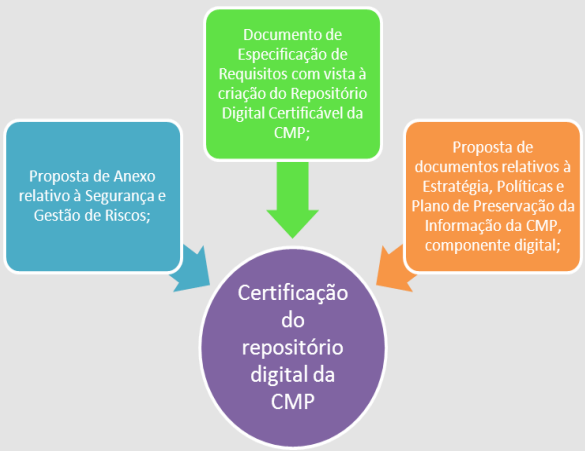
O Método Quadripolar serve para enquadrar e orientar tanto o trabalho como a dinâmica de pesquisa a realizar, com uma constante interação dos 4 pólos.

Será desenvolvida, a metodologia da investigação-ação dada a forma interativa como se desenvolve e permite a produção de saberes ao longo de todo o processo e a todo o grupo participativo.

Plano de Trabalho



Resultados Esperados



Universidade do Porto FEUP Faculdade de Engenharia
PORTO Câmara Municipal
Hugo Azevedo Oliveira (mci12011@fe.up.pt)
mci Mestrado em Ciência da Informação
U.PORTO FACULDADE DE LETRAS UNIVERSIDADE DO PORTO