GESTÃO DA INFORMAÇÃO: do modelo de segurança e preservação ao repositório confiável

INFORMATION MANAGEMENT: from the security and preservation model to trusted repository

Paula Maciel Carvalho de Sousa

Resumo: Em plena Era da Informação, as Tecnologias de Informação e Comunicação (TIC) assumem um papel preponderante nas atividades de qualquer organização. Destacam-se, por isso, a segurança e a preservação da informação. Precisamente numa altura em que a informação em meio digital assume cada vez maior importância, torna-se necessário repensar as tradicionais abordagens. Assim, pretende-se, com este artigo abordar a temática do "desafio digital" e as questões que suscita em torno da autenticidade, integridade, fidedignidade, confidencialidade, disponibilidade, inteligibilidade e usabilidade da informação, colocando o foco na Gestão da Informação (GI). Apresentam-se, ainda, alguns dos resultados do estudo desenvolvido em 2013 congregando a Gestão do Sistema de Informação (SI) e a Gestão de Serviço de TI numa autarquia, nomeadamente a proposta de bases para um *Modelo de Segurança e Preservação da Informação*, indissociável do objetivo estratégico de *certificação do repositório de informação organizacional* e da operacionalização da ISO 16.363:2012, cuja "*Checklist* para um Repositório Digital Confiável" se traduziu e apresenta em anexo.

Palavras-chave: Gestão da Informação; Segurança da Informação; Preservação da Informação; ISO 16.363:2012

Abstract: In the Information Age, Information and Communication Technologies (ICT) play a major role in the activities of any organization. It is noteworthy, therefore, the safety and preservation of information. Precisely at a time when digital information is gaining increasing importance, it becomes necessary to rethink traditional approaches. Thus, it is intended with this article to address the theme of "digital challenge" and the issues it raises about authenticity, integrity, reliability, confidentiality, availability, comprehensibility and usability of information, placing the focus on Information Management (IM). It is also presented some results of the study conducted in 2013 by pooling the Information System Management (ISM) and IT Service Management in a municipality, namely the proposed basis for a *Model of Information Security and Preservation*, inseparable from the strategic objective of the *organizational information repository certification* and the ISO 16.363:2012 operationalization, whose "Checklist for Trusted Digital Repository" is translated and presented in Annex.

Keywords: Information management; Information security; Information preservation; ISO 16.363:2012

Gestão da Informação: do modelo de segurança e preservação ao repositório confiável[1]

Introdução

Face ao exponencial crescimento da informação em formato *digital*, que coloca cada vez mais desafios à Gestão da Informação (GI), reforça-se a necessidade de assegurar uma correta e eficaz Gestão da Segurança e da Preservação da Informação (GSPInf) no decurso da atividade das instituições e demais organizações.

[1] Artigo que apresenta e desenvolve algumas das propostas que integram a dissertação defendida publicamente na Faculdade de Engenharia da Universidade do Porto em outubro de 2013: SOUSA, Paula Maciel Carvalho de – *Segurança e preservação da informação: um modelo para os Municípios*. Porto, 2013. Dissertação de Mestrado em Engenharia de Serviços e Gestão: Orientador da FEUP, António Brito; coorientadora da FLUP, Maria Manuela Pinto; orientador da CMP, Alexandre Sousa.

Desta forma, a conceção de um Repositório Digital, ou Arquivo Digital, confiável e perspetivado para o longo prazo, configura-se cada vez mais como um passo decisivo nesse sentido, exigindo a adoção de uma abordagem sistémica e integrada, no âmbito de uma Gestão da Informação organizacional teoricamente sustentada, que abarque todo o ciclo de vida da informação e na qual se assuma a função de Preservação e de Segurança como suas variáveis incontornáveis.

Convém, ainda, ressaltar a importância deste tema, enquadrando-o no quadro legislativo atual, no qual se destaca, a nível internacional a iniciativa da *Agenda Digital para a Europa,* enquadrada na Estratégia Europeia EU 2020, e que pretende prosseguir as políticas europeias no âmbito da Sociedade da Informação. Da revisão efetuada em 18 de dezembro de 2012, resultaram sete prioridades para a economia e sociedade digitais, através das quais se pretende um "aumento do investimento nas tecnologias da informação e da comunicação (TIC), a melhoria das qualificações digitais dos trabalhadores, a abertura do setor público à inovação e a reforma das condições quadro da economia da Internet"[2].

Neste sentido, a Câmara Municipal do Porto (CMP), enquanto instituição que integra a Administração Local, procura responder a este desafio avançando, entre outras medidas, para a criação do seu Arquivo Digital Certificável, com vista a garantir a produção, armazenamento, uso e disponibilização de informação confiável, autêntica, fidedigna, íntegra e inteligível.

Como principais instrumentos orientadores da operacionalização exigida ao nível da *segurança da informação*, identifica-se a ISO/IEC 27.001:2005; ao nível da *gestão de serviços de TI*, as boas práticas ITIL e a ISO/IEC 20.000:2005; e ao nível da *preservação da informação*, a ISO 14.721:2012 – *Space data and information transfer systems – Open Archival Information System – Reference Model,* a ISO/TR 18.492:2005 – *Long-term preservation of electronic document-based information* e a ISO 16.363:2012 – *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*[3].

A estes instrumentos acrescem-se as referências de casos de boas práticas, nomeadamente as orientações identificadas e sistematizadas por outros municípios e instituições no âmbito dos "tradicionais" serviços de informação, enquadrando este referencial normativo e experiência acumulada com uma base teórica, sustentada na Ciência da Informação (CI) e na área transversal da GI, que lhes confere a imprescindível base de conhecimento científico e organizacional que orientará a ação.

Conceitos e relevância da temática na Era da Informação

A informação é encarada, atualmente, como um dos ativos de maior valia numa organização, isto é, uma fonte de vantagem estratégica.

[2] ANACOM (2013) - *Comissão Europeia define prioridades digitais para 2013-2014.* [Em linha]. Disponível em: http://www.anacom.pt/render.jsp?contentId=1148610

[3] Norma que resulta da revisão da anterior *checklist* do TRAC. AMBACHER, B. U. A. - *Trustworthy Repositories Audit & Certification: criteria and checklist (TRAC)*. Chicago: CRL Center for Research Libraries, 2007. [Em linha]. [Consult. 15 jan. 2014]. Disponível em: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

A concentração de esforços relativa à segurança e à preservação da informação é uma condição *sine qua non* para se assegurar que as organizações estabeleçam eficazmente as suas linhas de ação, objetivos, missão e estratégia.

Frequentemente constata-se a utilização de alguns conceitos que, pela sua pertinência e por serem alvo de ambiguidade, necessitam de ser clarificados.

Destaca-se, neste caso, o conceito de **Sistema de Informação (SI)** que de acordo com Silva (2006), 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". Referencia, pois, a informação produzida, recebida e acumulada pela organização.

Por sua vez **Sistema de Tecnologia de Informação (STI)** constitui a designação vulgarmente atribuída aos "sistemas informáticos"/"sistemas de informação". Segundo Pinto (2009), 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".

É, por isso, visível uma proximidade que afirma a importância das Tecnologias de Informação na Gestão da Informação e de uma parceria que não pode ser confundida com substituição ou sobreposição.

Na perspetiva da Ciência da Informação, e de acordo com Silva e Ribeiro (2002), a informação, enquanto fenómeno e processo humano e social, é definida como sendo o "conjunto estruturado de representações mentais [e emocionais] codificadas (símbolos significantes) socialmente contextualizadas e passíveis de serem registadas num qualquer suporte material (papel, filme, banda magnética, disco compacto, etc.) e, portanto, comunicadas de forma assíncrona e multidirecionada".

Por sua vez, o conceito de **Gestão da Informação** encontra-se diretamente ligado com o **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).

Contudo e, como observa Pinto (2005), não basta possuir e gerir os meios eletrónicos de captura/produção, processamento, armazenamento e disponibilização de informação; possuir/gerir recursos de informação; disponibilizar e gerir informação. É fundamental o planeamento estratégico da tecnologia e da produção da informação; o planeamento da administração do sistema, dos sistemas de segurança, o acesso multinível e através de diferentes meios e suportes, o controle e avaliação de tempos de acesso e recuperação da informação e conhecer, avaliar e planear a estrutura produtora de informação/atores, os processos de negócio/produção de informação, os consumidores/clientes, o ambiente interno e externo da organização.

Atualmente, impera o desafio da gestão da informação em meio digital, predominando as questões em torno da obsolescência tecnológica, independentemente do seu nível (*hardware*, *software*, isto é, suportes de armazenamento, formatos, etc.). Este problema levanta duas questões que se prendem com (PINTO, 2010):

- 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.

Com a problemática que o meio digital impõe relativamente ao armazenamento, recuperação e acesso da informação, a **Gestão da Informação** tem que ser assumida em duas perspetivas (Pinto, 2013):

1. a **informacional**, isto é, como uma área-chave na Organização/Instituição abarcando e integrando no ciclo de gestão todo o ciclo de vida da informação;
2. a **organizacional**, tendo como referente os três principais vetores da Organização: os **processos**, as **pessoas** e a **tecnologia**.

Assim sendo, o desafio da criação de um Repositório/Arquivo Digital vai para além da *tecnologia*, envolvendo, igualmente, a *organização*, os seus *atores* e *processos*.

Pinto e Silva (2005), perspetivando a gestão do sistema de informação, 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". Neste pressuposto configuram o **modelo teórico de base sistémica SI-AP (Sistema de Informação – Ativa e Permanente)** que orientará a Organização e os seus colaboradores no processo de adequação da gestão da informação com vista à sua transformação, desde logo, numa organização "aprendente" e, posteriormente, numa "organização inteligente".

Políticas, Avaliação da Segurança da Informação e Estratégias de Preservação

Neste contexto, destaca-se o papel atribuído às Políticas, num enquadramento que se pretende estruturado e integrador da ação ao nível do SI e do STI.

No âmbito que despoletou o estudo desenvolvido, a segurança da informação e os serviços TI, as "políticas" reportam-se a um conjunto de práticas que devem orientar de forma a salvaguardar a informação de eventuais ataques, vulnerabilidades, ameaças ou riscos. Citando Zúquete (2008), "as **políticas de segurança** definem fundamentalmente requisitos de segurança que devem ser respeitados para garantir um determinado resultado". A ISO/IEC 27.003 (2010) define política como sendo "uma declaração de intenção e direção como formalmente expresso pela gestão".

A *Política de Segurança* é o documento por excelência que define, em linhas gerais, as regras de segurança. Define-se como sendo um conjunto de procedimentos, princípios, normas e diretrizes que explicitam os requisitos do negócio, e que regula a proteção e salvaguarda da informação e recursos da organização. Deve estar alinhada com a Gestão de Risco de forma a garantir o seu controlo e avaliação, bem como ser revista de acordo com a periodicidade definida, de forma a assegurar a sua adequação.

Figura 1 – Hierarquia de Politicas (Fonte ISO/IEC 27003:2010)

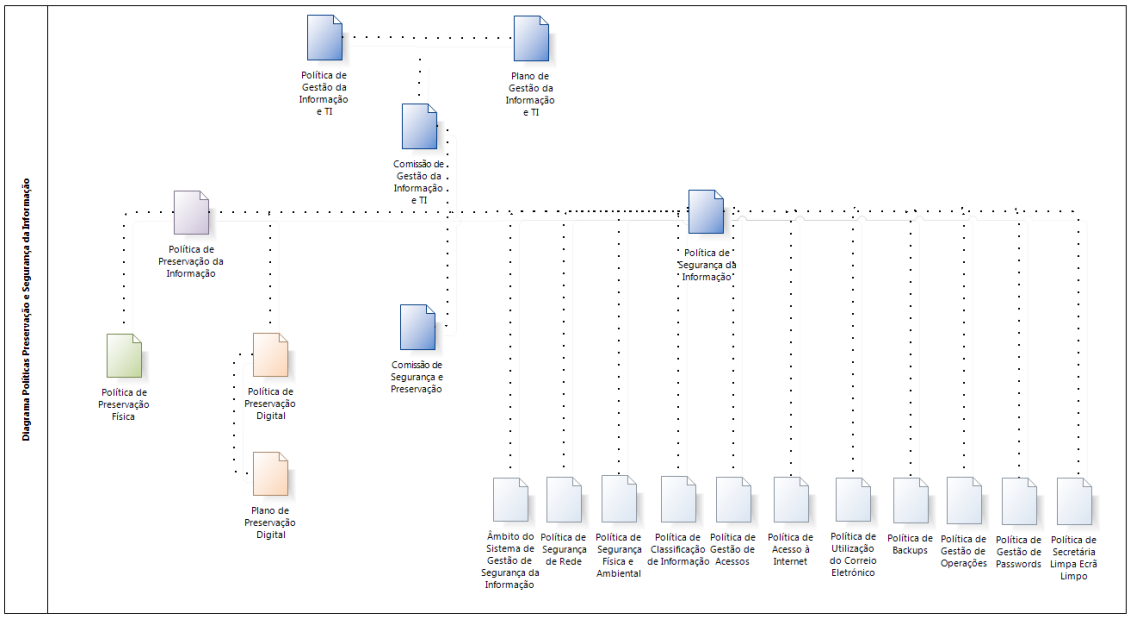
No entanto, as questões suscitadas pela segurança da informação colocam-se a outros níveis e, para serem efetivamente asseguradas, têm que ser equacionadas proporcionalmente à importância da informação, como ativo crucial em qualquer organização, e refletir o seu papel, presença e requisitos ou atributos que lhe são exigidos no seio e fora da Organização que a produz, recebe e acumula.

Importa, pois, pensar também em aspetos como a **autenticidade**, a **integridade,** a **acessibilidade continuada,** a **preservação a longo prazo** e, ainda, a **inteligibilidade**. Por isso, algumas normas (ISO/IEC 27.001:2005, ISO 14.721:2012 e ISO 16.363:2012) são contributos operacionais fundamentais para a preparação do processo de implementação e manutenção do Arquivo/Repositório Digital, nomeadamente no que diz respeito à salvaguarda da proteção da informação em formato digital e à garantia do acesso à mesma, particularmente nos documentos que se encontram autenticados digitalmente (por exemplo, através do Cartão do Cidadão).

A sua utilização deve ser assumida em termos de complementaridade. No que diz respeito às normas relativas à segurança da informação, "não têm em conta os componentes organizacionais, procedimentais e de preservação necessários para a gestão a longo-termo dos recursos digitais" (ISO, 2012). Por sua vez, a ISO 14.721 "providencia um modelo de referência ou *framework* de alto nível, identificando os participantes na preservação digital, os seus papéis e responsabilidades, e os tipos de informação a serem trocados durante o curso do depósito e ingestão em disseminação a partir de um repositório digital" (ISO, 2012).

No diagrama ilustrado na Figura 2, 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*.

Figura 1 – Estrutura de Políticas (Preservação e Segurança de Informação)



Políticas de Preservação de Informação

Ultimamente tem-se assistido a uma maior divulgação de normas e boas práticas relativas à preservação da informação em meio digital, pelo interesse e complexidade que esta suscita.

Desta forma, os esforços vão no sentido de contemplar políticas e processos relativos à preservação e acesso continuado à informação a que também tentam não ficar alheias as instituições de cariz mais tradicional que incorporam na sua Missão a preservação e a conservação, o que se reflete nos instrumentos orientadores que vão produzindo.

Barbedo, et al. (2010) referem que "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".

Numa perspetiva teoricamente sustentada da Gestão da Informação, e para a estruturação de um SI-AP, este processo terá que integrar, a par de outros, as ações planeadas, aprovadas e consignadas nas *Políticas de Gestão da Informação* da Organização em que essa colaboração é um pressuposto base para a Gestão da Informação, acompanhando todas as fases do ciclo de vida da informação e todos os processos, atores, tecnologias e planos operacionais sejam eles de digitalização, de construção dos pacotes de submissão da informação para o repositório digital ou do inerente plano de preservação. Este posicionamento exige a parceria e atuação articulada do Serviço de Informação e do Serviço de Informática que, no caso em análise, conduziu não só a respostas às solicitações de suporte mas à abordagem conjunta da problemática

da segurança da informação com a da preservação da informação, bem como à perspetivação do seu desenvolvimento, implementação e manutenção por uma equipa multidisciplinar.

Em alinhamento com as referidas Políticas, deve ser definida a *Política de Segurança e Preservação da Informação* (PSPI) corporizando duas linhas de atuação interligadas e que respondam às especificidades de cada âmbito.

O estudo desenvolvido, tendo sido suscitado pela necessidade de atuar no âmbito da segurança da informação, foi precisamente redirecionado por força do trabalho em parceria dos setores referenciados, tendo ficado evidente a necessidade de abarcar holisticamente as áreas indissociáveis da *segurança da informação* e da *preservação da informação,* tendo, no entanto, sido conferida uma atenção particular à primeira, ficando a segunda para uma abordagem que já se encontra em curso.

Políticas de Segurança de Informação

A gestão da Segurança da Informação é um processo essencial e imprescindível, sobretudo numa sociedade como a atual em que nos deparamos com a produção exponencial de informação em meio digital. É, por isso, necessária a elaboração de um conjunto de políticas de suporte que são essenciais para a observação dos três princípios básicos da segurança da informação: a confidencialidade, a integridade e a disponibilidade.

A este nível as políticas devem seguir a estrutura aconselhada pela ISO/IEC 27.003:

- **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 possibilitam a análise, identificação e tratamento de ameaças e riscos, potenciando um maior controlo e prevenção sobre as mesmas.

Sob a monitorização da *Comissão de Segurança e Preservação da Informação* (CSPI), contribuir-se-á para a estruturação de um *Sistema de Gestão da Segurança e Preservação da Informação* (SGSPI) com base num conjunto de documentos essenciais a saber: *Política de Segurança da Informação; Âmbito do SGSPI; Política de Classificação*

da Informação; Política de Gestão de Acessos; Política de Gestão de Passwords; Política de Utilização do 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.

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 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.

Deve ser igualmente produzido o documento que defina o **Âmbito do SGSPI**. Uma vez que a implementação de um SGSPI se reveste de um caráter complexo, é boa prática a definição de um âmbito mais reduzido, numa primeira fase, de forma a facilitar os procedimentos a levar a cabo durante este processo.

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.

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. 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.

A **Política de *Backups*** define o conjunto de procedimentos a levar a cabo para se salvaguardar os sistemas de informação.

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.

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.

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.

No que respeita à Preservação da Informação, enunciaram-se os traços gerais de atuação aos vários níveis.

Políticas de Preservação da Informação e Política de preservação em meio digital

No que concerne às Políticas de Preservação da Informação, assiste-se a uma subdivisão entre uma Política de Preservação Física e uma Política de Preservação Digital, seguida dos respetivos Planos de Preservação.

A **Política de Preservação Física** coloca o foco no suporte material/plataforma em que a informação é registada/armazenada, "analógico" e/ou digital.

No que diz respeito à preservação em meio digital, é essencial avaliar a informação neste meio e, deste modo, elaborar uma estratégia que defina as ações necessárias de preservação envolvendo as várias dimensões a preservar (PINTO, 2009). Assim, a **Estratégia de Preservação Digital** deve incluir (THE NATIONAL ARCHIVES, [20--?]a):

- um meio formal de aceitação de unidades informacionais, incluindo uma norma acordada para formatos de arquivo e níveis de descrição;
- um processo seguro para a transferência de unidades informacionais para o dispositivo de armazenamento, garantindo uma adequada gestão (incluindo verificações de integridade);
- mapeamento de processos para capturar a informação descritiva numa base de dados pesquisável associada aos registos por forma a que permaneçam localizáveis;
- um meio formal de disponibilizar a informação preservada aos utilizadores no formato mais apropriado tendo em conta esse conteúdo;
- um rigoroso sistema de monitorização das atividades de preservação que podem produzir dados de auditoria utilizáveis;
- a medida em que cada processo é utilizado dependerá da dimensão e da extensão do acervo.

No que concerne especificamente a uma **Política de Preservação Digital** esta deve prover à preservação no longo termo e acesso continuado à mesma, tendo presente como princípios essenciais: a autenticidade, a fidedignidade, a integridade, a inteligibilidade e a usabilidade no longo prazo (THE NATIONAL ARCHIVES, [20--?]b):

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

Objetivo a atingir: a certificação do repositório (ISO 16.363:2012)

Face à necessidade e urgência de se assegurar a preservação e acesso no futuro à informação em meio digital através de repositórios/arquivos digitais, surge um modelo que sintetiza as boas práticas relativas às componentes *infraestrutura técnica* e *organizacional* indispensável para a certificação de um repositório – a ISO 16.363:2012 – *Space data and information transfer systems – Audit and certification of trustworthy digital repositories*. Esta norma resulta de anos de trabalho desenvolvido em torno da *checklist* do TRAC - *Trustworthy Repositories Audit & Certification: criteria and checklist*[4].

Para que os repositórios assumam com plenitude a sua missão de preservação e acesso à informação, é imprescindível que sejam sujeitos a monitorização e manutenção. O controlo de ameaças e riscos assume, por isso, uma questão a não descurar e que deve estar implícito na estratégia.

Assim, devem ser efetuadas auditorias regulares que estabeleçam o nível de confiança do repositório e a conformidade com a ISO 16.363:2012.

Segundo esta norma, há três áreas principais a serem avaliadas, divididas por 109 critérios (cf. Anexo) que devem versar sobre o armazenamento, migração e acesso a acervos digitais através de um repositório confiável:

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

O projeto Portico serve como referência, dado que se constituiu como repositório digital confiável em 2010, através de uma auditoria levada a cabo pelo Center for Research Libraries[5].

A Portico é uma organização sem fins lucrativos que fornece um serviço de preservação de informação digital, através de um *arquivo permanente* de informação maioritariamente científica e técnica (livros, revistas eletrónicas e outros tipos de conteúdo académico).

Conforme análise aos relatórios da auditoria realizada, observa-se que a metodologia adotada pretendeu evidenciar a aceitação das boas práticas na gestão de sistemas digitais; os critérios a seguir; e o modelo de referência OAIS (Open Archival Information System).

Destacam-se alguns aspetos alvo de avaliação, sobretudo a nível da infraestrutura tecnológica:

---

[4] AMBACHER, B. U. A. – *Ob. cit.*

[5] PORTICO (2010) – *Portico certified as Trustworthy Digital Repository by the Center for Research Libraries.* [Em linha]. [Consult. 10 fev. 2014]. Disponível em: http://www.portico.org/digital-preservation/news-events/news/general-news/portico-certified-as-trustworthy-digital-repository-by-the-center-for-research-libraries

- Descrição de quaisquer mudanças significativas na arquitetura do sistema de suporte ao 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 seleção do conteúdo arquivado e 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.

Um repositório deverá contemplar toda a estrutura existente, através da definição de políticas e procedimentos que reflitam a gestão das unidades informacionais digitais, armazenamento e preservação, segurança e gestão de acessos, e infraestrutura tecnológica. Este conjunto de documentação deve contemplar os critérios estabelecidos na ISO 16.363:2012, de forma a proporcionar evidências de que se encontra em conformidade com a mesma.

Existe um conjunto de documentos que se revelam essenciais, a saber:

- Declaração de Missão, Visão e Objetivos e a definição da *comunidade-alvo*;
- Política e a Estratégia de Preservação - que definem a abordagem do repositório relativamente à preservação a longo prazo das unidades informacionais digitais;
- Planos de Contingência;
- Políticas de Segurança;
- Política de Gestão do Risco;
- Políticas de acesso à informação em meio digital;
- Definição das Estratégias de armazenamento e de migração/conversão das unidades informacionais digitais;
- Identificação de esquemas de metainformação adotados;
- Fichas/Manual de procedimentos de manutenção de *software* e *hardware*;
- Análises de custo-benefício, entre outros.

Nos critérios no âmbito da *Infraestrutura* e *Gestão de Riscos de Segurança* é ainda referido o emprego de normas relativas à área da segurança da informação, nomeadamente a ISO 27.002, que incide nas boas práticas relativas à gestão da segurança da informação, o que, mais uma vez, reforça a inter-relação entre a segurança e a preservação da informação.

Conclusão

Como se pode depreender, o mundo em que nos encontramos impõe-se como sendo cada vez mais digital, motivo pelo qual este se apresenta como um fator de extrema importância a considerar, precisamente quando a questão a equacionar diz respeito à preservação e à segurança da informação, funções inerentes à gestão da informação em contexto organizacional, garantindo, assim, o acesso continuado no longo prazo a um recurso estratégico e memória de instituições, organizações e pessoas.

Neste sentido, estão disponíveis modelos teóricos e conceptuais, bem como especificações e normas que auxiliam o processo de gestão da informação em geral e, de forma particular, os cada vez mais complexos processos de gestão da segurança e da preservação da informação.

No entanto, este constitui, na realidade, um longo caminho a percorrer, devendo-se atentar, sobretudo, na gestão e não apenas, e como vem sendo habitual, na tecnologia, separando orgânica e operacionalmente áreas que são indissociáveis como a da gestão do SI e a gestão dos STI.

Aliás, é este o mote referido, ao envolvermos a *Organização* no seu todo, isto é, os seus *atores*, *processos* e o inerente suporte *tecnológico*.

Recentemente vem emergindo uma nova perspetiva nas organizações que tende a destacar a noção de que o *fator humano* constitui, efetivamente, o pilar central para o sucesso de qualquer projeto, política ou procedimento. No entanto, o ponto central é efetivamente os equilíbrios que se têm que arquitetar, implementar e manter.

Desta forma, a *Estratégia de Preservação e de Segurança da Informação*, as *Estratégias e Políticas de Gestão de Informação e TI* a montante e as inerentes *Políticas e Planos de suporte* representam os eixos orientadores da Organização neste sentido, consolidando os objetivos a que a Organização se propõe, garantindo, inequivocamente, que as propriedades base da informação serão asseguradas.

Considerando o meio digital e os seus rápidos ciclos de obsolescência, bem como a transversalidade da sua presença na organizações e no suporte ao processo infocomunicacional, torna-se evidente a necessidade de reconhecer e assumir a inter-relação entre a segurança e a preservação da informação e consequentes processos de gestão.

Só com este ponto de partida poderemos perspetivar a finalidade última de constituir um Arquivo/Repositório Digital Confiável com impacto a dois níveis:

- garantindo o armazenamento seguro e íntegro, o acesso controlado e a preservação no longo prazo;
- garantindo a salvaguarda de atributos informacionais essenciais, ou seja, de que a informação se mantém autêntica, fidedigna, integra, inteligível, utilizável, disponível e preservável.

Um ponto de chegada que tem por base a Teoria Sistémica, a valorização do fenómeno infocomunicacional, humano e social, consubstanciando-se nas características de um

modelo teórico como o SI-AP. Este é, aliás, um fator crucial ao incidir num ciclo de vida da informação uno, equacionando a sua gestão integrada e a pluridimensionalidade de unidades de informação que integram sistemas de informação tendencialmente híbridos mas que exigem ser preservados num contexto que convoca a interoperabilidade dos sistemas, o seu eficiente e eficaz desempenho e a qualidade do serviço ao utilizador.

Barbedo (2005) referencia que "a preservação aplicada ao universo digital tem conseguido finalmente despertar a atenção de todos os setores profissionais na área da gestão da informação".

No entanto, e como acabámos de expor não é apenas a área da *Gestão da Informação* que é chamada a intervir a este nível, uma vez que, conscientes da sua transversalidade, é necessário assegurar uma base organizacional e tecnológica que contemple os requisitos que apenas se vislumbram parcialmente com a enunciação das *Políticas* a desenvolver em contexto organizacional.

Conforme refere Pinto (2010), este processo revela-se com caráter de urgência, porque se com o "analógico", e em linha com Maria Luísa Cabral, "amanhã é sempre longe demais", com o digital "hoje já pode ser tarde demais".

Referências bibliográficas

BARBEDO, Francisco
2005 Arquivos digitais: da origem à maturidade. *Cadernos BAD*. Lisboa. 2 (2005) 6-18.

BARBEDO, Francisco; CORUJO, Luís; SANTANA, Mário
2010 *Recomendações para a produção de planos de preservação digital*. Lisboa: DGARQ, 2010. [Em linha]. [Consult. 26 fev. 2014].
Disponível em: http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf

INTERNATIONAL STANDARD ORGANISATION
2010 *ISO/IEC 27.003:2010: Information technology: Security techniques: Information security management system implementation guidance*. Genève: ISO/IEC, 2010.

INTERNATIONAL STANDARD ORGANISATION
2012 *ISO 16.363:2012: Space data and information transfer systems: audit and certification of trustworthy digital repositories*. Genàve: ISO, 2012.

PINTO, Maria Manuela Gomes de Azevedo
2005 Uma era, uma visão, um paradigma: da teoria à prática. *Revista da Faculdade de Letras: Ciências e Técnicas do Património*. Porto. 1.ª Série. 4 (2005) 101-123.

PINTO, Maria Manuela Gomes de Azevedo
2009 Gestão da Informação e preservação digital: uma perspectiva portuguesa de uma mudança de paradigma. In CONGRESO ISKO-ESPAÑA, 9º, Valencia, 2009 -

Nuevas perspectivas para la difusión y organización del conocimiento: actas. [Em linha] Valencia: Universidad Politecnica de Valencia, 2009, p.323-355. [Consult. 26 fev. 2014].
Disponível em: http://repositorio-aberto.up.pt/bitstream/10216/25380/2/manuelapintogestao000100395.pdf

PINTO, Maria Manuela Gomes de Azevedo
2010 *Preservmap: um roteiro de preservação na era digital*. Porto: Edições Afrontamento; CETAC.MEDIA, 2010.

PINTO, Maria Manuela Gomes de Azevedo
2013 Gestão de Documentos e meio digital: um posicionamento urgente e estratégico. In SEMINÁRIO DE ESTUDOS DA INFORMAÇÃO, 3º, Niterói, 2013 - *Gestão do Conhecimento, Gestão da Informação, Gestão de Documentos em Contextos informacionais*. [Em linha]. [Consult. 8 fev. 2014].
Disponível em:
http://repositorio-aberto.up.pt/bitstream/10216/70837/2/000218862.pdf

PINTO, Maria Manuela Gomes de Azevedo; SILVA, Armando Malheiro da
2005 Um Modelo sistémico e integral de Gestão da Informação nas organizações. In CONTECSI - CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 2º, São Paulo, 2005 – *Actas do Congresso*. [Em linha]. [Consult. 8 fev. 2014].
Disponível em:
http://repositorio-aberto.up.pt/bitstream/10216/13461/2/modelo000071239.pdf

SILVA, Armando Malheiro da
2006 *A Informação: da compreensão do fenómeno e construção do objecto científico*. Porto: Edições Afrontamento; CETAC.COM, 2006.

SILVA, Armando Malheiro da
2009 Arquivologia e Gestão da Informação/Conhecimento. *Informação & Sociedade: estudos*. [Em linha]. João Pessoa. 19: 2 (maio/ago. 2009). [Consult. 18 jan. 2014].
Disponível em:
http://periodicos.ufpb.br/ojs2/index.php/ies/article/view/3712/3024>

SILVA, Armando Malheiro da; RIBEIRO, Fernanda
2002 *Das «ciências» documentais à Ciência da Informação: ensaio epistemológico para um novo modelo curricular*. Porto: Edições Afrontamento, 2002.

SOUSA, Paula Maciel Carvalho de
2013 *Segurança e preservação da informação: um modelo para os municípios*. Porto, 2013.
Dissertação de Mestrado em Engenharia de Serviços e Gestão, apresentada à Faculdade de Engenharia da Universidade do Porto.

UNITED KINGDOM. The National Archives
[20--?]a *Digital Preservation Strategy*. [Em linha]. [Consult. 10 fev. 2014].

Disponível em : http://www.nationalarchives.gov.uk/information-management/projects-and-work/digital-preservation-strategy.htm

UNITED KINGDOM. The National Archives
[20--?]b *Digital Preservation Policy*. [Em linha]. [Consult. 10 fev. 2014].
Disponível em : http://www.nationalarchives.gov.uk/information-management/projects-and-work/ digital-preservation-policy.htm

ZÚQUETE, André
2008 *Segurança em redes informáticas*. Lisboa: FCA - Editora de Informática, 2008.

Paula Maciel Carvalho de Sousa | macielsousa@cm-porto.pt
Câmara Municipal do Porto

ANEXO: Checklist para Repositório Digital Confiável e respetivos documentos

Nº Critério	Critérios	Documentos
3.	**Infraestrutura Organizacional**	
3.1	**Governança e Viabilidade Organizacional**	
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.
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.
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.
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 ira; 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 Acervo; Política de Preservação; missão, visão e objetivos do repositório.
3.2	**Estrutura Organizacional e de Pessoal**	
3.2.1.	O repositório deve ter identificado e estabelecido as tarefas/atribuições que precisa executar e deve ter nomeado funcionários com	Matriz de funções, competências e responsabilidades dos funcionários; descrições de cada cargo; organograma.

Nº Critério	Critérios	Documentos
	competências e experiência adequadas para as efetivar.	
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.
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.
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.
3.3	**Responsabilidade Processual e *Framework* de Política de Preservação**	
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 (SLAs) e condições de acesso dos utilizadores/permissões.
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.
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	Relatórios de auditorias e certificações técnicas e financeiras; documentação referente aos procedimentos de contratação pública; contratos com outras entidades.

Nº Critério	Critérios	Documentos
	longo do tempo.	
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.
3.4	**Sustentabilidade Financeira**	
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.
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.
3.5	**Contratos, Licenças e Passivos**	
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,	Acordos de licença ou de depósito; especificação de direitos transferidos para diferentes tipos de conteúdo digital (se aplicável).

Nº Critério	Critérios	Documentos
	devendo ser documentados os direitos transferidos.	
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.
4.	**Gestão de Objetos Digitais**	
4.1	**Ingestão: Aquisição [Entrada, Incorporação] de Conteúdos**	
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.
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.
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.
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 metadados.

Nº Critério	Critérios	Documentos
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 metadados.
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 controle suficiente sobre os objetos digitais para preservá-los.	Documentos que mostram o nível de controlo físico do repositório e os metadados associados.
4.1.7.	Durante os processos de ingestão, e em pontos acordados, o repositório deve fornecer respostas adequadas ao produtor/depositante.	Relatórios; 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 metadados ligados aos objetos digitais; registos de decisões e de medidas tomadas.
4.2	**Ingestão: Criação do AIP (*Archival Information Package*)**	
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 AIPs são derivados dos SIPs.

Nº Critério	Critérios	Documentos
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 AIPs são derivados dos SIPs.
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	

Nº Critério	Critérios	Documentos
	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.	

Nº Critério	Critérios	Documentos
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 dos metadados de preservação, armazenados e ligados aos objetos digitais; documentação sobre as decisões e ações tomadas.
4.3	**Planeamento da Preservação**	
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	Serviço de registo da Informação de Representação.

Nº Critério	Critérios	Documentos
	comunidade-alvo entender a informação armazenada.	
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.
4.3.4.	O repositório deve fornecer evidências da eficácia das suas atividades de preservação.	Esquemas de metadados de preservação adequados; prova de usabilidade de objetos digitais selecionados aleatoriamente dentro do sistema.
4.4	**Preservação dos AIPs**	
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.
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 dos metadados de preservação, armazenados e ligados 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 dos metadados de preservação, armazenados e ligados aos objetos digitais.
4.5	**Gestão da Informação**	

Nº Critério	Critérios	Documentos
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 metadados.
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 metadados.
4.5.3.	O repositório deve manter uma ligação bi-direcional 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.
4.6	**Gestão de Acessos**	
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.
5.	**Infraestrutura e Gestão de Riscos de Segurança**	
5.1	**Gestão de Riscos da Infraestrutura Técnica**	

Nº Critério	Critérios	Documentos
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.

Nº Critério	Critérios	Documentos
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*.
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; metadados de preservação; 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	Testes de validação da existência do objeto para cada localização

Nº Critério	Critérios	Documentos
	os objetos digitais.	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.
5.2	**Gestão de Riscos de Segurança**	
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).