Disponível em www.bad.pt/publicacoes
Paper

Avaliação de maturidade da governança da informação em Arquivos

Diogo Proença[a], Ricardo Vieira[b],, José Borbinha[c]

[a]*INESC-ID, IST, Universidade de Lisboa, Portugal, diogo.proenca@tecnico.ulisboa.pt*
[b] *INESC-ID, IST, Universidade de Lisboa, Portugal, rjcv@tecnico.ulisboa.pt*
[c] *INESC-ID, IST, Universidade de Lisboa, Portugal, jlb@tecnico.ulisboa.pt*

Resumo

A governança da informação pode ser definida como um quadro de definição de regras, direitos e responsabilidades em relação ao ciclo de vida da informação numa organização. Organizações que desejem cumprir com as melhores práticas de governança da informação devem procurar as referências mais relevantes na sua área de atividade. Nesta comunicação, apresentamos o modelo de maturidade para a governança da informação de arquivo A2MIGO, concebido para cenários onde os requisitos de preservação digital são relevantes, e desenvolvido no contexto do projeto E-ARK. Descreve-se também o método de desenvolvimento desse modelo, que considerou o estado da arte estabelecido para este fim e o resultado da sua aplicação a um conjunto de organizações reais.

Palavras-chave: Governança da Informação; Preservação Digital; Modelo de Maturidade; Avaliação de Maturidade.

Introdução

Um modelo de maturidade consiste em várias entidades, incluindo "níveis de maturidade" (muitas vezes seis) que são, do mais baixo para o mais alto, (0) Não Existente, (1) Inicial, (2) Básico, (3) Intermediário, (4) Avançado e (5) Otimização. Qualquer processo ou especto organizacional pode ter o seu próprio modelo de maturidade, que expressa quantitativamente o nível de maturidade de uma organização em relação a um determinado especto. Um modelo de maturidade também é um instrumento que as organizações podem utilizar para perceberem o que devem melhorar para passar ao próximo nível de maturidade, estando desta forma diretamente relacionado com o conceito de melhoria continua.

A utilização de modelos de maturidade é bastante generalizada e aceite, tanto na indústria como no meio académico. Existem inúmeros modelos de maturidade, com pelo menos um para cada um dos tópicos mais populares em áreas como as tecnologias da informação ou sistemas de informação. Os modelos de maturidade são amplamente utilizados e aceites devido à sua simplicidade e eficácia. Estes podem auxiliar uma organização a entender o nível atual de maturidade de um certo especto de forma significativa, de modo a que as partes interessadas possam identificar claramente os pontos fortes e fracos que exigem melhorias e, portanto, estabelecer prioridades ás alterações que devem ser implementadas para alcançar um nível mais elevado.

Existem vários exemplos de modelos de maturidade atualmente em uso. Por exemplo, na engenharia de software, existe o *Software Engineering Institute Capability Maturity Model Integration*, também conhecido como CMMI que tem sido melhorado continuamente nos últimos vinte anos, cobrindo um conjunto de aspectos relacionados aos ciclos de vida de produtos e serviços. No domínio da gestão da informação, existem vários exemplos de modelos de maturidade, como o *Enterprise Information*

Management Maturity Model da Gartner. Outros domínios onde os modelos de maturidade podem ser encontrados incluem gestão, gestão de processos de negócio, gestão de energia, governança e gestão de risco, entre outros.

Esta comunicação apresenta o modelo de maturidade para a governança da informação desenvolvido no âmbito do projeto E-ARK (http://eark-project.com/). Adicionalmente, detalha a avaliação dos níveis de maturidade das seis organizações inseridas no projeto: (1) Arquivo Nacional da Dinamarca; (2) Arquivo Nacional da Noruega; (3) Arquivo Nacional da Estónia; (4) Arquivo de Negócios da Estónia; (5) Arquivo Nacional da Eslovénia; e o (6) Arquivo Nacional da Hungria.

Método

A "governança da informação" é definida pela Gartner[1] como sendo a "especificação dos direitos de decisão e de um quadro de responsabilidades para incentivar a implementação de boas práticas na criação, armazenamento, uso, avaliação e arquivamento de informação. Inclui os processos, responsabilidades e métricas que garantem o uso eficiente da informação para permitir que uma organização atinja seus objetivos". De acordo com este conceito, e no âmbito do projeto E-ARK consideramos a governança da informação numa perspetiva de preservação digital. Para o efeito, as fontes consideradas foram o *Open Archival Information System – Reference Model* (OAIS / ISO14721) (ISO, 2010), o *Trustworthy Repositories Audit and Certification* (TRAC / ISO16363) (ISO, 2012) e o *Producer-Archive Interface Methodology Abstract Standard* (PAIMAS / ISO20652) (ISO, 2006).

Uma crítica recorrente aos modelos de maturidade é que eles carecem de base empírica e rastreabilidade (Röglinger, 2012). A principal razão para a crítica é que os modelos de maturidade existentes tipicamente não seguem um arcabouço ou metodologia teórica para o seu desenvolvimento (Röglinger, 2012). De fato, há uma ausência na literatura sobre métodos e práticas para o design e desenvolvimento de modelos de maturidade (Röglinger, 2012).

Um dos procedimentos de desenvolvimento de modelos de maturidade mais conhecidos para é o de Becker (Becker, 2009), um procedimento baseado em um método de investigação chamado Design Science Research (DSR). A argumentação do autor (Becker, 2009) é que os requisitos fundamentais derivados do DSR devem guiar o desenvolvimento de um modelo de maturidade. O artigo define um conjunto de etapas para desenvolver corretamente um modelo de maturidade. Ele descreve qual documentação deve resultar de cada etapa e inclui um método de desenvolvimento de modelos de maturidade iterativo que propõe que cada iteração do modelo de maturidade seja implementada e validada antes de desenvolver uma nova iteração. Este procedimento está representado na Figura 1.

A partir da análise dos modelos de maturidade existentes nas áreas de gestão de arquivo e preservação digital (Proença, 2017) concluímos que os modelos de maturidade selecionados não detalham o método de desenvolvimento utilizado

Outra conclusão é que os modelos de maturidade usam atributos com três objetivos: (1) Decompor o Modelo de Maturidade em seções facilmente compreensíveis; (2) Agregar vários processos de negócios em áreas de processo que agregam processos que atendem ao mesmo objetivo de negócios e (3) Fornecer diferentes pontos de vista do nível de maturidade. Podemos também concluir que os modelos de maturidade usam diferentes níveis de maturidade. Não há um número padrão de níveis de maturidade. Apesar disso, quando os modelos de maturidade são baseados ou seguem o SEI CMMI, eles frequentemente usam os mesmos cinco níveis e até mesmo tentam manter o mesmo racional dos níveis de maturidade usados pelo CMMI.

[1] http://www.gartner.com/it-glossary/information-governance

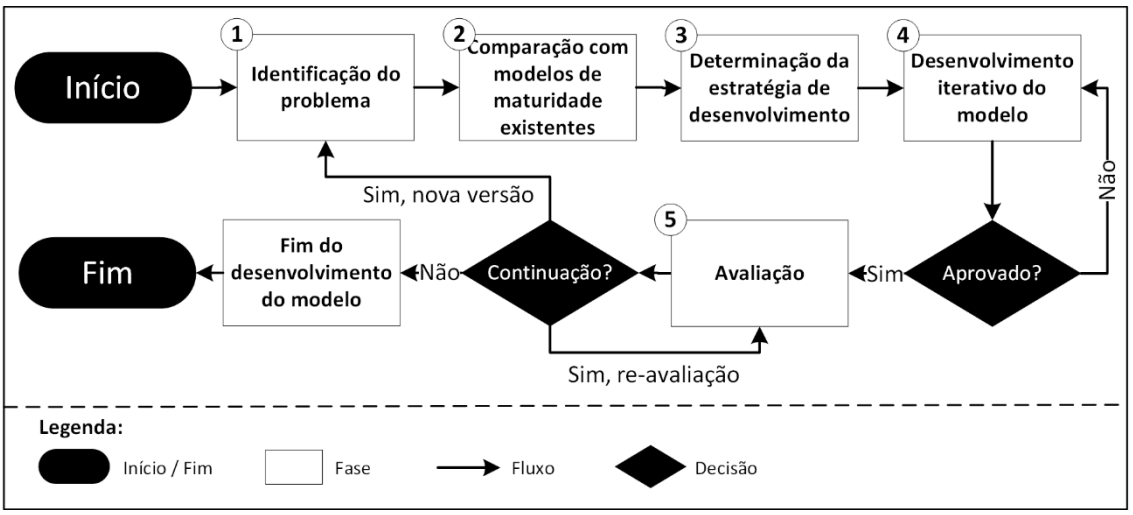

Figura 1: Procedimento de desenvolvimento de modelos de maturidade.

Outros modelos utilizam um número de níveis de maturidade considerados relevantes para o tema do modelo de maturidade que variam entre quatro e seis, com base nos modelos de maturidade analisados. Os que usam quatro níveis, de acordo com os quatro estágios de Nolan (Nolan, 1973), não fazem referência a esse facto, o que reforça a nossa conclusão que, apesar de terem o mesmo número de níveis /estágios, não são explicitamente sustentados nos quatro estágios de Nolan. Existem também modelos que usam o nível 0. Este nível geralmente mostra que há completa falta de maturidade e talvez até falta de consciência da necessidade de uma avaliação de maturidade.

Também observamos o trabalho existente na área dos Modelos de Maturidade da Preservação Digital realizados por Adrian Brown, onde o autor examina a noção de repositórios digitais "confiáveis" e propõe um modelo de maturidade para preservação digital, cujo objetivo é permitir que as organizações avaliem suas capacidades. e criar um plano de melhoria para atingir o nível de maturidade pretendido (Brown, 2013). Também analisamos o trabalho de Charles Dollar que propõe um Modelo de Maturidade para avaliar os requisitos de preservação digital (Dollar, 2013) de acordo com o OAIS/ISO14721 e o TRAC/ISO16363.

Resultados e Discussão

O modelo de maturidade do projeto E-ARK para a governança da informação cuja sigla é A2MIGO, consiste em três dimensões e cinco níveis de maturidade. As dimensões são:

- **Gestão:** "O termo gestão refere-se a todas as atividades que são usadas para coordenar, direcionar e controlar uma organização" (ISO, 2008);
- **Processos:** "Um processo é um conjunto de atividades que estão inter-relacionadas ou que interagem entre si. Processos utilizam recursos para transformar entradas (*Inputs*) em saídas (*Outputs*)" (ISO, 2008);
- **Infraestrutura:** "O termo infraestrutura refere-se a todo o sistema de instalações, equipamentos e serviços que uma organização necessita para operar" (ISO, 2008).

Estas dimensões fornecem diferentes pontos de vista da governança da informação que ajudam a decompor o modelo de maturidade e permitem uma fácil compreensão.

Na descrição dos critérios de maturidade são utilizados vários acrónimos para *Submission Information Package* (SIP), *Archival Information Package* (AIP), *Dissemination Information Package* (DIP), e

Preservation Description Information (PDI). Cujas definições podem ser encontradas no OAIS (ISO, 2010). Também são utilizadas siglas para cada uma das dimensões, gestão (G), processos (P), infraestrutura (I). Adicionalmente, existem critérios associados a todas as dimensões, critérios universais (U). Deste modo o critério P3.12, é o décimo segundo critério para o nível de maturidade três da dimensão dos processos.

No nível de maturidade 1, a organização ainda não reconhece a governança da informação como uma função relevante da organização.

No nível de maturidade 2 a governança da informação cumpre os seus objetivos. No entanto, não há uniformização de procedimentos, o que pode resultar em dois colaboradores a realizar tarefas diferentes para alcançar o mesmo objetivo o que, por sua vez, pode resultar na incapacidade de repetir tarefas que foram executadas anteriormente. Além disso, neste nível de maturidade não há atribuição de responsabilidades. Os critérios de avaliação para o nível de maturidade 2 estão detalhados na Tabela 1.

Critério de avaliação
G2.1 - Identificar se existe um compromisso com a preservação, retenção, gerenciamento e acesso no mais alto nível administrativo da organização.
G2.2 - Identificar se a organização possui uma definição de *designated community* que pode ser usada para verificar se a organização atende às necessidades desta.
P2.1 - Identificar se o arquivo pode negociar as condições de depósito com os produtores. Os termos de depósito podem incluir a especificação dos metadados que devem ser incluídos no momento do depósito, o cronograma e o método de depósito, as responsabilidades do produtor e do arquivo em relação às informações que estão sendo ingeridas, entre outros exemplos.
P2.2 - O objetivo é identificar se a organização fornece respostas ao produtor nos pontos acordados para garantir que não haja falhas na comunicação que possam levar à perda de um SIP.
P2.3 - O objetivo é identificar se a organização pode gerar um AIP a partir de um SIP. A organização deve garantir que o AIP represente corretamente o SIP.
P2.4 - O objetivo é identificar se a organização gera um identificador exclusivo e persistente para cada AIP, para que um AIP possa ser encontrado no futuro. Isso também garante que um AIP possa ser distinguido de todos os outros AIP no repositório. A organização deve ter registros que detalham como as alterações nos identificadores exclusivos devem ser realizadas para que o AIP não perca o contexto, não sejam perdidas e possam ser distinguidos de todos os outros AIP no repositório.
P2.5 - O objetivo é identificar se existem procedimentos que definem como o AIP é armazenado no nível de bit, garantindo que a informação possa ser extraída de um AIP.
P2.6 - Identificar se existem registos, de acordo com as disposições legais, para servir como evidência das ações realizadas durante o armazenamento e preservação do AIP, para garantir que a documentação seja válida e autêntica.
P2.7 - Identificar se a organização possui um serviço de resolução para encontrar um objeto identificado com um identificador exclusivo, independentemente da sua localização física, para que todas as ações relacionadas com um AIP possam ser rastreadas ao longo do tempo.
P2.8 - Identificar se existe um procedimento para criar um DIP a partir de um AIP.
I2.1 - Identificar se a organização gere a infraestrutura tecnológica que suporta os seus negócios.
I2.2 - Identificar se a organização pode garantir que fornece uma cópia autêntica de um AIP específico.
I2.3 - Identificar se a organização pode garantir que várias cópias de um AIP permanecem idênticas, dentro de um tempo estabelecido como aceitável pela organização, e que é possível utilizar uma cópia para o substituir.

Tabela 1: Critérios de avaliação para o nível de maturidade 2.

No nível de maturidade 3, a organização possui uma lista uniformizada de procedimentos com responsabilidades atribuídas. Existem também ferramentas e métodos que suportam a governança da informação, que são definidos e se tornam numa norma para toda a organização. Os procedimentos neste nível de maturidade são bem definidos e incluem o objetivo, entradas (Inputs), critérios de entrada, atividades, responsabilidades, fases de verificação, saídas (Outputs) e critérios de saída. Os critérios de avaliação para o nível de maturidade 3 estão detalhados na Tabela 2.

Critério de avaliação
G3.1 - Identificar se a organização garante que as competências técnicas relevantes estão identificadas e presentes na organização.
G3.2 - Identificar se existe um plano de formação desenvolvido e implementado na organização. Um plano de formação descreve as competências técnicas e sociais a serem obtidas, o prazo para atingir essas competências, a formação a ser realizada; entre outros aspetos.
G3.3 - Identificar se a organização partilha o conhecimento existente entre os colaboradores da organização, com especial foco na governança da informação.
G3.4 - Identificar se a organização requereu certificação ou se tem planos para fazê-lo.
G3.5 - Identificar se a organização procura estar alinhada com normas relevantes, tais como, a norma ISO 27001 para gestão da segurança da informação, a norma ISO 14721 (OAIS), a norma ISO 16363 (TRAC), a norma ISO 20652 (PAIMAS), entre outras.
G3.6 - Identificar se existe um plano estratégico de preservação que ajude a organização a tomar decisões administrativas, moldar políticas e alocar recursos para preservar com sucesso o seu acervo. O plano estratégico deve basear-se na missão, valores, visão e objetivos definidos da organização. Os planos estratégicos cobrem tipicamente um período de tempo finito, normalmente no intervalo de 3 a 5 anos.
G3.7 - Identificar se a organização pode fornecer um "rasto para auditoria" através da qual as partes interessadas podem identificar e rastrear todas as decisões.
G3.8 - Identificar se existe transparência na organização, disponível a qualquer individuo, como garantia de que a organização opera de acordo com as normas e práticas estabelecidas.
G3.9 - Identificar se a organização se pode proteger contra condutas ilegais ou outras atividades que possam ameaçar sua viabilidade económica. Através de práticas e procedimentos financeiros que sejam transparentes, estejam em conformidade com as normas e práticas relevantes e sejam auditadas por terceiros de acordo com os requisitos legais em vigor.
G3.10 - Identificar se a organização pode demonstrar que a organização identificou, documentou e gere o risco financeiro, investimentos e despesas. Ou seja, se identifica e mitiga riscos, especifica e equilibra os investimentos, antecipa e prepara as despesas. (incluindo ativos, licenças e passivos).
G3.11 - Identificar se a organização tem a capacidade de documentar os processos atuais e os processos anteriormente em vigor que foram aplicados ao seu acervo.
G3.12 - Identificar se a organização pode garantir que possui os direitos e autorizações necessárias para permitir o depósito e preservação de AIPs ao longo do tempo, bem como disponibilizar essas informações à sua *designated community*.
P3.1 - Identificar se o arquivo valida o SIP do produtor em relação ao formato e estrutura. Se o SIP tiver desvios, o arquivo poderá rejeitar o SIP e solicitar que o produtor forneça um SIP corrigido.
P3.2 - Identificar se a organização possui mecanismos para garantir a proveniência da informação depositada.
P3.3 - Identificar se um SIP do produtor é verificado e melhorado. A melhoria pode consistir em adicionar mais metadados ou reestruturar o SIP, entre outros procedimentos.
P3.4 - Identificar se o arquivo tem a capacidade de gerir *units of description* com base nas informações do SIP do produtor, ou se reutiliza informações já existentes para o novo SIP.
P3.5 - Identificar se a organização possui mecanismos para detetar e corrigir erros durante a criação de um SIP ou erros de transmissão durante uma sessão de depósito.
P3.6 - Identificar se a organização possui registos atualizados de toda a documentação relevante para o processo de depósito.
P3.7 - Identificar se o arquivo tem a capacidade de gerir os direitos legais (direitos de autor, proteção de dados e propriedade) de objetos durante o depósito no arquivo. Nesse sentido, a gestão dos direitos legais envolve a verificação dos direitos legais associados ao conteúdo durante o depósito. Incluí ainda, verificar se o conteúdo não é um duplicado de depósitos e inclui a criação de restrições de acesso a determinados objetos quando o produtor assim o solicita.
P3.8 - Identificar se a organização tem procedimentos definidos para demonstrar que um SIP específico foi aceite e incorporado como um AIP ou foi rejeitado e descartado.
P3.9 - Identificar se a organização tem a capacidade de criar classes para AIP para descrever os AIP que armazenam o mesmo tipo de informação. As classes para AIP são importantes para entender a variedade de informações armazenadas e para permitir a análise correta de todas as informações armazenadas no arquivo.
P3.10 - Identificar se a organização possui procedimentos definidos para garantir que a PDI esteja associada às informações de conteúdo relevantes. O que permite garantir a autenticidade dos objetos preservados e permite a deteção de alterações não autorizadas.
P3.11 - Identificar se a organização possui procedimentos definidos para garantir que a PDI seja mantida

durante o seu ciclo de vida. Isto inclui a realização de alterações na PDI como resultado de alterações de requisitos externos.
P3.12 - Identificar se a organização tem um procedimento para testar se a informação do conteúdo de um AIP é compreensível pela *designated community* para que todos os objetos depositados sejam considerados relevantes e utilizáveis.
P3.13 - Identificar se a organização verifica se todas os AIP estão completos e corretas aquando da sua criação para garantir que todos os AIP possam ser rastreados até ao SIP fornecido pelos produtores.
P3.14 - Identificar se a organização possui registos, de acordo com seu regras legais em vigor, para servir como evidência dos procedimentos executados para criar um AIP, a fim de garantir que nada seja omitido do AIP. Estes registos podem ser necessários para verificar se todos os AIP foram criados adequadamente e de acordo com os procedimentos documentados.
P3.15 - Identificar se a integridade do AIP é monitorizada, pois é necessário para proteger a integridade de um AIP ao longo do tempo.
P3.16 - Identificar se existe um procedimento para recolher e rever os requisitos da *designated community* para os AIP.
P3.17 - Identificar se a organização possui um mecanismo para verificação da integridade do conteúdo possibilitando auditorias independentes.
P3.18 - Identificar se a organização possui ferramentas ou métodos para identificar o tipo de ficheiro de todos os objetos depositados, para determinar qual a informação de representação é necessária para tornar cada objeto compreensível. Isto também garante que toda a informação de representação está associada aos objetos relevantes.
P3.19 - Identificar se o arquivo permite a pesquisa e casso aos objetos no seu acervo.
P3.20 - Identificar se o arquivo garante que as informações descritivas estão associadas ao AIP. O arquivo deve evidenciar que associa a cada AIP, a informação descritiva mínima que foi recebida do produtor ou criada pelo arquivo. A associação da informação descritiva com o AIP é importante, embora não exija correspondência um-a-um e não tenha de estar necessariamente armazenada juntamente com o AIP. Esquemas hierárquicos podem permitir que algumas informações descritivas sejam associadas a muitos AIP.
P3.21 - Identificar se o arquivo garante que todos os AIP possam ser localizados e recuperados. Um arquivo deve ter procedimentos sobre como estabelecer e manter as relações entre a informação descritiva e o AIP, e deve assegurar que cada AIP tenha informação descritiva associadas e que todas essas informações apontem para pelo menos um AIP.
P3.22 - Identificar se a organização possui políticas de acesso definidas com a *designated community*.
P3.23 - Identificar se a organização está em conformidade com as políticas de acesso definidas com a *designated community*.
P3.24 - Identificar se a organização mantém um registo e analisa todas as falhas e erros de acesso, o que pode ajudar a identificar ameaças de segurança e falhas do sistema.
P3.25 - Identificar se a organização regista o acesso ao seu acervo, como medida para detetar abusos ou uso indevido.
P3.26 - Identificar se a organização investiga e resolve os relatórios de incidentes e problemas acerca de erros em dados ou respostas dos utilizadores, essenciais para se tornar um arquivo confiável perante os seus utilizadores.
P3.27 - Identificar se a organização mantém uma cadeia auditável de autenticidade de um DIP para um AIP.
I3.1 - Identificar como a infraestrutura tecnológica é mantida e atualizada para que permaneça operacional e atenda aos requisitos dos utilizadores.
I3.2 - Identificar se a organização possui procedimentos de segurança para a infraestrutura e como esses procedimentos estão implementados.
I3.3 - Identificar se a organização possui mecanismos de monitorização de tecnologia e como estão implementados.
I3.4 - Identificar como a gestão de riscos é realizada na organização.
I3.5 - Identificar se a organização mantém um plano adequado de preparação e recuperação para desastres.
I3.6 - Identificar se a organização pode fornecer uma cadeia auditável através da qual as partes interessadas podem identificar e rastrear decisões.
I3.7 - Identificar se a organização pode cumprir a parte da sua missão relacionada com preservação dos objetos no seu acervo.
I3.8 - Identificar se a organização pode fornecer documentação que demonstre que desenvolveu ou adaptou medidas apropriadas para assegurar a integridade do seu acervo.
I3.9 - Identificar se a organização pode rastrear, atuar e verificar direitos e restrições relacionados ao uso dos objetos sobre sua custódia, conforme exigido pelo contrato de depósito ou licença.

Tabela 2: Critérios de avaliação para o nível de maturidade 3.

No nível de maturidade 4, a organização estabelece objetivos quantitativos de qualidade e desempenho de todas as funções relacionadas com a governança da informação. Medidas específicas de desempenho são recolhidas e analisadas utilizando métodos e técnicas estatísticas e quantitativas. Existem também limites de desempenho definidos e são utilizadas técnicas que apoiam na definição de objetivos de qualidade. Uma diferença fundamental entre os níveis de maturidade 3 e 4 é a previsibilidade do desempenho, uma vez que estas previsões são baseadas em análises estatísticas da informação. Os critérios de avaliação para o nível de maturidade 4 estão detalhados na Tabela 3.

Critério de avaliação
G4.1 - Identificar se a organização executa um processo de planeamento que pode ser usado para garantir a viabilidade da organização durante o período em que esta garantiu fornecer acesso ao seu acervo perante a sua *designated community*.
G4.2 - Identificar se os processos críticos podem ser monitorizados para garantir que estes continuem a cumprir as suas responsabilidades e para assegurar que quaisquer mudanças nesses processos sejam examinadas e testadas.
I4.1 - Identificar se a organização monitoriza o desempenho da infraestrutura.
U4.1 - Identificar se os objetivos de qualidade e desempenho do processo são estabelecidos e negociados com um nível de detalhe que permita uma avaliação geral dos objetivos e riscos ao nível do processo.
U4.2 - Identificar se a organização seleciona medidas e técnicas analíticas para serem utilizadas em gestão quantitativa.
U4.3 - Identificar se as medidas selecionadas são analisadas para determinar o desempenho dos processos das organizações.
U4.4 - Identificar se os limites de desempenho dos processos são estabelecidos e comparados com os objetivos de qualidade e desempenho dos processos da organização. Este procedimento permite determinar se os objetivos de desempenho de qualidade dos processos são atingidos.

Tabela 3: Critérios de avaliação para o nível de maturidade 4.

Finalmente, no nível de maturidade 5, a organização melhora continuamente os seus procedimentos de governança da informação com base na análise quantitativa de desempenho e dos objetivos de negócios. A organização emprega técnicas quantitativas para entender as variações nos procedimentos e encontrar as causas dos resultados obtidos. A organização concentra-se em melhorar continuamente o desempenho através procedimentos inovadores. Além disso, os objetivos de qualidade e desempenho são estabelecidos e revistos continuamente de modo a refletir possíveis mudanças nos objetivos de negócio e no desempenho da organização. Uma diferença fundamental entre o nível de maturidade 4 e 5 é o foco na melhoria continua e na gestão do desempenho da organização, que neste nível está preocupado em analisar o desempenho utilizando dados recolhidos de múltiplas fontes. Esses dados ajudam a identificar lacunas e pontos fracos no desempenho que são usados para criar um plano de melhoria. Os critérios de avaliação para o nível de maturidade 5 estão detalhados na Tabela 4.

Critério de avaliação
G5.1 - Identificar se a organização instiga a melhoria contínua das políticas e procedimentos de gestão, bem como das aptidões e outros aspetos relevantes da administração.
G5.2 - Identificar se a comunidade reconhece a organização como um bom exemplo de governança da informação por meio da disseminação de procedimentos implementados e abordagens inovadoras para a governança da informação.
U5.1 - Identificar se a organização identifica potenciais áreas de melhoria que poderiam contribuir para atingir os objetivos do negócio.
U5.2 - Identificar se há uma seleção e implementação de melhorias em toda a organização com base em uma avaliação de custos, benefícios e outros fatores.
U5.3 - Identificar se a organização avalia os efeitos das melhorias implementadas com base na qualidade e no desempenho dos seus processos, utilizando técnicas estatísticas e quantitativas.
U5.4 - Identificar se a organização seleciona, analisa e determina sistematicamente as causas dos resultados obtidos.
U5.5 - Identificar se a organização implementa e avalia as propostas de melhoria selecionadas.

Tabela 4: Critérios de avaliação para o nível de maturidade 5.

O que uma organização pode esperar ao progredir ao longo dos níveis de maturidade é que a sua implementação das boas prática e normas relacionadas com a governança da informação será cada vez melhor definida e otimizada.

Com vista à avaliação de maturidade das organizações inseridas no projeto E-ARK utilizando o A2MIGO foi decidido desenvolver um questionário de autoavaliação. O questionário é composto por três seções principais, cada uma das dimensões do modelo de maturidade, com um conjunto de perguntas em cada seção. No total este questionário é composto por 73 questões. A Figura 2 mostra a comparação dos resultados da avaliação de maturidade entre as organizações.

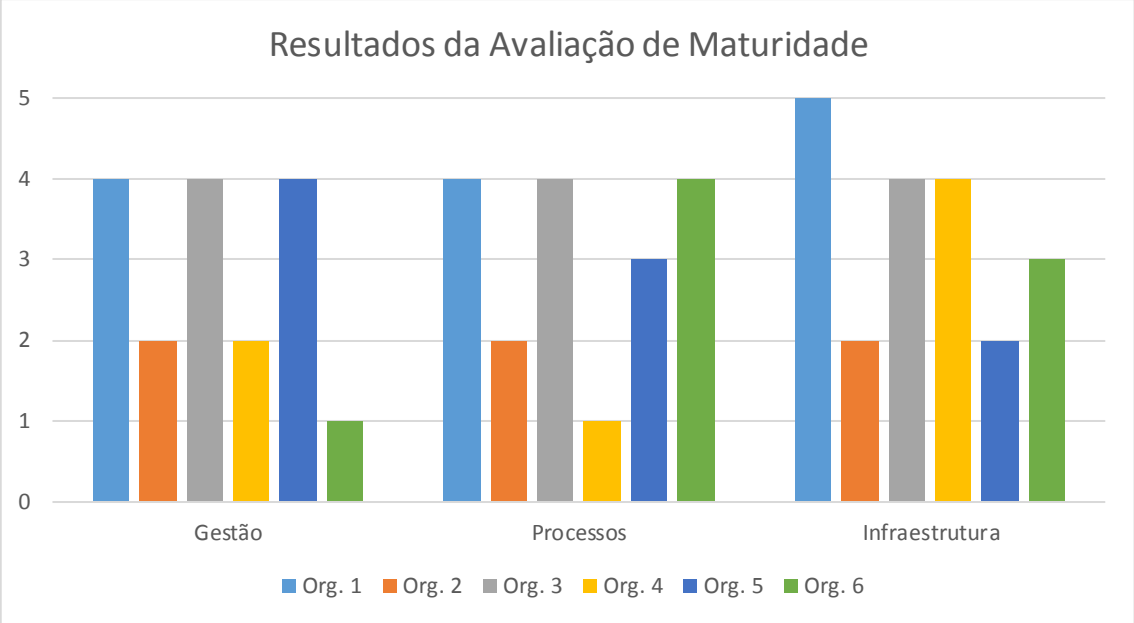

Figura 2: Resultados da avaliação de maturidade.

Conclusões

O A2MIGO permitiu avaliar as organizações inseridas no projeto E-ARK de uma forma simples e eficaz, permitindo encontrar os pontos fortes e fracos das organizações que foram avaliadas.

Contudo, foram identificados dois critérios principais com os quais a maioria das organizações não cumpriu, o que pode significar que é um critério muito complexo de implementar ou não é considerado relevante pela maioria destas organizações. O primeiro refere-se a um plano de certificação para a organização. A certificação pode ser utilizada para garantir que os processos e técnicas implementadas na organização estão alinhadas com as melhores práticas. A certificação representa também uma forma para potenciais clientes ou entidades financiadoras terem um certo grau de confiança na organização. Como tal, este é um especto relevante relacionado com a gestão de um arquivo. Um especto a ter em consideração é que este critério se concentra na averiguação da existência de um plano de certificação e não da existência de qualquer certificação. Como tal, as organizações que identificaram certificações relevantes ou definiram planos para uma futura certificação cumprem com este critério.

O segundo critério está relacionado com os requisitos das *designated communities* para os objetos no arquivo. O objetivo deste critério é identificar se existe um procedimento para reunir e rever os requisitos para os objetos no arquivo junto das *designated communities*. O objetivo é garantir que as *designated communities* tenham um forte relacionamento com a organização, que por sua vez melhorará a confiança

na organização. Ao cumprir este critério, a organização garante que os requisitos das *designated communities* são levados em consideração ao criar e preservar os objetos no arquivo. Por sua vez, isto garante que os objetos arquivados serão de facto relevantes para as *designated communities*.

O questionário de autoavaliação está disponível on-line em http://earkmaturitysurvey.dlmforum.eu. Qualquer organização pode utilizar para avaliar a maturidade dos seus processos e técnicas de governança da informação e com base nos resultados definir um plano de melhoria.

Contudo, ainda existem aspetos a melhorar no questionário, incluindo um guia detalhado sobre como preencher o questionário e analisar os resultados que estará disponível on-line com o questionário de autoavaliação.

Agradecimentos

Este trabalho foi financiado por fundos nacionais através da Fundação para a Ciência e a Tecnologia (FCT) com a referência UID/CEC/50021/2013.

Referências

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *BISE, 1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Brown, A. (2013). Practical Digital Preservation - A how-to guide for organizations of any size. Facet Publishing.

Dollar, C., Ashley, L. (2013). Assessing Digital Preservation Capability Using a Maturity Model Process Improvement Approach. Relatório Técnico.

ISO. (2006). *ISO 20652:2006 – Space data and information transfer systems – Producer-archive interface – Methodology abstract standard*. International Organization for Standardization, 2006.

ISO. (2008). *ISO 9001:2008 – Quality management systems – Requirements*. International Organization for Standardization.

ISO. (2010). *ISO 14721:2010 – Space data and information transfer systems – Open archival information system – Reference model*. International Organization for Standardization.

ISO. (2012). *ISO 16363:2012 – Space data and information transfer systems – Audit and certification of trustworthy digital repositories*. International Organization for Standardization.

Nolan, R. (1973). Managing the Computer Resource: A Stage Hypothesis. *Communications of the ACM*, 16, 399-405.

Proença, D., Vieira, R., Borbinha, J., Calado, P., & Martins, B. (2017). A Maturity Model for Information Governance – Final Version. Instituto Superior Técnico - Universidade de Lisboa. Retrieved from http://www.eark-project.com/resources/project-deliverables/95-d75-1

Röglinger, M., Pöppelbuß, J. and Becker, J. (2012). Maturity models in business process management. *Business Process Management Journal*, 18(2), 328 – 346.