FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Melhoria de Processos de Software em Pequenas Empresas com base no Modelo ITmark

Duarte Gil Araújo Gomes

Mestrado em Engenharia de Software

Supervisor: João Carlos Pascoal Faria

24 de Julho de 2018

Melhoria de Processos de Software em Pequenas Empresas com base no Modelo ITmark

Duarte Gil Araújo Gomes

Mestrado em Engenharia de Software

Aprovado em provas públicas pelo Júri:

Presidente: Prof. Nuno Flores
Arguente: Prof. Alberto Sampaio
Vogal: Prof. João Carlos Pascoal Faria

---

24 de Julho de 2018

Resumo

As pequenas empresas de desenvolvimento de software representam hoje uma grande quota da indústria de software, devido à sua capacidade de entregar os produtos sem o uso de muitos recursos e colaboradores, conquistando facilmente o mercado. A Indústria reconhece a sua importância pois são requisitadas até pelas grandes empresas para colaborarem no desenvolvimento do seu software. Apesar deste reconhecimento, as pequenas empresas de desenvolvimento de software mostram algumas preocupações sobre o processo que usam para o seu ciclo de desenvolvimento de software.

Assim, após uma investigação, deparámo-nos com um paradoxo que este tipo de empresas enfrentam, que é a necessidade de entrega, gestão dos seus produtos e projetos com metodologia ágil, necessidade em usarem modelos de melhoria de processo para garantir a estabilidade organizacional e cobrir os requisitos do RGPD para evitar perdas.

O modelo de certificação ITmark é uma boa base para responder a estas preocupações, na medida em que é um modelo leve direcionado para pequenas empresas, abrange não só os processos de desenvolvimento de software como também os processos de gestão de segurança de informação (relevantes para o cumprimento do RGPD) e mesmo os processos de gestão de negócio. No entanto, o modelo ITmark é um modelo genérico, que se situa a um nível de abstração elevado, sem preocupação de alinhamento específico com Scrum e RGPD.

O problema que este projeto se propõem a resolver é: uma solução que permita às pequenas empresas de desenvolvimento de software garantir a certificação dos seus processos de desenvolvimento de software, adotar métodos ágeis no seu processo de desenvolvimento de software e cumprir o novo regulamento geral de proteção de dados.

Para resolver o problema, foi realizado o mapeamento entre as áreas de processo do modelo ITmark e Scrum, um mapeamento e refinamento entre modelo ITmark e o RGPD de forma a cumprir os requisitos do RGPD.

A estrutura do relatório apresenta uma revisão do estado de arte, ou seja um levantamento das investigações realizadas em torno dos tópicos identificados para a dissertação de forma a criar as fundações para o restante trabalho.

Na segunda parte temos a pesquisa efetuada, onde foi realizado um mapeamento entre as boas práticas de desenvolvimento de software incluídas no modelo ITmark e elementos de Scrum (artefactos, eventos, etc.). São também identificadas as principais lacunas (*gaps*) e cuidados adicionais a ter (além da implementação de Scrum) para cumprir os requisitos de ITmark. Quanto ao novo regulamento geral de proteção de dados, foi elaborado um questionário complementar ao questionário de ITmark para avaliação de processos de gestão de segurança de informação.

O caso de estudo foi realizado com sucesso num pequena empresa de desenvolvimento de software, focando-se nas áreas de planeamento de projetos, monitorização e controlo de projetos,

gestão de requisitos e gestão de segurança da informação.

Keywords: Pequenas empresas de desenvolvimento de software, ITmark, Scrum, RGPD, Melhoria de processos, Certificação

Abstract

Small software development companies today represent a large share of the software industry due to their ability to deliver the products without the use of many resources and collaborators, easily conquering the market. The industry recognizes its importance because it is required by large companies to collaborate on the development of its software. Despite this recognition, small software development companies show some concerns about the process they use for the software development cycle.

So, after our research, we have encountered a paradox that this type of business faces, which is the need to deliver and manage their products, projects following an agile methodology, and at the same time use process improvement models to ensure organizacional stability and cover the requirements of GDPR to avoid losses.

The ITmark certification model is a good basis for responding to these concerns, to the extent that it is a lightweight model targeted at small businesses,it covers not only software development processes but also the security management processes of information (relevant for compliance with GDPR) and even business management processes.However, the ITmark model is a generic model, which is situated at a high abstraction level, with no concern for specific alignment with Scrum and GDPR.

The problem that this project proposes to solve is: a solution that allows small software development companies to ensure the certification of their software development processes, adopt agile methods in their software development process and meet the requirements of new general data protection regulation.

To solve the problem, a mapping was carried out between the process areas of the model ITmark and Scrum, also a mapping between model ITmark and GDPR and finally a refinement of the model ITmark to meet the requirements of GDPR.

The structure of the report presents a revision of the state of the art, i.e,a survey of the research carried out around the topics identified for the dissertation to create the foundations for the remainder of the work.

In the second part we have the research carried out, where a mapping was carried out between the good software development practices included in the ITmark model and elements of Scrum (artifacts, events, etc.). The main gaps and additional care (in addition to the Scrum implementation) are also identified to meet the ITmark requirements. About the new general data protection regulation, a supplementary questionnaire to the ITmark questionnaire was prepared for evaluation of information security management processes.

The case study was successfully carried out in a small software development company, focusing on project planning, monitoring and control, requirements management and information security management.

Keywords: Small entities, ITmark, Agile, GDPR, Process improvement, Certification

Agradecimentos

Este relatório é resultado de vários meses de trabalho, nos quais tive o privilégio de privar com pessoas que muito contribuíram para a sua elaboração.

Assim, começo por agradecer ao meu orientador, o professor João Pascoal Faria, que se mostrou sempre disponível para me auxiliar na conceção deste documento.

Agradeço, igualmente, aos meus orientadores da empresa, Celso Campos, Adaílson Júnior e aos restantes membros da equipa por todo o apoio prestado e pelas horas que despenderam a contribuir para o desenvolvimento deste projeto e enorme disponibilidade demonstrada.

Queria a agradecer também à Strongstep e ao Pedro Castro Henriques pela ajuda prestada no que toca a fornecimento de informação e material, assim como no *feedback* prestado sobre o estudo produzido nesta dissertação sobre o modelo ITMark, que se vieram revelar uma ajuda inestimável.

À minha família, por se ter mostrado sempre disponível para contribuir em todas as situações, fornecendo ânimo e coragem ao longo do processo de elaboração da dissertação.

Aos meus amigos do Mestrado de Engenharia de Software pela ajuda, força e companheirismo demonstrado ao longo destes dois anos.

A todos agradeço, cada minuto que me cederam, bem como as palavras de incentivo que se revelaram determinantes em momentos mais difíceis.

Duarte Gomes

"Continuous Improvement,
is better than delayed perfection"

Mark Twain

Conteúdo

Lista de Figuras

Acrónimos

CMMI	*Capability Maturity Model Integration*
ESI	Instituto Europeu de Software
IS	*Information Security*
ISMS	*Information Security Management*
ISO/IEC	*International Organization for standardization and the International Electrotechnical Commission*
IT	*Information Technology*
GDPR	*General Data Protection Regulation*
PDCA	*Plan Do Check Act*
RGPD	Regulamento Geral Proteção de Dados
RH	Recursos Humanos
SPICE	Software Process Improvement and Capability Determination
XP	*Extreme Programming*

Capítulo 1

Introdução

1.1 Contexto

O desenvolvimento de software cresceu bastante na última década, o que gerou uma evolução industrial. As pequenas empresas como parte dessa evolução conquistaram sua posição na indústria devido à sua flexibilidade e adaptabilidade a cada entrega do produto. A sua importância é reconhecida por todos, porque ajudam as grandes empresas a produzir software e ainda produzem o seu próprio software, o que permite o avanço do conhecimento e da inovação.

Apesar do constante crescimento das empresas todas eles têm um ponto em comum: começam de micro para pequenas e continuam até chegarem ao topo. Mas esta não é uma tarefa fácil pois exige muitas modificações e preocupações durante a vida da empresa.

As pequenas empresas, são um exemplo real disso, enfrentam inúmeras preocupações e dificuldades, devido à falta de metodologia. Portanto surge a necessidade de obter um processo e uma solução de desenvolvimento de software estável. Contudo quando é necessário mudar para obter um desempenho mais estável, o que se torna um problema devido ao seu bem estar relativamente ao fluxo já implementado. Mas isso não é tudo, o investimento que este tipo de alterações traz para as pequenas empresas é um extra que estas não podem suportar e é automaticamente rejeitado na maioria dos casos. O processo, manutenção e recursos humanos são sua principal preocupação e consomem quase todo o orçamento.

Ainda assim, as pequenas empresas têm sempre o objetivo de crescer e melhorar, e dessa forma acompanhar as novidades da indústria de software. A implementação das metodologias ágeis, a obtenção da certificação e cumprimento do regulamento geral de proteção de dados surgem como as principais preocupações.

Como tal, torna-se necessário um novo tipo de solução que aborde as necessidades e automaticamente as cumpra numa solução única sem custos e esforço adicionais para as pequenas empresas.

1.2 Objetivos

O objetivo deste estudo é identificar uma solução na área de melhoria de processos de software. Esta solução pretende responder às necessidades que as pequenas empresas atualmente têm que são a obtenção de certificação nos seus processos de desenvolvimento de software, agilização do desenvolvimento de software e cumprimento do novo regulamento geral de proteção de dados. O modelo ITMark, um modelo de certificação, foi escolhido pois é constituído por três componentes que são o CMMI, ISO 27001 e *Ten squared* e que servirão como solução para cobrir as necessidades identificadas pois fornece certificação a estas três vertentes. Assim a investigação caracteriza-se por elaborar uma solução que permita às pequenas empresas de desenvolvimento de software garantir a certificação dos seus processos de desenvolvimento de software com base no modelo ITmark, adotar métodos ágeis no seu processo de desenvolvimento de software como a metodologia Scrum e cumprir o novo regulamento geral de proteção de dados, será realizado um caso de estudo corporativo numa pequena empresa de desenvolvimento de software para observar os resultados de implementar ITmark, Scrum e RGPD ao mesmo tempo.

Depois de realizado o caso de estudo será efetuada um levantamento de oportunidades de melhoria para informar a empresa das suas falhas e onde pode melhorar, recolhendo no fim a opinião da empresa relativamente a relevância das falhas levantadas.

Resumindo, esta pesquisa consistirá num trabalho de consultoria, que se foca nas preocupações que as pequenas empresas têm quanto ao seu processo de desenvolvimento de software, como a necessidade de estabilidade no seu processo de desenvolvimento de software, agilidade no desenvolvimento de software e a conformidade com a nova regulamentação geral de proteção de dados.

Espera-se assim que este projeto corresponda às necessidades pequenas empresas quanto à melhoria de processos de software. O desafio consiste em juntar estes três componentes, ITMark, RGPD e Scrum e desenvolver uma solução que encaixe os três nas pequenas empresas.

A seleção do ITMark é justificada pela sua constituição diversificada, que abrange os três pontos que mencionamos anteriormente, que constituem o principal problema. Caracterizado por um esquema de certificação que é construído especificamente para pequenas empresas, com diretrizes diretas para ajudar a melhorar os seus métodos e técnicas necessários para fornecer a estabilidade necessária ao seu processo.

Mas isso não é tudo, o ITMark é constituído com a ISO 27001, padrão para proteção da informação, importante para obedecer aos requisitos da nova regulamentação de proteção de dados. Então, será interessante se, quando adotarmos o ITMark, verificar se também automaticamente estamos a respeitar as *guidelines* impostas pelo RGPD.

Enquanto a ITMark se preocupa com a certificação e com a proteção de dados, o Scrum foca-se nas técnicas e práticas para gerir e entregar os produtos rapidamente e com qualidade.

Isso levará diretamente a um software com melhor qualidade. Permitir que as organizações consigam um melhor processo para o seu ciclo de desenvolvimento de software e, ao mesmo tempo, produtos de acordo com a nova regulamentação de proteção de dados.

1.3 Estrutura do documento

O primeiro capítulo deste relatório, Introdução, fornece informações gerais sobre o projeto. Há uma apresentação do contexto do projeto, juntamente com os objetivos a serem alcançados e a motivação por trás do projeto. Este capítulo também apresenta a estrutura constituinte do relatório.

O segundo capítulo, Estado da Arte, contém uma introdução aos Padrões de Engenharia de Software para pequenas empresas, onde são explicados alguns dos padrões que são usados na indústria de software por parte destas empresas. A secção ITMark contém uma explicação deste modelo de certificação de processos de desenvolvimento de software. Indica também os constituintes e a adoção em todo o mundo e alguma pesquisa já efetuada que será importante no trabalho posterior, que é o mapeamento entre as áreas de processo do ITMark e métodos Scrum. A secção de Padrões e Regulamentos de Segurança da Informação, explica a importância de cumprir os requisitos do RGPD, demonstra os padrões usados e algumas diretrizes para pequenas empresas de Software. A secção de Conclusão, descreve algumas das conclusões obtidas após o desenvolvimento do Estado de Arte, o que foi encontrado e algumas opiniões. Mostra também o que será feito nos próximos meses durante esta pesquisa.

O terceiro capítulo, ITmark - Refinamento do modelo, demonstra o mapeamento realizado entre a metodologia ágil Scrum com o modelo de certificação ITmark e o mapeamento entre o modelo ITmark e o RGPD. Na secção melhorias são identificadas sugestões de melhoria de forma a garantir a adaptabilidade do Scrum ao modelo ITmark e do modelo ITmark ao RGPD.

O quarto capítulo , Caso de estudo, caracteriza-se por demonstrar a metodologia aplicada para a realização do estudo na empresa, aqui podemos verificar o contexto da realização do estudo assim como o objetivo. Neste capitulo são demonstrados também os resultados do caso e estudo e são realizadas avaliações quanto a esses resultados.

O quinto capítulo , Avaliação final, demonstra as conclusões finais quanto ao estudo realizado na empresa e ao refinamento do modelo ITmark, estas conclusões são demonstradas por três perspetivas, do avaliador, empresa onde foi realizado o estudo e uma entidade independente com o objetivo de demonstrar as vantagens dos estudos realizados.

O sexto capítulo, Conclusão e trabalho futuro, identifica as principais conclusões obtidas após a realização da dissertação, demonstra as principais dificuldades obtidas e o trabalho futuro do estudo.

Capítulo 2

Estado da arte

2.1 Padrões de Engenharia de Software para pequenas empresas

Quando falamos sobre o setor de software, pensamos imediatamente em empresas de grandes dimensões como Google, Facebook, Apple, Microsoft, etc. Este pensamento não está completamente errado porque estas empresas produzem grande parte dos softwares que utilizamos. Contudo existe outra fração com outro tipo de característica que constitui uma parte da indústria de software. Estas empresas têm um papel preponderante no software porque as grandes empresas dependem de software de terceiros nas suas atividades e que normalmente é desenvolvido por empresas de pequenas dimensões.[12]

"Very small entities are, enterprises, organizations, projects or departments with up to 25 people"[12]. As pequenas empresas são a força dominante da indústria de software e são cruciais para essa mesma indústria, pois fornecem competitividade e inovação.

Na Europa, por exemplo, 85 por cento das empresas do setor de tecnologia da informação (TI) têm de um a 10 funcionários. Em Portugal, como podemos ver na figura 2.1 na página 6 recolhida de pordata [16], uma base de dados que mantém estatísticas ligadas ao comércio e à indústria sobre empresas portuguesas e europeias, podemos ver que as pequenas e médias empresas são a principal empresarial [12].

O que outrora costumava ser feito apenas pelas grandes empresas como auditorias, agora é uma grande preocupação e objetivo para as pequenas empresas. Apesar de encontrarmos muitos modelos para melhoria de processos, nem todos contêm as características necessárias para corresponder a estas empresas. O processo de software é uma área de pesquisa para engenharia de software e a gestão desse mesmo processo de software torna-se um grande desafio.

As grandes organizações geralmente usam modelos tradicionais de melhoria de processos de software, como CMMI e ISO / IEC 15504 também conhecidos como Software Process Improvement and Capability Determination ou simplesmente (SPICE) [11]. As pequenas organizações geralmente não fazem isso por muitas razões. Como por exemplo a perceção de que estes esforços foram desenvolvidos por e para organizações maiores, que são extremamente dispendiosos, exigem muita documentação e burocracia. Para as pequenas empresas de software, a implementação

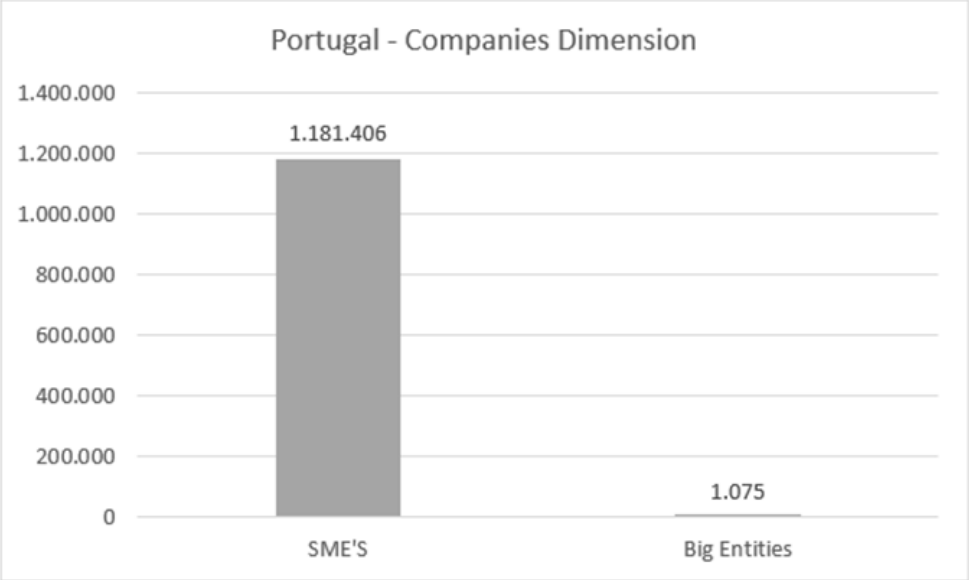

Figura 2.1: Constituição do mercado empresarial em Portugal (Em Milhões) [16]

de controlos e estruturas de gestão de desenvolvimento de software é um grande desafio.

Como tal é necessário ajudar estas organizações a entender o benefício destes conceitos, processos e práticas descritos na Organização Internacional de Normalização / Comissão Eletrotécnica Internacional (ISO/IEC).

Assim sendo e tendo em vista a melhorar o desempenho das pequenas empresas, algumas mudanças foram realizadas e adotadas por comissões e entidades internacionais. E assim nasceu um novo padrão, o ISO 29110 que se concentra nos perfis do ciclo de vida do software, fornecendo diretrizes e boas práticas que ajudam no processo. Diretamente feitos para pequenas empresas, oferecem uma família de padrões que cobrem todas as principais áreas deste tipo de organizações. Existem outras iniciativas que são dedicadas a pequenas empresas, algumas da América Latina, como a Competisoft e outras na Europa, como o ITmark [11].

Numa altura em que a qualidade do software é a chave para a vantagem competitiva, as organizações estão apenas a usar alguns dos sistemas ISO / IEC de engenharia de software. As pesquisas demonstram que as pequenas empresas muitas vezes têm dificuldade em relacionar e justificar os padrões ISO / IEC às suas necessidades e práticas comerciais.

A maioria não vê os seus benefícios, a falta de experiência ou a impossibilidade do pagamento aos funcionários, o custo e o tempo necessário são algumas das razões para a não utilização destas normas, como podemos ver na figura 2.2 [11].

O padrão ISO / IEC 29110 Software Engineering Lifecycle para as pequenas empresas visa abordar as práticas de engenharia de software e gestão de projetos. Os guias são baseados em subconjuntos de elementos de padrões apropriados, denominados perfis VSE (ISO / IEC 12207, ISO / IEC15289, ISO / IEC 15504, ISO 9001). Os chamados guias são reunidos nos padrões

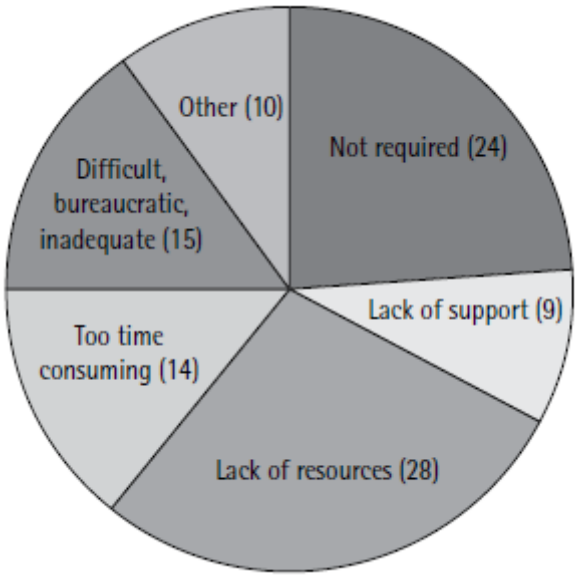

Figura 2.2: O porque das pequenas empresas não usarem Padrões de Software? [11]

ISO / IEC 29110 Software Engineering Lifecycle para pequenas empresas, que pretende facilitar o acesso e a utilização de padrões de engenharia de software ISO[12].

O núcleo da ISO / IEC 29110 é um guia para a gestão e engenharia (ISO / IEC 291105), com foco em gestão de projetos e implementação de software. Ele compreende um conjunto de grupos de perfis, cada um contendo perfis relacionados pela composição do processo (como atividades ou tarefas), nível de capacidade ou ambos.

Para as pequenas empresas que desenvolvem software não crítico, existem quatro perfis: inicial, básico, intermediário e avançado. Cada compilação baseada no processo anterior, adicionando tarefas de gestão e implementação de software, bem como processos de suporte, para projetos mais complexos ou pequenas empresas em crescimento [12].

Uma série de pacotes de implementação definem as diretrizes e explica os processos ISO / IEC 29110 para ajudar as pequenas empresas a implementar o padrão e implementar o guia de gestão e de engenharia. Os pacotes de implementação geralmente incluem descrições de processos, atividades, tarefas, etapas, papéis, produtos, modelos, listas de verificação, exemplos, ferramentas, referências e um mapeamento para outros padrões e modelos como ISO / IEC 12207, ISO 9001 e CMMI. Os pacotes de implementação permitem que as pequenas empresas implementem processos, atividades e tarefas ISO / IEC 29110 sem ter que implementar a estrutura completa de gestão e engenharia [4].

Na Figura 2.3, observamos a descrição dos padrões internacionais (IS) e Relatórios Técnicos (TR) ISO / IEC 29110 e posiciona as peças dentro do quadro de referência. Numa visão geral da norma de certificação, encontramos alguns documentos como guia de avaliação, guia de gestão e

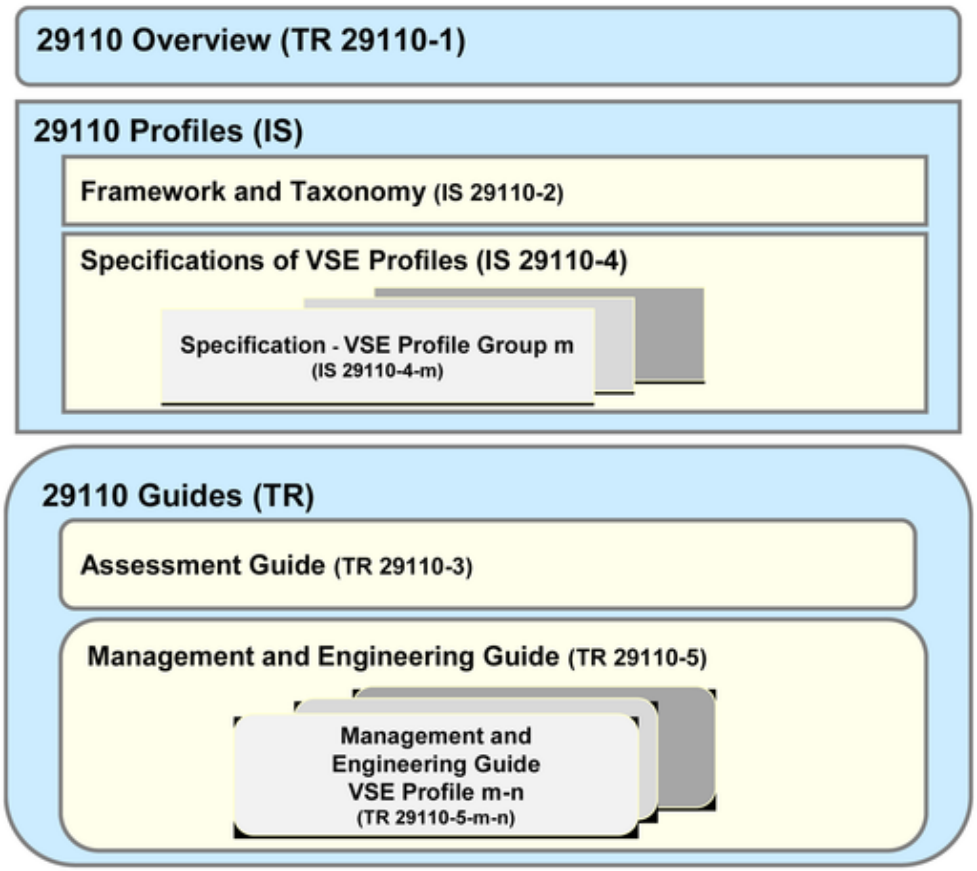

Figura 2.3: Constituintes da ISO 29110
[7]

engenharia, relatórios técnicos (TR) da ISO / IEC, as especificações de perfil e os esquemas de certificação que são publicados como padrões internacionais (IS).

2.2 ITmark

O ITmark é um esquema de certificação para pequenas e médias empresas. Melhora a eficácia organizacional e o sucesso nos processos de negócios dedicados ao desenvolvimento, manutenção de sistemas, aplicações e produtos de software. Caracteriza-se como um guia para etapas sistemáticas e organizadas que podem atingir níveis de capacidade e maturidade excelentes [15].

É o primeiro modelo de qualidade internacional projetado para pequenas e médias empresas que tem como objetivo fornecer um selo de qualidade sobre a maturidade e capacidade de desenvolvimento de software.

Foi criado pela ESI (European Software Institute), para cobrir as novas necessidades de pequenas e médias empresas e que dessa forma aparece como uma solução para seus problemas. Como para a grande maioria das pequenas e médias empresas é complicado adotar uma auditoria exaustiva como o CMMI, o ITmark é uma alternativa a esse paradigma.

Este padrão ajuda as pequenas empresas a alcançar a certificação de melhoria de processo e ajuda essas empresas a alcançar novos mercados e competir por concursos públicos que exigem este tipo de regulamentos. Apesar de existirem outro tipo de certificações estas não são sempre os melhores ou os mais aplicáveis a esse tipo de empresas [20].

O ITmark é adequado para entidades pequenas porque observa apenas as partes principais que podem influenciar diretamente o meio ambiente, como área de negócios, sistemas de software, proteção de dados e privacidade, mas isso não é tudo, a entidade com este processo acaba por economizar nos seus gastos porque esse tipo de auditoria é mais leve e flexível em contraste com outros modelos de melhoria de processo.

2.2.1 Componentes do ITmark

A constituição é diversificada, como podemos ver na figura 2.4 na página10, o que é uma vantagem, porque, como referido anteriormente, a maioria das pequenas empresas não podem efetuar grandes investimentos, então, com esta certificação, eles conseguem visualizar a maioria dos seus departamentos de negócios em busca de melhorias.

Portanto, o ITmark é constituído pelo *CMMI-DEV*, até ao nível de maturidade três, que se concentra em diretrizes para o desenvolvimento de software, fornecendo as melhores práticas para ajudar as equipes de desenvolvimento e aumentar o seu desempenho e organização.

Outro componente é a ISO 27001, um padrão que se preocupa com a proteção de dados e a gestão de segurança da informação. O que capacita a organização com um conjunto de processos para gerir corretamente o riscos que afetam os dados e a informação corporativa.

O terceiro componente é o método *Ten Squared*, uma ferramenta metodológica que avalia a gestão de negócios, recorrendo às melhores práticas na indústria, também conhecido como *benchmarking*. Analisa as áreas corporativas que se concentram principalmente no mercado, recursos humanos, questões financeiras e atores de investimento, ajudando a organização a alcançar um melhor fluxo de negócios evitando riscos e perdas [20].

2.2.2 Certificação ITmark

A avaliação começa com um diagnóstico inicial através de toda a empresa para entender o fluxo e as características que representam e são realizadas durante o ciclo de vida do desenvolvimento de software. Em seguida, um *workshop* é conduzido com a empresa, explicando como é que o ITmark funciona e como as práticas podem e devem ser implementadas na empresa.

A terceira fase é um relatório intermediário, que consiste em uma verificação das novas implementações e verifica a evolução da empresa com essas mudanças.

Finalmente, é estabelecida uma avaliação e recolha dos resultados. O resultado é atribuído com base no cumprimento dos objetivos estabelecidos, a certificação é entregue e assim a empresa deve ser incluída na lista de empresas certificadas, caso contrário, é importante verificar o que não foi implementado e melhorar esses aspetos.

Figura 2.4: Componentes ITmark

Esta avaliação é conduzida por uma equipa de auditores que são designados para a empresa onde contemplam auditores externos e internos estes nomeados pela organização. Os auditores internos recebem treino para implementar e ensinar a todos os colegas da organização as melhores práticas para atingir o objetivo. Na figura 2.5, são mostrados os diferentes níveis de certificação e os requisitos específicos para atingir o nível.

Level	Business Process Assessment	Security Process Assessment	Software Process Evaluation	
			Type of Evaluation	Evaluation Result
it mark Elite	No Red Categories>75%	Level 3	Class B/Maturity Level Three	N° Red Processes + N° Green Processes >=11
it mark Premium	No Red Categories>60%	Level 2	Class B/ Maturity Level Two	N° Red Processes + N° Green Processes >=3
it mark	No more than one Red Category>50%	Level 1	Class C Maturity Level Two	**Class B**: No more than 2 Red Processes. (These cannot be PP, PMC). **Class C**: Class C: No more than 2 processes reach less than 50% (These cannot be PP, PMC).

Figura 2.5: Níveis de Certificação ITmark
[19]

2.2.3 Adoção do ITmark

O ITmark é amplamente adotado no continente americano, especialmente nos países latino-americanos, porque as entidades de IT são constituídas por poucos elementos e pequenas infra-estruturas e não podem gastar muito quando se trata de realizar uma auditoria. É por isso que esta certificação é selecionada e tem muito sucesso.

Na figura 2.6, podemos observar o número de países que adotaram ITmark e na figura 2.7, visualizamos o número de certificados ITmark atribuído por nível de certificação. Como pode ser

Country	Certificates
Colombia	146
Spain	21
Portugal	14
Bulgaria	10
Republic of Macedonia	7
Mexico	7
Moldova	6
Brazil	5
Albania	5
Peru	4
Republic of Kosovo	3
Serbia	4
Croatia	2
Bosnia and Herzegovina	2
Armenia	2
Ecuador	1
Argentina	1
Perú	1
France	1

Figura 2.6: Adoção mundial do ITmark
[8]

visto na figura 2.7 [8], Portugal é o terceiro país no mundo com mais certificados ITmark após a Colômbia e a Espanha.

2.2.4 ITmark e proteção de dados

A informação assume um papel extremamente importante nas organizações atualmente pois é um fator preponderante para tomadas de decisões. Assim, a implementação de modelos de proteção de informação é um ponto chave para todas as empresas de software. Devido aos vários riscos e ameaças que enfrentam atualmente, torna-se claro que algo deve ser feito para evitar grandes perdas de informação.

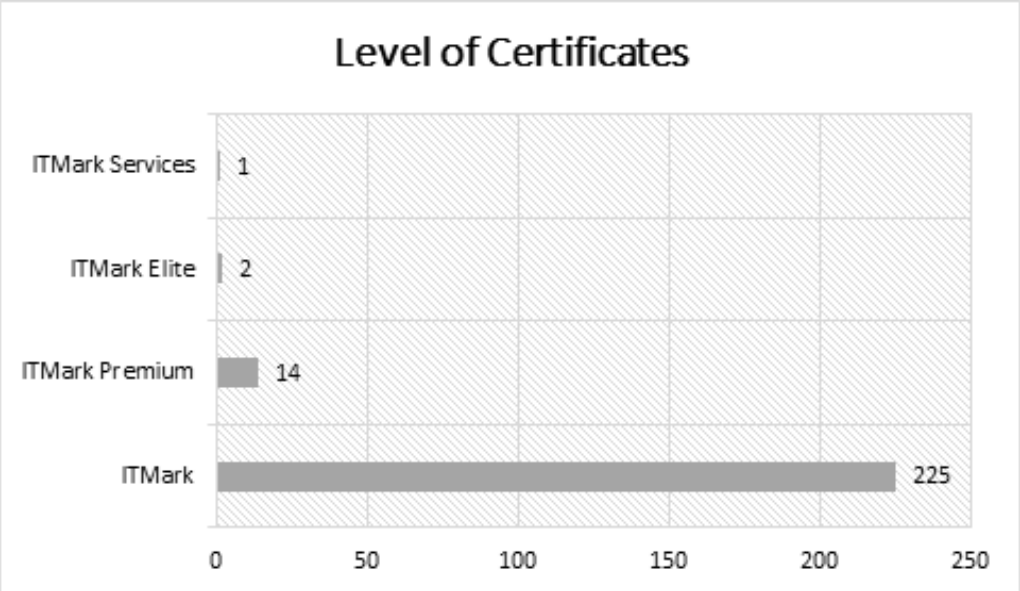

Figura 2.7: Numero de certificados atribuídos por nível
[8]

Além disso, com a implementação do RGPD, alguns requisitos precisam de ser cumpridos, porque, caso contrário, as entidades enfrentarão grandes penalidades. Como referido anteriormente na secção sobre os componentes do ITmark 2.2.1, o ISO 27001 é uma das partes que constituem a estrutura do ITmark, para que possamos usar o ITmark como uma solução para resolver os requisitos do RGPD. A ISO 27001 é uma norma para a gestão da segurança da informação, mas que necessita de ser adaptada para o desenvolvimento de software. Com a crescente dependência da tecnologia e sua exposição a um crescente número de ameaças e vulnerabilidades, é necessário que as empresas tenham um sistema eficiente de gestão de segurança da informação que inclua políticas, processos, gestão de riscos e seus ativos de informação.

O acesso a informações confidenciais hoje tornou-se um fator chave que resulta no sucesso do negócio. A este respeito, a segurança adequada da informação e dos sistemas que a processam é fundamental para o funcionamento de todos os negócios. Portanto, as organizações devem entender e melhorar o estado atual do seu sistema de gestão da informação para garantir a continuidade do negócio. Para isso, é necessário preservar as três propriedades do SI:

1. Confidencialidade - Propriedade na qual a informação não é divulgada às entidades do sistema se esta não tiver sido previamente autorizada.

2. Integridade - Propriedade na qual a informação não é alterada, destruída ou perdida de forma não autorizada ou acidental.

3. Disponibilidade - A propriedade de um sistema ou recurso do sistema é acessível e utilizável por uma entidade de sistema autorizada de acordo com as especificações de desempenho do sistema.

A segurança da informação não precisa de ser considerada apenas como uma solução técnica. Deve ser considerado como um sistema integrado que interage com outros sistemas dentro da organização, tais como:

- Regulamentos - Padrões e Diretivas Legais;
- Estrutura Organizacional - Responsabilidades e Papéis;
- Metodologias- Políticas e Estratégias;
- Controlos - Processos, Procedimentos e Controlos [19].

Hoje em dia, a informação é um recurso, sem a qual muitas organizações não funcionam. No entanto, no mundo interligado em que vivemos, a informação é muito mais vulnerável e valiosa.

Atualmente, o ISO / IEC 27000 é uma norma extremamente utilizada para padrões de segurança de IT, abordando requisitos de gestão, identificando áreas específicas de controlo de segurança da informação. O seu processo adapta-se às necessidades de segurança de qualquer tipo de organização e aos seus padrões que descrevem cenários de uso da norma.

Mesmo sendo uma referência na maioria das empresas que implementaram o ISO / IEC 27000, o modelo é limitado quando se trata de equipas de desenvolvimento de software, e é necessário preencher esta lacuna e indicar e estabelecer diretrizes específicas sobre este assunto.

2.2.5 ITmark e alinhamento com Scrum

Na dissertação, irei focar-me no mapeamento entre ITmark e Scrum, pois é importante para as pequenas empresas não só adotar a estabilidade usando o ITmark, mas também a agilidade na entrega do seu produto, para isso, o uso do Scrum é importante.

O principal problema que encontrei é a falta ou a ausência de recursos sobre ITmark como solução para a melhoria de processos. Contudo um dos recursos principais do ITmark é o CMMI-DEV nível 2 e 3 de maturidade. E como tal crucial para concretizar este alinhamento, assim baseei a minha pesquisa nas áreas de processo CMMI-DEV e nos métodos Scrum, para dessa forma executar o mapeamento entre estes dois inputs para entender como é feito e de que maneira poderá ser uma solução para um dos problemas levantados na motivação da dissertação.

Os primeiros adotantes do CMMI-DEV (anteriormente CMM) eram as indústrias aeroespacial e de defesa dos Estados Unidos. Com o sucesso alcançado estes modelos foram adotados por organizações de grande porte no setor tecnológicos e automotor. Os primeiros adotantes aplicaram o CMMI-DEV para melhorar as existentes operações tradicionais, como *waterfall* [9].

Reconhecido como um modelo que alinha os métodos com os objetivos da organização, preenche lacunas. Instala uma cultura de melhoria contínua para elevar o alinhamento estratégico e o desempenho da organização independentemente dos métodos particulares em causa.

No desenvolvimento de software, o movimento ágil por sua vez começou a crescer e automaticamente a ser abordado pelas empresas de desenvolvimento de software. Com características

como a flexibilidade, rapidez, capacidade de melhoria, a colaboração e ao mesmo tempo a capitalização da força dos indivíduos e a confiança pessoal tornou-se claramente um conjunto de métodos extremamente popular. A adoção do movimento ágil cresceu exponencialmente ao longo da década, em grande parte como uma reação às características *low-trust* das abordagens tradicionais favorecidas pela maioria das organizações que desenvolviam software na época.

As metodologias ágeis abandonam muitos dos eventos e comportamentos tradicionais favorecidos pelas organizações de *waterfall*, escolhendo albergar auditorias de projetos e medidas tradicionais.

Atualmente, a metodologia ágil mais popular é o Scrum [9], uma abordagem colaborativa para gerir o trabalho que enfatiza as iterações curtas, fixas e temporizadas, com equipas pequenas e consistentes e com planeamentos de curto prazo. Como tal, muitos dos primeiros implementadores de Scrum são pequenas organizações ou pequenas equipas em organizações maiores [3].

Mas porquê *CMMI-DEV* e Scrum? As organizações usam o CMMI para identificar lacunas de desempenho em seus processos, operações e fornecer uma base para a melhoria contínua com base nas melhores práticas da indústria. Ao abordar essas lacunas, as organizações criam a estabilidade que precisam [9].

Como o meu estudo se concentra na necessidade de ajudar as pequenas empresas a obter um melhor processo de desenvolvimento, ITmark é o principal condutor para isso, mas não está completo. As pequenas empresas querem obter agilidade no seu processo e na entrega dos seus produtos, e dessa forma precisamos dos métodos agéis como Scrum pois através deles conseguimos obter isso mesmo, assim o ITmark fornece um mapa do que uma organização deve fazer e o Scrum prescreve como fazê-lo.

À medida que os métodos e as técnicas são adaptados e evoluem, o CMMI fornece as bases sobre as quais as organizações podem adaptar as suas técnicas de forma apropriada à dinâmica do seu ambiente de negócios. Para engenheiros de software, uma simples analogia seria pensar no ITmark como os requisitos para a sua organização e os métodos ágeis como uma instanciação desses requisitos.

CMMI e Scrum são compatíveis, conforme realçado na figura 2.8 na página 15 [13]. No nível do projeto, o CMMI fornece um alto nível de abstração sobre o que não é feito nos projetos e o tipo de metodologia de desenvolvimento que é usado, enquanto o Scrum concentra-se em como os projetos se comportam no desenvolvimento dos produtos. Portanto, ITmark e Agile podem coexistir e criar um sinergia com muitas vantagens para quem implementar ambos [18]. O ITmark claramente pode ser introduzido em um ambiente ágil onde é utilizado numa abordagem iterativa, que é perfeitamente compatível com o ITmark. Podem-se complementar criando uma relação que beneficia a organização. Como podemos observar na figura 2.8 na página 15 [13], percebemos que é possível construir uma relação com Scrum e áreas de processo ITmark. O Scrum fornece ao desenvolvimento de software "How To?"que falta nas práticas recomendadas do ITmark que funcionam bem especialmente com pequenas empresas.

O ITmark também fornece práticas de gestão e suporte de processos que ajudam a implementar, sustentar e melhorar continuamente o uso do Scrum nas pequenas empresas.

Esta é uma abordagem *win-win*, porque as organizações que albergam métodos ágeis como o Scrum lutam com problemas de desempenho e voltam-se cada vez mais para o CMMI-DEV e ITmark para obter resultados comprovados. O ITmark fornece um modelo de melhores práticas para olhar além do desempenho da equipe para aplicar princípios *lean* ao nível do sistema. Em alguns casos, resultou num aumento de 30 a 40 por cento na obtenção de compromissos de *sprint*, um aumento de 30 por cento no número de *user stories* entregues em cada *sprint* e um aumento de 40 por cento na entrega do prazo após a aplicação de CMMI para processos ágeis existentes [6].

Nesta secção podemos observar duas tabelas, que representam o mapeamento entre as áreas de processo CMMI-DEV do Nível de Maturidade 2 e Nível de Maturidade 3 com técnicas específicas dos Métodos Scrum.

CMMI Process Area	Agile	Specific Process
Requirements Management (REQM)	Project Backlog	Kick-off meeting, User stories, Clarifications, Backlog refinement, Review and approval of requirements.
Project Planning (PP)	Sprint Planning	Stories / Sprint Planning Standardization of estimation model.
Project Monitoring & Control (PMC)	Daily Meetings	Daily huddle Meeting, Project Dashboards, Burndown charts, Sprint closure meeting
Supplier Agreement Management (SAM)	NA	NA
Process & Product Quality Assurance (PPQA)	No Audits	Regular Audits by external quality auditor using standard audit checklist Retrospective meetings
Configuration Management (CM)	Configuration tools	Configuration Tools
Measurement & Analysis (M & A)	Measurements as per project dashboard, tools used for project monitoring	Standardized few measurements across the Sprints maintained in standard contract dashboard

Figura 2.8: Mapeamento CMMI nível 2 com métodos ágeis [13]

2.3 Padrões e regulamentos de segurança de informação

2.3.1 Regulamento Geral de Proteção de Dados (RGPD)

O Regulamento Geral de Proteção de Dados (GDPR) é um regulamento que foi aprovado pela União Europeia em 27 de abril de 2017 e diz respeito à utilização de dados privados e à livre

CMMI Process Area	Agile	Specific Process
Integrated Project Management (IPM)	Continuous Integration	NA
Risk Management (RSKM)	Risk Management	Maintain Projects Risk register
Decision Analysis & Resolution (DAR)	NA	NA
Requirement Development (RD)	User Stories	User case documentation
Technical Solution (TS)	Decision on Tooling	Decided at the beginning of the project
Product Integration (PI)	Continuous Integration	Continuous Integration
Verification(VER)	Pair Programming	Peer Review, Peer testing, Code review checklist, Sonar Dashboard
Validation(VAL)	Automated Testing	QTP, CIBORG
Organization Process Focus(OPF)	NA	Innovation workshops, regular tech forums
Organization Process Definition (OPD)	NA	NA
Organization Training(OT)	Agile Coaches	The continuous Agile training program, Innovation workshops. Tracking training using Learning Management system

Figura 2.9: Mapeamento CMMI nível 3 com métodos ágeis [13]

circulação desses dados.

Devido à enorme quantidade de armazenamento de dados que aumentou recentemente, é importante proteger os direitos e a liberdade dos dados pessoais. Numa sociedade onde empresas e indivíduos são capazes de recolher e armazenar muita informação rapidamente e transformá-la, torna-se necessário ser mais rigoroso. Esta nova regulamentação irá mudar a forma como as empresas gerem os seus dados e dos seus consumidores, será possível aceder, alterar, transferir, excluir e solicitar os dados como consumidor, fornecedor ou empregado [10].

Assim, as entidades terão que entender esta nova regulamentação e adaptar nos seus sistemas, processos e modelos de organização. Caso contrário, irá resultar em multas pesadas e sanções às entidades, que não respeitam os regulamentos determinados. Exemplos deste tipo de sanções são vinte milhões de euros ou 4 por cento do volume financeiro global do ano anterior se o regulamento

não for respeitado.

Esta nova regulamentação passa por uma hetero-regulação onde a entidade avisa a Comissão Nacional de Proteção de Dados sobre as operações que eles vão realizar. Neste modelo, todas as entidades assumiram a responsabilidade pela interpretação de dados e operacionalização de acordo com o novo regulamento.

As principais mudanças em relação ao regulamento anterior são a inclusão de um gestor de proteção de dados responsável pela gestão desses dados, exigência do consentimento pessoal ao utilizador, grande transparência no uso dos dados pessoais. Dois novos direitos, o direito ao esquecimento e à portabilidade.

No que diz respeito ao desenvolvimento de software, ainda não exista uma maneira específica de cumprir este regulamento e com isso são geradas preocupações por parte das empresas.

O uso do ITmark para melhorar o processo de desenvolvimento nas empresas traz automaticamente a proteção de dados, mais precisamente a ISO 27001 como um dos seus componentes, como uma preocupação principal, mas é muito generalista, apenas refere o que precisa ser feito, em geral e não para processos como o de desenvolvimento de software.

Portanto, o RGPD com o uso da ISO 27001 e algum refinamento, aparece como uma solução porque indica o que precisa ser feito e fornece instruções. Por exemplo, a ISO 27001 indica que é importante coletar dados sensíveis e seus requisitos, por isso é importante referir que tipo de dados precisam ser recolhidos e quais requisitos de segurança devem ser usados para tal [14].

Assim, durante esta pesquisa, um dos objetivos é adaptar o RGPD para a área do processo de desenvolvimento e entender como é que essa regulação irá mudar e transformar as rotinas e hábitos diários das empresas de desenvolvimento de software. Isso incluirá tópicos como estrutura, software, design e sistemas para proteger dados importantes e sensíveis que respeitem a regulamentação e os requisitos de segurança. Quanto a informações privadas, surge aqui um novo desafio porque o cliente tem o direito de editar, alterar e excluir informações pessoais a qualquer momento. Isso traz novas preocupações e, provavelmente, em certos casos, a modificação ou a criação de uma nova rotina / processo por completo. Sobre as empresas, é importante manter em segurança seus artefactos e rotinas de construção e que estejam de acordo com o RGPD.

2.3.1.1 RGPD em entidades de desenvolvimento de software

Para garantir e poder demonstrar que as entidades operam e realizam o processamento de dados pessoais de acordo com os requisitos estabelecidos no RGPD, os principais impactos da regulamentação, informações utilizadas e implementadas devem considerar diferentes aspetos como o nível de adoção de medidas de segurança da informação e nível de medidas dos requisitos funcionais dos sistemas.

Ao mesmo tempo, o desenvolvimento destas medidas deve garantir o cumprimento dos requisitos de confidencialidade e tratamento não discriminatório. O RGPD é mais do que apenas segurança de informação, gestão de dados ou treinamento de funcionários. É uma legislação complexa e abrangente, que inclui muitos componentes que tocam as organizações de várias maneiras e níveis.

O RGPD é apenas o mais recente no crescente número de regulamentações que precisa de um forte programa de gestão da informação para ter sucesso. É necessária uma abordagem abrangente, levando todos os seus aspetos em consideração [17].

No entanto, quando falamos sobre a implementação do novo regulamento em entidades de software, o caso muda, porque este regulamento identifica as falhas principais de uma forma geral. No desenvolvimento de software, é importante ser mais incisivos e específicos, porque um pequeno caso de uso indevido pode levar ao não cumprimento das regras do regulamento [14]. Portanto, é importante padronizar este regulamento e ajudar as empresas de desenvolvimento de software a implementá-lo. Para garantir e poder demonstrar que as entidades operam e executam o processamento de dados pessoais de acordo com os requisitos estabelecidos no RGPD.

Assim, existem alguns métodos e exemplos que podem ajudar as entidades de desenvolvimento de software a desenvolver as suas atividades de forma a cumprirem o novo regulamento geral de proteção de dados.

Alguns exemplos são:

- Criação de uma rede distinta para os diferentes tipos de dados e fluxos como desenvolvimento, pré-produção e produção, assegurando a máxima proteção de todas as informações, especificamente os dados pessoais;
- Restrição às instalações de acordo com seu *status* e função do trabalho, identificando e autenticando todos os utilizadores da instalação;
- Identificação de partes interessadas que são representantes dos departamentos de RH, Marketing, IT, Formação e Dados Pessoais.
- Entrevistas e workshops;
- Uso da segurança lógica, por exemplo, não autorizar a instalação de software que não é aprovado pela empresa e que rastreie os privilégios atribuídos aos contribuintes dos componentes;
- Instalação de mecanismos contra ameaças externas;
- Inventário de cada componente de IT aprovado pela empresa.
- Definição de políticas internas sobre desenvolvimento e sistemas de softwar;
- Desenvolvimentos de software devem ocorrer em sistemas segregados com medidas de segurança adequadas ao tipo de dados tratados;
- Realização de testes durante o processo de desenvolvimento;
- Criptografia de dados, incluindo dados pessoais, informações da empresa.

Estas representam algumas das medidas de segurança que ajudam as empresas, mas há uma necessidade de ser mais específico, até mesmo indicar melhorias neste regulamento em casos como

equipas de desenvolvimento de software, porque elas serão claramente afetadas e é importante estar preparado para mudar o seu status quo a fim de satisfazer a nova regulamentação [2].

2.3.2 Família de padrões ISO 27000

A indústria de software preocupa-se muito com a informação porque a informação e seus sistemas interligados são a base de todas as empresas, por isso é importante construir um plano sólido que mantenha esses dados seguros. Constituído por um conjunto de padrões ISO, como ISO 27000, ISO 27001 e ISO 27002 que se concentram em fornecer controlos, requisitos e diretrizes específicos, com os quais a empresa pode obter segurança de informação adequada [1].

Para a proteção dos sistemas de informação e informação, os padrões permitem um sistema de segurança da informação rigorosamente aplicado e gerido de acordo com um padrão organizacional internacionalmente reconhecido. Também reduz o risco de multas ou compensações devido a disputas legais.

Ao conduzir este estudo, vou-me concentrar nas ISO 27001 e ISO 27002, porque indicam os procedimentos e as melhores práticas, e como referido inicialmente este estudo terá em mente as preocupações com a nova regulamentação de proteção de dados e a ISO 27001 e ISO 27002 fornecem orientação nesse assunto.

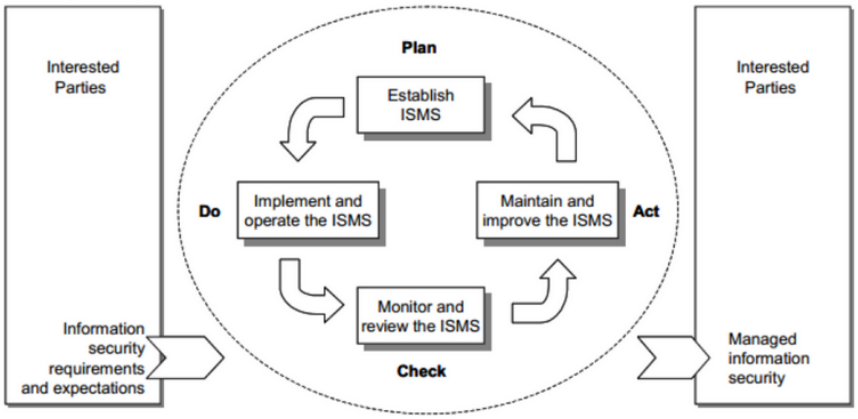

Figura 2.10: Ciclo PDCA na ISO 27000
[7]

2.3.2.1 ISO 27001

O padrão ISO 27001 foi publicado em 2005. Ele descreve os requisitos que um sistema de gestão e segurança de informação (SGSI), deve cumprir para obter a certificação. Destina-se a empresas de todos os setores e de todos os tamanhos. Os requisitos de certificação da ISO 27001 são elucidados através da elaboração de termos e conceitos e complementados com uma diretriz de implementação dentro da ISO 27002 [7].

O ponto focal da ISO 27001 é o requisito de planeamento, implementação, operação, monitorização contínua e melhoria de um SGSI orientado a processos, alinhado com o ciclo PDCA, figura

2.10 [7]. A cobertura e o alcance de um SGSI baseia-se na identificação de riscos, medidas para proteger operações baseadas em riscos, treinamento adequado para implementar os respetivos procedimentos e para estabelecê-los e mostrar a sua importância. O cumprimento dos procedimentos deve ser monitorizado continuamente. As medidas devem ser verificadas e melhoradas continuamente e os riscos de segurança devem ser identificados e avaliados para aumentar continuamente a eficiência do SGSI [7].

Os requisitos, que devem ser aplicados à documentação do SGSI, são descritos no padrão através da estipulação de conteúdo, tais como:

- Processos de mudança e aprovações;
- Controlo de versão;
- Regras para direitos de acesso e proteção de acesso;
- Especificações para sistemas de arquivo.

A melhoria e o desenvolvimento do SGSI devem ser implementados de forma contínua, com base na política de segurança, nos *logs*, na avaliação das operações, nos resultados dos testes e das medidas de melhoria. figura 2.11 na página 20 [5], podemos observar a adoção da ISO 27001 em todo o mundo. Estes resultados pertencem a um relatório elaborado pela ISO / IEC e estão disponíveis no repositório para todos observarem. Assim, como demonstrado, a Ásia Oriental e a Europa são os principais implementadores desta certificação, seguidos pela Ásia Central e América do Norte.

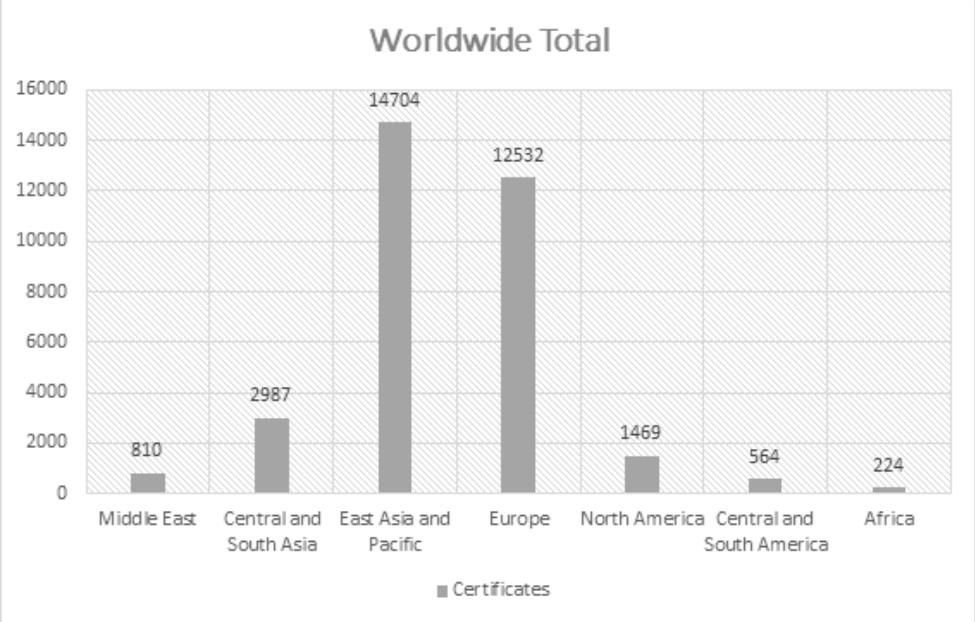

Figura 2.11: Número de certificados atribuídos mundialmente pela ISO 27001 [5]

2.3.2.2 ISO 27002

A ISO 27002 fornece as *guidelines* a implementar no SGSI, demonstra os procedimentos e métodos que podem ajudar na prática, o que pode ser adaptado aos requisitos específicos das empresas.

As etapas necessárias para identificação e avaliação de riscos de segurança são descritas para verificar a forma de proteger informações e sistemas de informação. O desenvolvimento contínuo da ISO 27002 baseia-se na apresentação da ISO 27001, as diretrizes fundamentais para garantir a segurança da informação devem ser definidas e especificadas sob a forma de políticas de segurança pela gestão da empresa. A segurança da informação deve ser organizada e ancorada na empresa para que as medidas de segurança da informação possam ser promovidas e estabelecidas de forma eficiente. Assim, a ISO 27002 mostra exemplos específicos de técnicas e métodos que são importantes para serem implementados nas empresas para fornecer um SGSI confiável.

Departamentos corporativos, têm responsabilidades para manter a confidencialidade e regras para as comunicações com terceiros (clientes, fornecedores, autoridades etc.). Todos os ativos tangíveis e intangíveis que devem ser protegidos pelas medidas de segurança da informação devem ser identificados e classificados para elaborar responsabilidades específicas e regras de manipulação, pois grande parte dos riscos de segurança para os sistemas de IT, surgem de ataques que são iniciados por pessoal interno e outra porção por ações conjuntas de pessoal interno e externo.

Os riscos correspondentes devem ser considerados como medidas de pessoal, como recrutamento e alocação. Do mesmo modo, os processos e procedimentos para circunstâncias excecionais, atrasos, interrupções, falhas ou eventos catastróficos devem ser especificados e documentados. As mudanças técnicas ou organizacionais devem ser verificadas quanto a possíveis efeitos sobre as operações dos sistemas de IT antes de serem implementadas. Os incidentes de segurança devem ser documentados, analisados e avaliados quanto a melhorias possíveis no sistema de segurança.

Concluindo, a ISO 27002 oferece diretrizes e práticas recomendadas que ajudam as empresas a melhorar a gestão e a entrega de informação, identificando todos os envolvimentos de terceiros diretos ou indiretos, que podem influenciar o bem-estar do sistema de informação. Para isso, indica o que precisa de ser feito para cumprir os requisitos e obter a certificação em proteção de informação [7].

2.4 Conclusões do estado de arte

Depois do estado de arte terminado, é possível obter algumas conclusões sobre o que observamos e identificamos sobre a melhoria de processos de software em pequenas empresas.

Há uma grande quantidade de informação sobre melhoria de processos e experiências ligadas ao setor do software. Durante esta pesquisa, encontrei vários casos científicos sobre como proceder para obter uma melhoria de processos em indústrias de software.

Os modelos de melhoria de processos e os métodos ágeis têm muitas coisas em comum e juntos, podem trazer as duas características importantes para as pequenas empresas, que são a agilidade e estabilidade. Ainda assim, para as pequenas empresas, não podemos usar estruturas que sejam muito exaustivas e dispendiosas para a empresa.

Os resultados encontrados baseiam-se sobretudo no uso do modelo de melhoria de processos CMMI-DEV o que torna mais difícil para as pequenas empresas implementarem pois é mais exigente com as suas *guidelines* e exaustivo. Assim o ITmark além de ser o melhor modelo para esta pesquisa é o mais indicado a implementar nas pequenas empresas, mas não existe muita informação científica publicada ou seja, a forma de como é efetuada a avaliação, a forma como são determinadas as falhas, ou se existe uma lista de verificação especifica para cada área da empresa o que é uma desvantagem.

Ainda assim, o ITmark, como referi anteriormente, é muito diversificado, então como na sua constituição usa automaticamente CMMI-DEV de uma forma mais flexível, posso basear a minha pesquisa no CMMI-DEV. O procedimento, para criar e construir este alinhamento entre eles, será baseado na seleção das áreas de processo do CMMI-DEV e nos eventos Scrum e suas respetivas práticas de forma a cobrir as áreas de processo CMMI-DEV, para determinar se ao implementar Scrum automaticamente estamos a cobrir os requisitos de avaliação e certificação do ITmark e vice-versa.

Outra questão sensível é a implementação do RGPD, aprovada pela União Europeia. O ITmark contém a ISO 27001 dedicado à proteção de informação, mas quando falamos de desenvolvimento de software, o padrão não é tão específico, e esse é um problema em aberto que precisa de uma solução. Portanto, é importante indicar às empresas de software o que precisam de fazer especificamente, não lhes dando apenas diretrizes genéricas, mas práticas e técnicas especificas para cumprir com este regulamento.

Em seguida será necessário começar por analisar estes três tópicos e entender como combiná-los para obter uma solução que pode ser implementada em pequenas empresas. Os próximos passos serão dedicados ao mapeamento do ITmark com o Scrum.

Em seguida, serão elaboradas algumas técnicas específicas para o RGPD e respetivamente implementadas no processo de desenvolvimento de software, com práticas específicas. O passo final é aplicar esta solução num caso de estudo corporativo e observar os resultados que esta solução pode trazer para as pequenas empresas. Será também efetuada uma recolha de feedback na empresa para determinar se as falhas encontradas e o modelo são relevantes, assim como uma reflexão pessoal sobre se o modelo poderá ser visto como uma solução para este tipo de empresas.

Capítulo 3

ITmark - Refinamento do modelo

3.1 Refinamento de ITmark para Scrum

Um dos objetivos propostos para esta dissertação era endereçar uma preocupação que as pequenas empresas de desenvolvimento de software têm atualmente, que é a obtenção de certificação e a necessidade de obter uma maior agilidade no seu processo de desenvolvimento de software, pois com esta implementação a empresa obtém um mercado mais abrangente e aumenta o seu retorno financeiro.

Partindo do modelo ITmark como base, pois avalia se a prática do modelo está implementada atribuindo a certificação, faltava a implementação de agilidade no processo de desenvolvimento de software.

Este segundo ponto é coberto pela introdução da metodologia Scrum onde através de um mapeamento entre áreas de processo do modelo ITmark e os artefactos e cerimónias Scrum tornou-se possível atribuir a certificação e agilidade no processo de desenvolvimento de software numa única solução.

Este estudo irá ser demonstrado ao longo deste capítulo, onde foi efetuado o mapeamento do modelo de forma ao implementar ITmark e automaticamente cobrir Scrum e vice-versa e que resulta num levantamento de oportunidades de melhoria ao Scrum de forma a obter o máximo de cobertura às áreas de processo ITmark.

3.1.1 Mapeamento entre ITmark e Scrum

Neste capítulo procedemos à implementação do estudo pretendido de forma a cumprir os objetivos identificados inicialmente. Assim procedemos ao refinamento do modelo ITmark, modelo extremamente adaptável, contudo era necessário determinar se o modelo têm a capacidade de se adaptar ao Scrum e ao RGPD e assim garantir os objetivos pretendidos.

Foi então elaborado o refinamento que se baseia na necessidade das pequenas empresas em obter certificação e agilidade no seu processo de desenvolvimento de software agrupando tudo numa única solução. Assim e de forma a corresponder a essa necessidade é efetuado o primeiro mapeamento entre áreas de processo do ITmark e cerimónias, artefactos de Scrum, com o objetivo

de verificar o grau de cobertura do Scrum relativamente ao modelo ITmark e suas áreas de processo pode ser observado com maior especificidade no anexo B na página 65.

As áreas de processo do ITmark selecionadas para efetuar o mapeamento foram as de ***Project Monitoring and Control***, ver figura 3.2, ***Project Planning***, ver figura 3.1 e ***Requirements Management***, ver figura 3.3. Estas são as áreas de processo cruciais para o desempenho da própria empresa quer para a avaliação e certificação. Foi verificado que o Scrum consegue cobrir maioritariamente o modelo ITmark .

Contudo existem melhorias que podem ser realizadas pois algumas das áreas de processo não são totalmente cobertas e implementadas (*Not Implemented*) ou estão parcialmente implementadas (*Partially Implemented*).

Os níveis são atribuídos de acordo com o número de evidências e a sua relevância para a prática específica, o nível de implementação *Not Implemented* é atribuído quando temos ausência de evidências relevantes, *Partially Implemented* quando existem evidências mas que não são suficientes para cobrir a prática específica, *Largelly Implemented* aplica-se quando existem evidências relevantes mas em número reduzido para verificar claramente a prática da atividade, *Fully Implemented* demonstra inúmeras evidências relevantes que cumprem os requisitos da prática específica. Após esta análise são efetuadas e aconselhadas melhorias que possam ser efetuadas, fornecendo *guidelines* para essas práticas, podem ser observadas com mais detalhe na secção 3.1.3 na página 30.

ITmark PP	SCRUM													
	Sprint planning	Sprint review meeting	Daily scrum meeting	Sprint retrospective meeting	Product backlog	Sprint backlog	Release planning	Backlog grooming	Sprint burndown chart	Release burndown chart	User stories	Team estimating	Epics	Level of implement.
Estimate scope of the project	x				x		x	x			x	x	x	F. I
Establish estimates of work product and task attributes	x				x		x	x						F. I
Define Project lifecycle phases	x						x							L.I
Estimate Effort and Costs	x						x	x				x		F. I
Establish the budget and schedule	x						x							L.I
Identify project risks	x	x	x	x										F. I
Plan data management	x				x				x			x		F. I
Plan the project's resources	x													P. I
Plan needed knowledge and skills	x													P. I
Plan stakeholder involvement	x							x						L.I
Establish the project plan	x				x									L.I
Review Plans that affect the project	x			x										L.I
Reconcile work and resource levels	x										x			L.I
Obtain plan commitment	x										x			L.I

Legenda: F.I – Fully Implemented, L.I - Largely Implemented, P.I – Partially Implemented, N.I – Not Implemented

Figura 3.1: Mapeamento entre ITmark e Scrum na área de processo planeamento do projeto (PP)

ITmark PMC	SCRUM												
	Sprint planning meeting	Sprint review meeting	Daily scrum meeting	Sprint retrospective meeting	Product backlog	Sprint backlog	Backlog grooming	Sprint burndown chart	Release burndown chart	User stories	Team estimating	Epics	Level of implement.
Monitor project planning parameters		x	x	x					x				F. I
Monitor commitments		x	x					x	x				F. I
Monitor project risks		x	x			x							L.I
Monitor data management													N. I
Monitor stakeholder involvement		x							x				L.I
Conduct progress reviews		x		x	x		x	x					F. I
Conduct milestone reviews		x						x					L.I
Analyze issues		x	x										L.I
Take corrective action		x			x								L.I
Manage corrective action		x											P. I

Legenda: F.I – Fully Implemented, L.I - Largely Implemented, P.I – Partially Implemented, N.I – Not Implemented

Figura 3.2: Mapeamento entre ITmark e Scrum na área de processo monitorização e controlo de projeto (PMC)

ITmark REQM	SCRUM												
	Sprint planning meeting	Sprint review meeting	Daily scrum meeting	Sprint retrospective meeting	Product backlog	Sprint backlog	Backlog grooming	Sprint burndown chart	Release burndown chart	User stories	Team estimating	Epics	Level of implement.
Understand requirements	x				x		x			x		x	F. I
Obtain commitment to requirements	x				x		x			x		x	F. I
Manage requirements change			x		x								L.I
Maintain bidirectional traceability of requirements		x					x			x		x	L.I
Ensure alignment between project work and requirements		x					x						L.I

Legenda: F.I – Fully Implemented, L.I - Largely Implemented, P.I – Partially Implemented, N.I – Not Implemented

Figura 3.3: Mapeamento entre ITmark e Scrum na área de processo gestão de requisitos (REQM)

3.1.2 Pré-preenchimento do *Appraisal Assistant*

O Appraisal Assistant é uma aplicação de software desenvolvida pelo Instituto de Qualidade de Software, *Universidade Griffith*, para apoiar a avaliação da capacidade de processos e maturidade organizacional. Segue de perto abordagens consistentes como: avaliação de processos e os requisitos de avaliação para CMMI. Ao contrário de outras ferramentas existentes, o appraisal assistant tem uma abordagem explicitamente orientada a evidências e para registar as informações geradas numa avaliação.

O pré preenchimento do Appraisal Assistant,[1] serviu como uma ferramenta de apoio para mapearmos as cerimónias e artefactos de Scrum com as áreas de processo de desenvolvimento de software ITmark. Com este mapeamento conseguimos ter uma visualização da cobertura do Scrum relativamente ao ITmark.

Este pré - preenchimento é importante também para ajudar os auditores que enfrentam dificuldades quando têm de encontrar e mapear evidências de raiz nos projetos. Automaticamente têm uma ferramenta com evidências previamente definidas que cumprem as área de processo do ITmark e assim sabem exatamente o que procurar para cada área de processo, diminuindo o tempo de mapeamento permitindo focar mais o tempo na análise organizacional. Nas figuras 3.4, 3.5, 3.6 nas páginas 28 e 29, podemos observar o trabalho efetuado na ferramenta *Appraisal Assistant*, foram selecionadas as cerimónias e artefactos do Scrum e com base na sua relevância foram mapeadas para as áreas de processo do modelo ITmark, dessa forma obtemos um ficheiro do Appraisal Assistant pré-preenchido que facilita a avaliação ao auditor, obtemos quais as áreas de processo que são cobertas e as que não são cobertas pelo Scrum. Com base nessa análise é efetuado um levantamento de aspetos positivos e negativos nas áreas de processo, onde os aspetos negativos servem como base para a realização das sugestões de melhorias que serão demonstradas na secção 3.1.3.

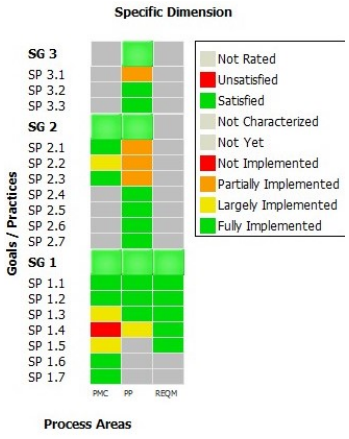

Figura 3.4: Resultado do mapeamento relativamente ao nível de implementação das práticas entre Scrum e ITmark

[1] Ficheiro disponível em https://github.com/drti1994/Appraisal-Assistant

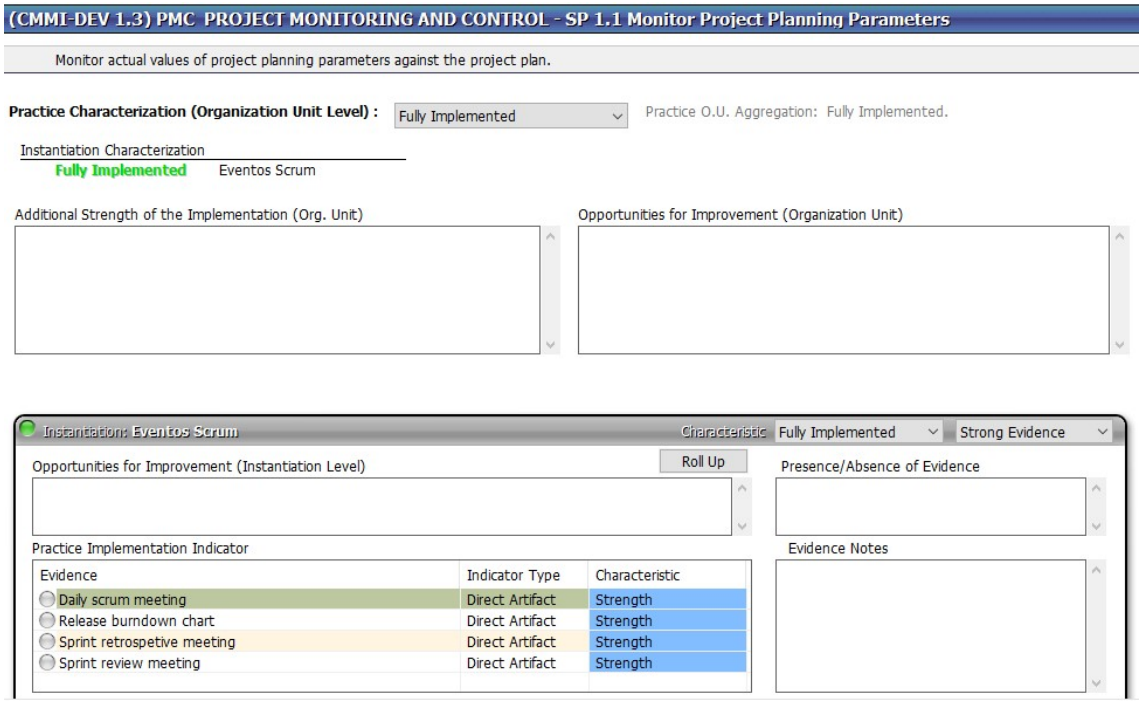

Figura 3.5: Exemplo de Mapeamento dos artefactos e cerimónias Scrum com uma prática específica de ITmark

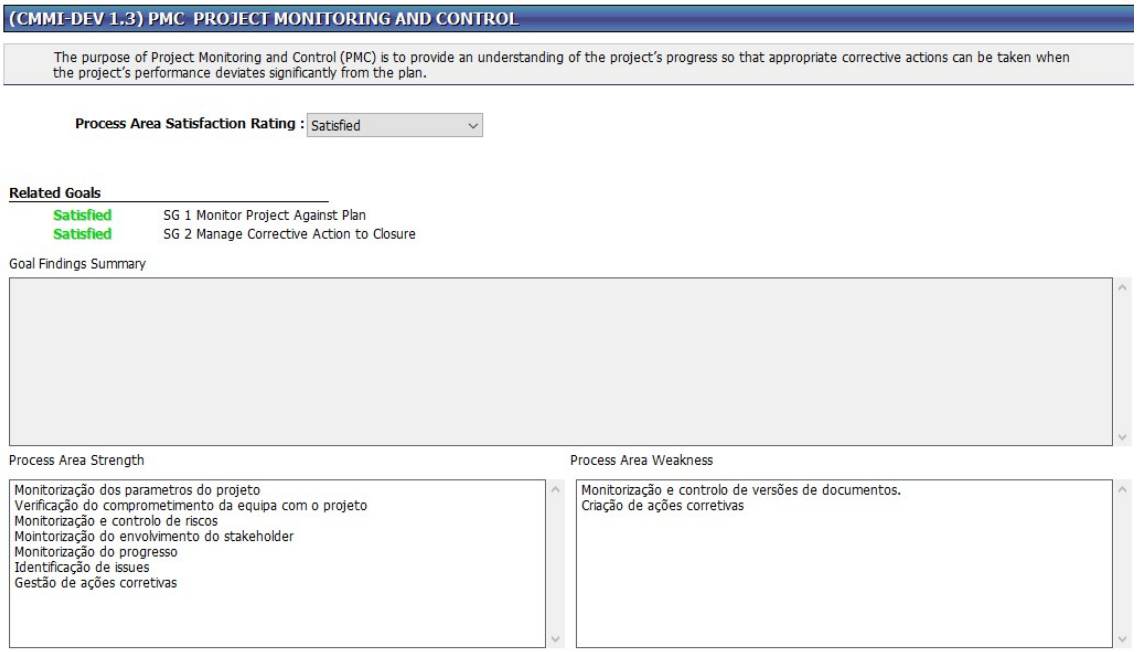

Figura 3.6: Exemplo de aspetos positivos e negativos da área de processo PMC resultantes do mapeamento de evidências entre Scrum e ITmark

3.1.3 Lacunas e sugestões de melhorias

Na primeira área de processo ***Project Planning***, apesar de estar ligada com as cerimónias do Scrum, existem algumas que necessitam de um refinamento. Como no caso da prática específica ***Estimate Efforts and Costs***, onde o cálculo do esforço é claramente endereçado no Scrum, recorrendo ao uso das *user stories* e *sprints*, mas que para o cálculo do custo não se encontra nenhuma técnica. Como tal, uma das soluções, recorrendo aos eventos Scrum, pode passar por calcular os custos da seguinte forma. Começar por calcular o custo da equipa, com base nas horas para cada *Sprint*. Por sua vez, multiplicar a taxa de cada membro da equipa pelo número de horas de trabalho por semana, em seguida, multiplicar esse valor pelo número de semanas num *Sprint*. Calcular os custos dos recursos e extras, como tecnologia, licenças, equipamentos e viagens. Normalmente, não precisam ser calculados para cada *Sprint*, pois costumam ser preços fixos. Após todas as *users stories* serem apresentadas, devemos dividi-las em tarefas para ter uma perspetiva aproximada de quantas horas/homem são necessárias e assim conseguimos encontrar os custos totais que o projeto terá para a organização.

Quanto à prática específica ***Establish the budget and shedule*** é mais um exemplo de uma prática que está parcialmente implementada pelo Scrum, que cobre o planeamento da calendarização recorrendo à *user story* e ao cálculo do seu esforço, que resulta em iterações as quais são atribuídas um número de semanas e que dessa forma permite definir um prazo quer para a equipa , quer para a entrega do produto. Contudo o planeamento do orçamento não é abordada pelo Scrum. Como sugestão pode passar pelo seguinte: de uma forma simples passar por iterações/*sprints* onde são definidas iterações limitadas (por exemplo, sprints de 4 ou 2 semanas). A equipa, completa o máximo possível de *user stories* na quantidade de tempo estabelecida e do preço definido inicialmente com base no esforço ou em projetos anteriores. Todas as histórias ou pelo menos as necessárias devem ser concluídas em acordo com o cliente.

Na prática específica ***Identify project risks***, podemos confirmar que apesar das equipas recolherem impedimentos regularmente em eventos Scrum como *Daily Scrum Meeting* e *Sprint Review Meetings*, não é totalmente o esperado pelas diretrizes do ITmark, que refere que devemos manter uma documentação ativa e atualizada sobre a gestão de riscos. Como solução poderemos implementar um *template* baseado na norma ISO 27005 que foca claramente os riscos que podem afetar o desenvolvimento e todo o procedimento para a conclusão do projeto. Um exemplo de artefacto direto pode ser uma matriz de gestão de riscos extremamente usual no desenvolvimento de software, que deve ser mantida atualizada ao longo do projeto.

Na prática específica ***Review Plans that affect the project***, é a prática especifica que não tem nenhum evento associado ao Scrum, porque basicamente é uma função que pode ser realizada presencialmente por parte da gestão. Contudo, e de encontro ao nosso objetivo de termos um cobertura total deste ponto, é importante indicar uma solução. Como tal, o uso de um *plan charter* poderá ser a solução pois aborda outros planos, tais como o *project plan*, *risk plan* que estão diretamente ligados ao projeto. Basta então manter uma documentação atualizada e com versões para dessa forma cobrirmos esta prática específica. Estas sugestões de melhorias da área de processo

planeamento do projeto podem ser observadas na figura 3.7.

Quanto à área de processo, ***Project Monitoring and Control***, verificamos que a grande maioria das práticas específicas encontram-se claramente cobertas, contudo quatro práticas necessitam de atenção para se adequarem ao ITmark. A primeira é a prática específica ***Monitor Data Management***; o Scrum não refere claramente a necessidade de manter um registo sobre informação e dados criados durante as suas cerimónias, contudo para uma melhor gestão do processo e manter um suporte à informação digital torna-se um ponto importante a implementar.

O que nos é referido como artefacto direto na prática específica é manter um registo da informação sobre as atividades realizadas durante o projeto, sobre os riscos e impedimentos encontrados e sobre os resultados e alterações dessas atividades.

Com base num componente característico do ITmark, a ISO 27001, podemos aproveitar algumas boas práticas que não são de todo excessivas e que ajudam a cobrir este ponto. Exemplos de artefactos são manter um registo automático dos *logs* das atividades de desenvolvimento. Registar alterações efetuadas nos requisitos sejam no *product backlog* ou no *project plan*. Quanto aos riscos poderá simplesmente manter-se um registo do plano de contenção de riscos e suas alterações, por exemplo criação de versões de cada vez que é alterado algum ponto. Outros exemplos de artefactos são atas de reuniões, ações corretivas, *checklists*, histórico de alteração de documentos e documentação pós incidente.

Quanto à prática especifica ***Analyse Issues***, o ITmark refere a necessidade de manter uma lista de *issues*. Esta atividade já está inerente nas *daily scrum meetings* onde são identificados impedimentos ao projeto, mas para tornar mais eficaz este procedimento seria interessante utilizar por exemplo um "*scrumboard* de *issues* onde estes seriam ordenados de acordo com o seu risco para o projeto. Outro exemplo é manter os registos desses mesmo impedimentos que muitas vezes são descritos em *flip charts*.

A prática específica ***Take corrective Action***, não é completamente coberta pelo Scrum. É uma atividade realizada nas *daily scrum meeting*. Apesar disso, o ITmark refere que nesta atividade se deve de criar um plano para executar no caso de ser necessário efetuar alguma alteração. Um exemplo é o plano de riscos que pode ser adaptado para impedimentos onde são identificados e indicados os passos necessários a executar para colmatar o risco.

Por fim na prática específica ***Manage Corrective Actions***, que se caracteriza por manter um registo dos resultados da gestão de ações corretivas, podemos determinar que na maior parte das vezes esta atividade é feita pelo líder da equipa ou pelo *product owner*. Muitas vezes é simplesmente presencial. Esta ação pode ser absorvida fazendo uso de *sprint burndown charts* ao determinar o tempo que levou a efetuar essa alteração. Pode ser alinhada também com o uso de um *workflow* de monitorização assim com um *template* específico para registar esta informação. Estas sugestões de melhorias da área de processo monitorização e controlo do projeto podem ser observadas na figura 3.8.

Em suma o Scrum e o ITmark são uma boa solução a implementar nas pequenas empresas, porque após realizarmos este mapeamento e descrição de algumas *guidelines* verificamos que é possível implementar ambos com sucesso. Assim demonstramos a existência de uma solução

acessível que implementa práticas ágeis e maturadas com o intuito de ajudar e fornecer as características necessárias às organizações para obterem melhorias no seu processo, obter a certificação e capacitar os seus auditores com uma melhor compreensão sobre esta metodologias e práticas.

Área de Processo PP	Prática Scrum
SP 1.4 - Estimate Effort and Cost	• Registo automático de logs das atividades. • Registar alterações efetuadas nos requisitos sejam no "product backlog" ou no "project plan".
SP 2.1 - Establish the budget and shedule	• Iterações. • Budget - Atribuir um número de user stories a cada projeto e calcular com base no esforço e projetos anteriores.
SP 2.2 - Identify Project Risks	• Matriz de Gestão de Riscos.
SP 3.1 - Review Plans that Afect project	• Plan Charter.

Figura 3.7: Sugestão de melhorias para a área de processo monitorização e controlo do projeto (PP)

Área de Processo PMC	Prática Scrum
SP 1.4 - Monitor Data Management	• Registo automático de logs das atividades. • Registar alterações efetuadas nos requisitos sejam no product backlog ou no project plan.
SP 2.1 - Analyse Issues	• Daily Scrum meetings - Identificação de Issues. • Plano de Riscos
SP 2.3 - Manage Corrective Actions	• Uso de sprint burndown charts. • Template indicado para este tipo de registo.

Figura 3.8: Sugestão de melhorias para a área de processo monitorização e controlo do projeto (PMC)

3.2 Refinamento de ITmark para RGPD

O novo regulamento de proteção de dados, irá alterar as operações e o fluxo das empresas. Com as novas alterações, novas preocupações surgem, como tal é necessário procurar soluções de forma a evitar as multas e a cumprir a regulamentação.

Estas preocupações enquadram-se claramente na melhoria de processos de software, sobretudo no que toca à recolha da informação pessoal e ao seu tratamento. Este ponto afeta claramente o desenvolvimento de software, pois muitas tarefas consistem na recolha de informação pessoal como

são os casos da recolha de requisitos, nos testes de software assim como no design e manutenção do software.

Como um dos objetivos da dissertação é importante corresponder às necessidades das pequenas empresas de maneira a que se consiga englobar o máximo de dependências existentes.

O ITmark claramente tem valias para suprir este aspeto recorrendo a ISO 27001 e ao CMMI nível 2. Como ambas as *frameworks* apresenta um conjunto de recursos com valias que são capazes de suprir todos os artigos e regulamentações apresentados pelo RGPD.

Contudo, o RGPD abrange e avalia inúmeras áreas de processo de negócio, o que torna necessário uma pesquisa e um cuidado acrescido, pois o nosso foco é o processo de desenvolvimento e de que forma é afetado com estas alterações e o que necessita de ser alterado para cumprir este mesmo regulamento.

Apesar de existir pesquisa efetuada sobre o RGPD, é necessário ainda algum trabalho quanto às implicações para o desenvolvimento de software. Existe a necessidade de realizar um *tailoring*, para encontrar soluções, de forma que as equipas de desenvolvimento com dificuldade em lidar com a novas regulamentações tenham um conjunto de *guidelines* que ajude no seu cumprimento. Assim esta secção será dedicada a indicar um modelo de exemplo de como cumprir o RGPD recorrendo ao ITmark, mais precisamente a um dos seus constituintes, a ISO 27001 que nos fornece diretrizes quanto a proteção de informação, com os artigos do RGPD que afetam a área de desenvolvimento de Software.

3.2.1 Identificação de artigos relevantes do RGPD

Nesta secção são identificados os artigos do RGPD que claramente afetam a recolha e definição de requisitos, design, testes e validação assim como manutenção do software.

Estas são as áreas do ciclo de desenvolvimento de software que lidam com dados e informação pessoal, que é umas das principais preocupações do RGPD. E que essencialmente cumprem com as preocupações que temos, que são o uso de boas práticas no desenvolvimento de software no que toca à nova regulamentação de proteção de dados.

O processo passa essencialmente por identificar quais os artigos que afetam as atividades de desenvolvimento de software que são o levantamentos de requisitos, que geralmente poderá envolver o uso de dados pessoais, o desenho e implementação do software, em que importa cumprir com questões de privacidade, manutenção e operacionalização do software e equipamentos organizacionais, preparar o sistema interno da empresa para cumprir com o RGPD. O resultado pode ser observado na figura 3.9 na página 34.

Software Cycle Activities	RGPD	Satisfied If
Software Requirements	Consent (Article 7)	Creation of Terms and conditions and privacy policy (regarding information to be provided by the client) and request client approval via email. Can be an NDA.
	Processing not allowing Identification (Article 10)	The company must ensure the security of personal data during collection, storage, alteration, viewing, communication, and deletion. E.g., use of data masking and pseudonymization techniques regarding third-party personal data present in requirements elicitation documents.
	Right to Rectification (Article 16)	The company must ensure the security of personal data during alteration. Provide mechanisms for updating personal data, like a portal with appropriate access control mechanisms. (Example: create a form in the platform where the user can change personal data.)
Software Design and Implementation	Privacy by Design (Article 25)	Build software products in accordance to privacy framework based in the seven fundamental principles of the RGPD. This includes the right to rectification and the right to be forgotten. (Also: Use a combination of manual reviews, sampling, and scorecard metrics to assess the current design controls and related information-handling practices)
	Privacy by Default (Article 25)	Use only the needed information (Example: If you only need the email form the client, you shouldn't add other information).
Software Testing	The processing of personal data by automated means (Article 2)	Limit the utilization of personal data as test data. Use data masking and pseudonymization techniques whenever possible, and make sure proper consent exists in other cases. Define a risk management plan to prevent and be ready if a violation occurs regarding personal data used as test data.
	Right to be Forgotten and Erasure (Article 17th)	Developers and testers should create methods that allow them to eliminate personal data that they are using for their personal work. So, when the user decides to eliminate his personnel data, the developers and testers should do this with accuracy and security. (Example: remove the specific user data from the test data.)
Software Operation and Maintenance	Cybersecurity and notification of violations (Article 32th)	The system workflow must be ready to determine violations or when a violation happen. (Example: Impact Assessment, Impact evaluation, Risk management)
	The processing of personal data by automated means (Article 2)	Limit the recording of personal data in application logs and its subsequent usage in software maintenance (corrective, perfective, etc.). Use data masking and pseudonymization techniques whenever possible, and make sure proper consent exists in other cases.

Figura 3.9: Levantamento de artigos relevantes do novo regulamento geral de proteção de dados e mapeamento com atividades de desenvolvimento de software, com uso da ISO 27001 para cumprimento desses artigos

3.2.2 Elaboração de questionário complementar para avaliação ITmark e RGPD

Nesta secção pode ser observado o resultado do levantamento efetuado que resultou num conjunto de perguntas a inserir na pergunta 26 do guião original do ITmark referente a proteção de dados, com o objetivo de verificar se as empresa cumprem o regulamento nestes pontos críticos. Desta forma, cobrimos não só o aspeto da segurança da informação como o do RGPD fornecendo um guião único e completo que permite avaliar estas duas áreas. Com este refinamento ajudamos tanto as empresas como os auditores com o desenvolvimento de um um instrumento de avaliação único que permite a redução de custos para as empresas e ajuda os auditores na redução de tempo e na qualidades das suas ferramentas para a avaliação. O resultado do levantamento pode ser observado na figura 3.10 na página 36.

Atividades Desenvolvimento Software			
Requisitos de Software - Perguntas	**Desenho e Implementação de Software - Perguntas**	**Testes de Software - Perguntas**	**Manutenção e Operacionalização do Software – Perguntas**
1. A organização faz uso de dados pessoais? Existe algum tipo de consentimento por parte do cliente, fornecedor, etc.? 2. A organização usa técnicas que não permitem a identificação do utilizador em causa? (Pseudonimização) 3. A organização assegura ao utilizador a possibilidade de alteração dos dados em uso para pesquisa e desenvolvimento?	4. A organização produz o seu software de acordo com a framework de privacidade são tidos em conta os sete fundamentos? (Possibilidade de esquecimento e retificação). 5. A organização usa apenas os dados necessários à sua pesquisa? (Privacy by default, não usa dados desnecessários que podem resultar em desvantagens).	6. A organização tem em atenção o processamento de dados por meios automáticos de processamento? 7. A organização contempla medidas e técnicas que permitem a possibilidade de apagar todos os dados de um respetivo utilizador? (Right to be Forgotten and Erasure).	8. A organização consegue detetar, determinar violações caso ocorram no sistema? 9. A organização aplica medidas de segurança quanto a recolha de Logs? 10. Existe um limite de recolha de dados quanto a pessoas e aplicações?

Figura 3.10: Guião de entrevista com perguntas para verificação do cumprimento do novo regulamento geral de proteção de dados

O guião de perguntas é resultado do levantamento dos artigo identificados no RGPD e do mapeamento com boas práticas do componente do ITmark, ISO 27001.

3.2.3 Proposta de alteração de critérios de avaliação ITmark

Como o RGPD é extremamente importante para as empresas é necessário realçar este ponto no guião predefinido do ITmark.

O RGPD é atualmente uma preocupação enorme devido às enormes multas que podem surgir no seu incumprimento, por isso, e após o estudo efetuado, seria importante colocar as subperguntas que estão anexadas na pergunta 26 do guião sobre o RGPD como perguntas obrigatórias.

No caso de alguma delas não serem cumpridas, automaticamente a empresa não cumpre o regulamento assim como o modelo de avaliação de segurança de informação do ITmark. Porque, apesar de parecerem temas diferentes estão claramente relacionado pois se não cumprimos um artigo do RGPD automaticamente estamos a pôr em causa o nosso sistema de segurança de informação.

Assim a sugestão e melhoria passa por esta mudança no guião, na reformulação de cálculo de percentagem, pois até aqui eram sub-tarefas da pergunta 26 e agora passariam a mais 10 perguntas no guião da entrevista, assim como uma mudança nos requisitos de avaliação adicionando estas 10 perguntas como obrigatórias de cumprimento para passar na avaliação do modelo ITmark.

O que resulta em inúmeras vantagens pois ao seguirem esta metodologia, podem agora implementar um sistema de segurança de informação que cumpre ao mesmo tempo a nova regulamentação de proteção de dados evitando incumprimentos, mantendo o prestígio e sem a complexidade de efetuar inúmeras avaliações. Na figura 3.11, podemos observar os critério do ITmark quanto à avaliação da segurança da informação.

Requisitos detalhados da Avaliação de Segurança		
	Respostas "Sim"	Perguntas obrigatórias
Nível 1	**66 %**	**A1, A10, A13, A14, A15, A17, A20**
Nível 2	80 % (grupo perguntas de nível 1) 70 % (grupo perguntas de nível 2)	A1, A10, A13, A14, A15, A17, A20 + B1, B9, B15, B16
Nível 3	93 % (grupo perguntas de nível 1) 80 % (grupo perguntas de nível 2) 80 % (grupo perguntas de nível 3)	A1, A10, A13, A14, A15, A17, A20 + B1, B9, B15, B16

Figura 3.11: Requisitos para obtenção de certificação ISO 27001 no ITmark

Capítulo 4

Caso de estudo

4.1 Contexto e objetivos

O caso de estudo corporativo tem como objetivo demonstrar a aplicação do estudo e pesquisa efetuada anteriormente. Surge após a realização do mapeamento, do ITmark com Scrum e RGPD, para demonstrar que é possível aplicar esta solução no contexto corporativo e que poderá servir como exemplo futuro para empresas que necessitem deste tipo de requisitos. Será dividido em duas fases, a primeira de avaliação quanto ao processo de software existente para determinar as evidências e mapear com áreas de processo ITmark onde serão escolhidos dois projetos da empresa onde é realizado o estudo de forma a comprovar se têm processo de software e se o cumprem. Esta análise recorre ao uso da ferramenta *Appraisal Assistant*, que tem a capacidade de realizar uma mapeamento entre as evidências do processo da empresa com as áreas de processo ITmark. Dessa forma é possível determinar quais as áreas que apresentam lacunas assim como as que já cumprem os requisitos. O resultado será um *gap analysis*.

A *gap analysis* é um relatório que tem por objetivo compreender as práticas e processos atuais de gestão e de engenharia de software da organização e as lacunas em relação a um modelo de referência. É um processo onde, com ajuda do modelo CMMI as organizações podem definir e a manter um processo organizacional uniforme baseado nas melhores práticas quer para desenvolvimento quer para manutenção de produtos. O *gap analysis* avalia a diferença (*gap*) entre as práticas da organização e os requisitos do modelo CMMI-DEV. Obtém evidências que permitem emitir um parecer objetivo quanto ao grau de cumprimento das áreas de processo avaliadas em relação ao modelo. Identifica os principais pontos fortes do processo de desenvolvimento de software da empresa. E determina oportunidades de melhoria: do processo de desenvolvimento de software da empresa.

A outra parte será a avaliação quanto à nova regulamentação de proteção de dados (RGPD). Recorrendo ao questionário de avaliação do sistema de segurança de informação que faz parte do ITmark, foi possível adaptá-lo. Como para esta pesquisa a grande preocupação são os artigos que afetam diretamente as equipas de desenvolvimento de software, foi necessário encontrar soluções que correspondem ao cumprimento da regulamentação. O resultado permitiu acrescentar uma

série de questões ao questionário já existente e que por sua vez resulta numa avaliação à empresa, para determinar se já são aplicadas técnicas e métodos para o cumprimento dos artigos.

Com este caso de estudo corporativo pretende-se verificar se a empresa em questão cumpre os requisitos mínimos para uma possivel atribuição de certificação ITmark. Tem também por objetivo determinar se os mapeamento realizados servem como ferramenta de apoio para os auditores e facilita a sua análise em termos temporais e de desempenho. Por fim surge como uma ajuda para a empresa, quanto à identificação de falhas e dessa forma melhorar o seu processo para atingir uniformidade nas suas atividades.

4.2 Caracterização da organização

O caso de estudo corporativo foi realizado numa organização de desenvolvimento de software. A organização cumpria os requisitos para a implementação desta pesquisa, ou seja, pretendia obter uma certificação quanto ao seu processo de desenvolvimento de software, tinha a necessidade de tornar o seu processo mais rápido e pretendia corresponder à nova regulamentação de proteção de dados. A equipa de desenvolvimento é constituída por 25 elementos e dessa forma cumpre o critério como pequena empresa.

O objetivo da empresa caracteriza-se pelo desenvolvimento de soluções inovadoras para o comércio *online*. Conta com uma enorme experiência e um vasto leque de projetos que sustentam o crescimento.

A empresa é focada no desenvolvimento de plataformas *E-Commerce*, como o *business to business* (B2B), onde são implementadas operações de compra e venda, de produtos e de serviços através da Internet. Plataformas *business to customer* (B2C), onde os retalhistas obtêm a sua própria loja virtual e colocam os seus produtos possibilitando as compras dos mesmos. Assim aumentam as vendas dos seus produtos junto dos clientes servindo como fonte de enorme retorno.

Desenvolve também sites institucionais onde é demonstrada a caracterização da empresa, ou seja, o seu âmbito, atividades, setor empresarial. Representa o cartão de visita para a organização em causa. Estes são os produtos de desenvolvimento no qual a organização se foca.

Relativamente ao ponto de vista organizacional, a organização é constituída por 8 departamentos: gestão de projeto, design, html, conteúdos, api, implementação, qualidade e *delivery*. Conta também com uma equipa de suporte responsável por lidar com anomalias e duvidas dos clientes.

São estes departamentos que constituem a organização e que são os responsáveis pela entrega e desenvolvimento do produto.

4.3 Análise de práticas de desenvolvimento de software

4.3.1 Metodologia

Como referido anteriormente a primeira fase desta avaliação é avaliar a organização quanto ao processo de software existente para determinar as evidências e mapear com áreas de processo

ITmark nível 1. Como metodologia foi usado um guião de entrevista com perguntas baseado nas áreas de processo ITmark com o intuito de determinar se a empresa cumpre os mínimos exigidos por parte do modelo de avaliação.

As entrevistas foram realizadas a membros da equipa como gestor de projeto, líder da equipa de HTML, implementação, delivery, responsável do processo organizacional da organização. As evidências resultantes dessas entrevistas foram devidamente anotadas.

Os guiões das entrevistas, que podem ser observados no anexo A disponível na página 63, servem também para determinar que evidências são criadas por parte da empresa que mais tarde serão inseridas no *Appraisal Assistant* para retirar ilações quanto ao estado em que se encontra o processo de desenvolvimento.

Depois surge o mapeamento entre evidências e áreas de processo que são inseridas no *Appraisal Assistant*, aí são mapeadas e efetuada a verificação quanto ao seu grau de cobertura do modelo ITmark onde são gerados gráficos e obtemos uma visualização geral do panorama da organização.

O próximo passo são é o levantamento das falhas por áreas de processo e recomendação de oportunidade de melhoria, onde é efetuada uma apresentação, onde estão identificadas todas áreas de processo e para cada uma delas são indicadas essas oportunidades de melhoria. Por fim, e com base nos critérios de ITmark, é dado o veredito final da avaliação onde é fornecido uma percentagem ao cumprimento do modelo de certificação ITmark e é determinado se a empresa passa na avaliação ou se reprova.

4.3.2 Resultados da avaliação

A realização desta análise como referido anteriormente dividiu-se em duas partes: a primeira em entrevistas aos membros da equipa de desenvolvimento gestor de projeto, líder da equipa de HTML, implementação, delivery e responsável do processo organizacional da organização com objetivo de entender como é que as atividades se procedem. Esta atividade permite obter uma visão de quais as áreas de processo que poderão estar em piores condições e que necessitam de uma maior atenção.

A segunda parte é a recolha de evidências, documentação organizacional ou de projeto que indica se a empresa cumpre com determinados requisitos que o ITmark exige. A partir daqui é obtida uma visão geral do estado da organização, do que é necessário melhorar e produzir de forma a cumprir os requisitos da certificação em processos de software.

São então identificadas a partir daqui um conjunto de oportunidades de melhoria por área de processo com o intuito de informar a organização do que é necessário alterar e implementar para obter um processo compatível com o modelo.

Esta prática acaba por sensibilizar os vários elementos e setores da organização para a importância e vantagens de um processo bem estabelecido, que passam desde uma entrega mais rápida e com a mesma qualidade do produto, eliminação de custos, melhor comunicação entre equipas assim como o acesso a informação de forma mais célere.

Depois da primeira fase de análise, onde foram realizadas as entrevistas as áreas de processo de Plano de Controlo e Monitorização, Plano de Projeto e Gestão de Requisitos foi possível obter

uma análise quanto ao ponto de situação da organização. A primeira visualização que é retirada é o nível de maturidade em que se encontra a organização. O nível neste momento é ML1 onde o produto é acabado, mas com atraso, a metodologia utilizada pela organização é *watterfall* com refinamento *Agile*, com base no uso de ferramentas como o *trello*.[1]

A cultura de definição de um processo e fluxo organizacional não está definida, o processo é conhecido com base na experiência e na passagem da palavra, não existe nada físico para que os funcionários assim como a gestão possam consultar em caso de necessidade. Existe uma enorme falta de documentação assim como de recolha de métricas. Não existe uma recolha e identificação de risco a nível organizacional. São falhas extremamente prejudiciais à organização e que podem resultar em perdas.

Na segunda parte da avaliação, que é o mapeamento de evidências com as áreas de processo ITmark, identificamos também bastantes oportunidades de melhoria que, ao serem implementadas, resultariam numa melhoria organizacional. Como na entrega do produto, recolha de métricas, eficiência da equipa assim como melhoria contínua.

A avaliação final é que a empresa não cumpre os requisitos necessários identificados na figura 2.5 na página 10 para obter a certificação do ITmark nivel 1 em processos de software pois não atinge os 50% de cobertura do modelo como podemos observar na figura 4.4 na página 44.

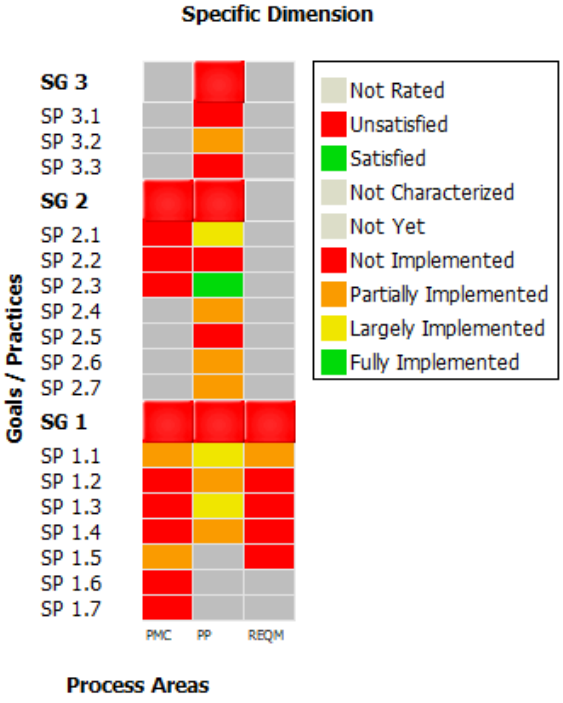

Figura 4.1: Avaliação das práticas específicas da empresa

[1] https://trello.com/

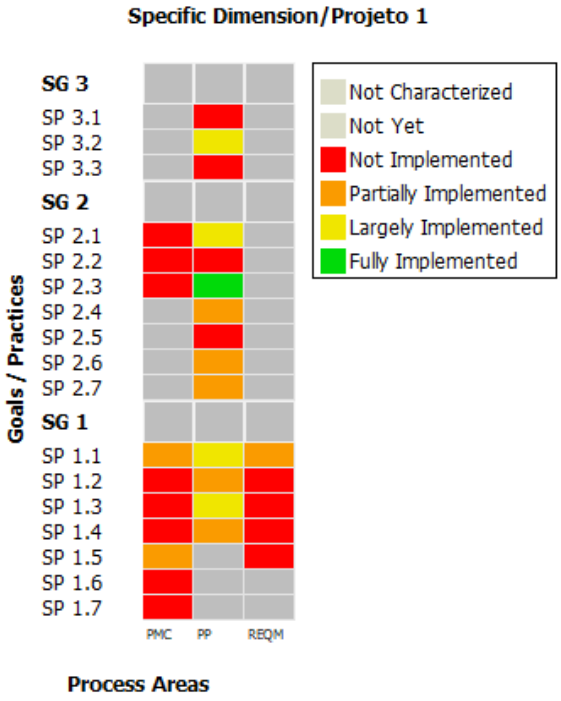

Figura 4.2: Avaliação das práticas específicas do projeto 1

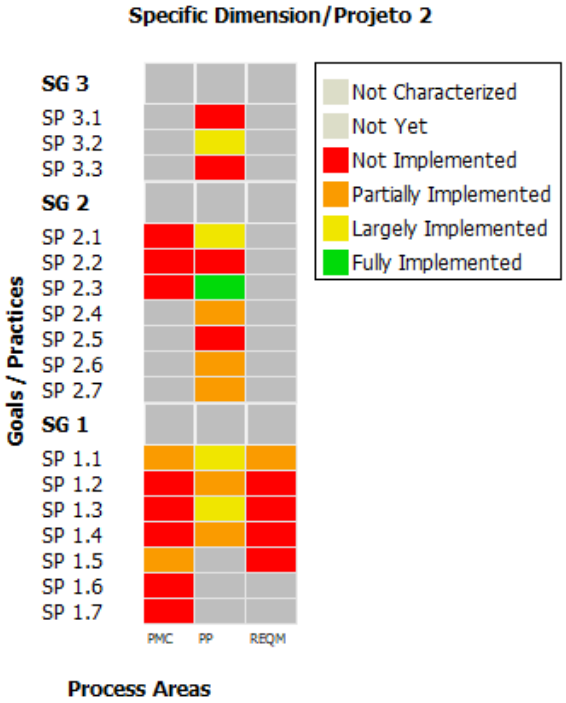

Figura 4.3: Avaliação das práticas específicas do projeto 2

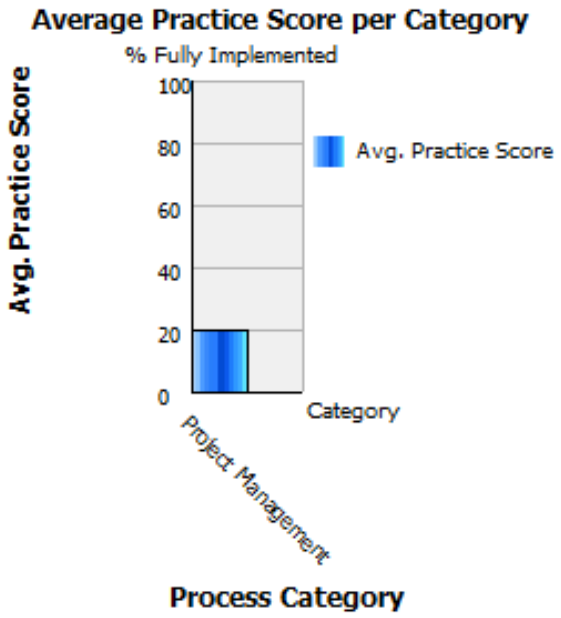

Figura 4.4: Avaliação da cobertura do modelo ITmark de ambos os projetos do caso de estudo

4.3.3 Oportunidades de melhoria

PMC - Monitorização e controlo do projeto O objetivo da monitorização e controlo do projeto (PMC) é fornecer uma compreensão do progresso do projeto e tomar ações corretivas apropriadas quando o desempenho do projeto se desvia significativamente do plano.

- SG 1 Monitoriza o projeto contra o plano: O progresso e o desempenho do projeto real são monitorizados contra o plano do projeto.
- SG 2 Gere as ações corretivas para encerramento: Ações corretivas são geridas para encerramento quando o desempenho do projeto ou resultados se desviam significativamente do plano.

Análise da área de processo

Feita a análise á área de processo de PMC, foram obtidas as seguintes oportunidades de melhoria:

1. Criar um processo organizacional para a empresa;
2. Criar um registo de versões de documentos importantes quer para o projeto, quer para a organização;
3. Implementar e realizar uma gestão de risco de todos os projetos;
4. Realizar análise quanto ao progresso do projeto e às *milestones* de forma mais natural, uniforme e constante. Por exemplo quando passa de um departamento para outro e obter um registo dessa transição. Ter isso refletido no processo;

Figura 4.5: Avaliação da área de processo monitorização e controlo do projeto

5. Auditar os projetos de forma a identificar não conformidades e aplicar ações corretivas;
6. Definir um registo e recolha de ações corretivas;
7. Alguns aspetos a ser monitorizados:
   - Grau de execução das tarefas atribuídas aos colaboradores;
   - Revisão dos riscos;
   - Revisão dos progressos;
   - Indicadores de projeto;
8. Deverá existir um registo (mínimo) das reuniões de acompanhamento do projeto;

PP - Planeamento do projeto O objetivo do planeamento do projeto (PP) é estabelecer e manter planos que definam as atividades de projeto da organização. Dessa forma será possível ter uma visualização de todas as atividades do projeto. Esta área engloba os seguintes objetivos específicos.

- SG 1 Estabelecer estimativas: Estimativas dos parâmetros de planeamento do projeto são estabelecidas e mantidas.
- SG 2 Desenvolver um plano de projeto: Um plano de projeto é estabelecido e mantido como base para a gestão do projeto.
- SG 3 Obter o compromisso com o plano: Os compromissos para o plano de projeto são estabelecidos e mantidos.

Análise da Área de Processo

Feita a análise à área de processo de PP, foram obtidas as seguintes oportunidades de melhoria:

1. Processo Organizacional – Que reflita todas as fases da vida do processo;

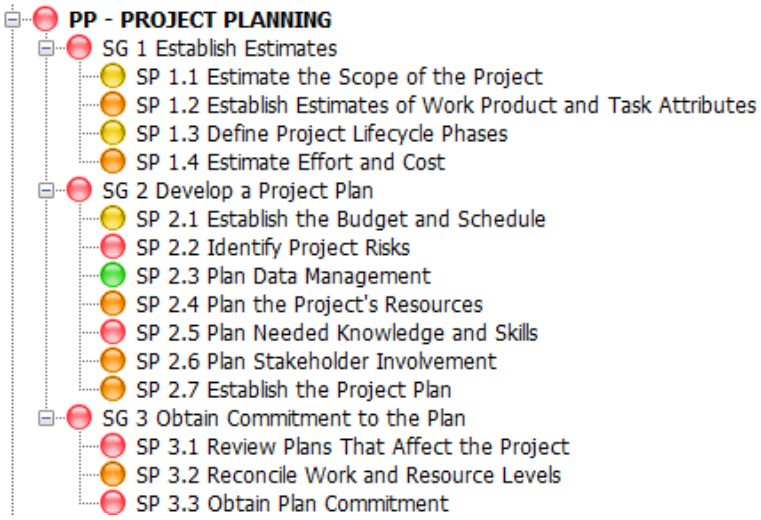

Figura 4.6: Avaliação da área de processo e planeamento do projeto

2. Processo Organizacional – Onde é indicado como criar um plano de projeto e os seus passos;
3. Estabelecer estimativas para as diferentes tarefas do produto (*planning poker*);
4. Estabelecer um Plano de Projeto com as várias fases do processo de desenvolvimento, com inputs e outputs;
5. Plano de Projeto com as seguintes características: Cronograma e calendarização;
6. Identificação de Riscos assim como definição de uma escala com as várias ações a tomar;
7. Estabelecer um sistema de gestão de documentação onde são colocados os documentos importantes a todos os membros que participem no projeto, onde também são registadas as versões desses mesmos documentos;
8. Criar um plano de comunicação onde é identificado o envolvimento dos *stackeholders*;
9. Definir um plano de formação para todos os funcionários onde é determinada a calendarização e periodicidade;
10. Estabelecer as diretrizes para criação do plano do projeto a nível organizacional;
11. Realizar reuniões com os representantes principais da organização de forma a obter um compromisso com o plano de projeto e realizar um registo de forma a verificar que esta compromisso e cumprido;
12. Validar e aprovar o planeamento do projeto com todos os stackeholders relevantes;
13. Garantir que são identificadas e geridas as dependências entre as tarefas e/ou outros projetos caso se aplique;

14. Nas reuniões do projeto verificar se os compromissos estão a ser cumpridos;

REQM - Gestão de Requisitos

O objetivo da gestão de requisitos (REQM), é gestão dos requisitos, dos produtos do projeto e componentes do produto. Pretende também garantir o alinhamento entre esses requisitos e os planos e produtos de trabalho do projeto.

- SG 1 Gestão de Requisitos - Requisitos são geridos e são identificadas inconsistências quer no plano de projeto quer nos produtos de trabalho.

Análise da Área de Processo

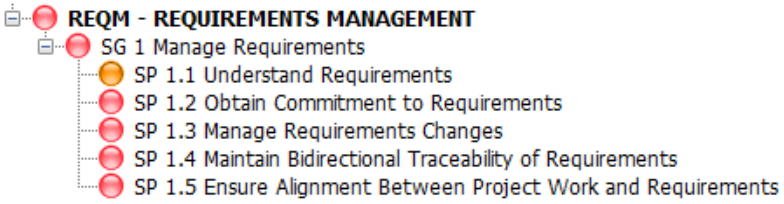

Figura 4.7: Avaliação na área de processo gestão de requisitos

Feita a análise à área de processo de REQM, foram identificadas as seguintes oportunidades de melhoria:

- Definição de um processo organizacional sobre a gestão de requisitos, onde seja demonstrada o processo a realizar na presença de um novo projeto, como produzir os requisitos de acordo com a política da empresa, como é efetuada a sua gestão;

- Realizar reuniões e obter um registo de compromisso de acordo com os requisitos entre a organização e as partes interessadas;

- Realizar uma gestão de requisitos, quando é efetuada uma alteração num requisito verificar o resultado e como é procedida essa alteração (Pedido de Alteração);

- Clarificar como é feita a aprovação dos requisitos;

- Manter uma rastreabilidade de requisitos ao longo do projeto, ou seja, conseguirmos entender as atividades relacionadas com eles;

- Manter um alinhamento entre os requisitos definidos e o produto de maneira a demonstrar uniformidade entre projeto e produto;

4.4 Análise de práticas de gestão de segurança da informação

4.4.1 Metodologia

A análise de práticas de gestão de segurança de informação faz parte da segunda fase da avaliação a organização. Foca-se na avaliação quanto à nova regulamentação de proteção de dados.

Como metodologia foi usado um guião de entrevista que faz parte do modelo ITmark com perguntas baseadas nos vários níveis da norma ISO 27001 e que cobrem o RGPD. O guião da entrevista foi alvo de um refinamento de forma a adaptar quanto as novas necessidades da regulamentação de proteção de dados que pode ser observado na secção 3.2.2.

O nosso foco quanto a esta questão do RGPD foi no desenvolvimento software, ou seja, departamentos que estão associados a esta atividade como requisitos de software, desenho e implementação de software, testes de software e manutenção e operacionalização do software. Estes foram os departamentos identificados que de certa forma podem lidar diretamente com os pontos sensíveis a que o RGPD refere e que podem resultar em coimas para a organização. Este refinamento esta referido no secção 3.2.

Como tal e com base na pergunta 26 do questionário de avaliação de informação do ITmark, foram adicionadas questões com base no mapeamento entre ITmark e ISO 27001, que refletem as grandes preocupações quanto a esta nova regulamentação.

As entrevistas foram realizadas a membros da equipa da organização, gestor de projeto, líder da equipa de HTML, líder da equipa de implementação, líder de equipa de *delivery*, responsável do processo organizacional. Os resultados foram devidamente registados para mais tarde serem analisadas.

Os guiões das entrevistas recolhidos servem também para determinar se a empresa cumpre os requisitos mínimos e fornece ao mesmo tempo uma percentagem de cobertura do modelo por parte da empresa.

Por fim, e com base nos critérios do ITmark (ver figura 3.11 na secção 3.2.3, é dado o veredito final da avaliação onde é fornecido uma percentagem com base no calculo das várias perguntas que determinam se o modelo ITmark é cumprido e por sua vez se a empresa passa na avaliação ou se reprova.

4.4.2 Resultados da avaliação

Na avaliação de Segurança de Informação (SI), participaram os responsáveis pela Qualidade pela Segurança da Informação nas empresas, foram também percorridas os setores de desenvolvimento assim como o perímetro dos servidores. Na realização desta avaliação foram efetuadas 28 perguntas de segurança de informação do nível 1 do ITmark. Dessas questões, 19 têm de ser respondidas com ‘Sim’ para que a empresa fosse aprovada, cerca de 50 % do total de perguntas. A figura 4.8 mostra as questões: As questões destacadas em negrito são as perguntas obrigatórias (também chamadas de *killers questions*). Para obter a certificação Nível *Basic*, nenhuma destas questões deve ser respondida com ‘Não’.

Na figura 4.8 podemos observar as perguntas respondidas com "Sim"e com "Não"e a respetiva percentagem obtida, a percentagem foi calculada através do número de perguntas com "Sim "que foram 18 e divididas por 28 o número total de perguntas, que depois é multiplicada por 100 e dá origem à percentagem final. Depois do cálculo efetuado verificamos se passa no do modelo de avaliação de segurança e se cumpre o nível 1 do ITmark.

No caso da nova proposta do questionário para avaliação do RGPD (pergunta 26), o processo para obter a percentagem de aderência foi o mesmo para o de avaliação de segurança de informação.

O veredito final é que a empresa não passa na avaliação de segurança de informação pois não cumpre uma série de questões obrigatórias do modelo ITmark, apesar da percentagem de 64% no total e no RGPD uma percentagem de 80% pois respondeu a 8 perguntas das 10 do questionário. A empresa precisa melhorar vários aspetos de forma a obter a certificação do Modelo ITmark nivel 1 em avaliação de segurança.

	Perguntas	**Percentagem**	**Obrigatórias**
Perguntas "Sim"	A1, A2, A8, A9, A11, A12, A13, A14, A16, A17, A20, A22, A23, A24, A25, A26(a), A27, A28	**64%**	**A1, A10, A13, A14, A15, A17, A20**
Perguntas "Não"	A3, A4, A5, A6, A7, A10, A15, A18, A19 A21	**36%**	

Figura 4.8: Resultados da avaliação à segurança de informação

Perguntas "Sim"	**Perguntas "Não"**	**Grau de Aderência**
18	**10**	**64%**

Figura 4.9: Quantificação das Perguntas da avaliação de segurança de informação

Perguntas RGPD	**Número de Perguntas**	**Percentagem**
Perguntas "Sim"	A26 - (1), (2), (3), (4), (5), (6), (7), (8)	**80%**
Perguntas "Não"	A26 -(9), (10)	**20%**

Figura 4.10: Resultados da avaliação quanto ao cumprimento do RGPD

Perguntas "Sim"	Perguntas "Não"	Grau de Aderência
8	2	80%

Figura 4.11: Quantificação da avaliação RGPD

4.4.3 Oportunidades de melhoria

Depois de termos realizado as entrevistas aos vários membros da equipa e de termos efetuado o cálculo e avaliação da organização quanto ao cumprimento do modelo de segurança de informação é importante determinar e informar a organização de medidas e práticas que têm de ser tomadas de forma a melhorar o seu processo e boas práticas quanto à segurança de informação. Estas oportunidades de melhoria surgem com base nas perguntas que obtiveram "Não" como resposta, pois não cumprem ou não esta implementada essa prática. Com base no estudo e levantamento realizado são sugeridas as seguintes oportunidades de melhoria.

A3 – Política de segurança ineficaz ou inexistente. A organização possuía uma política de segurança pouco clara e que não contempla todos os itens considerado importantes pelo modelo ITmark.

Solução: Criação de um plano de segurança de informação onde são definidos todos os tópicos que a organização deve abordar, gestão de riscos e medidas de prevenção e ação com base nas boas práticas e requisitos da ISO 27001.

A4 – Implementação de procedimentos padrão no que toca à classificação de informação. Foi verificado que na empresa não existe qualquer implementação nem preocupação com este aspeto.

Solução: Criar processos e documentação onde são descritos o que fazer e realizar quando determinada informação é produzida. Exemplo: Plano de Classificação.

A5 – Verifica-se que na organização não existe nenhum elemento ou departamento definido para gerir segurança da informação o que torna impossível a atribuição de papéis, pois esta metodologia não foi implementada.

Solução: É necessário definir um elemento que leva a cargo essa função. Fornecer formação de forma a criar um processo homogéneo por toda a organização.

A6 – Ficou evidente na organização que não está ninguém identificado como responsável pela segurança da informação, como tal também não temos um substituto no caso da sua ausência.

Solução: Nomear elemento principal para manutenção e gestão do sistema de segurança de informação, instruir outro elemento como substituto no caso da ausência do elemento principal e fornecer a devida formação.

A7 – Outro ponto é o perímetro de segurança. A organização não controla a segurança física e o acesso restrito aos computadores onde são efetuados os desenvolvimentos. Enorme risco de fugas de informação confidencial da organização.

Solução - Instalação de medidas de segurança como dispositivos biométricos nas zonas mais críticas da organização.

A10 – De acordo com o levantamento efetuado na organização não existe identificação única para cada utilizador. Os computadores têm todos a mesma identificação, o acesso a organização pode ser efetuado sem qualquer tipo de controlo e registo. Todos têm acesso a todos os níveis da organização.

Solução - Criar uma identificação exclusiva de acesso aos periféricos e aos departamentos de acordo com a sua classe organizacional.

A18 – As cópias de segurança estão livres ao acesso de todos, não existe qualquer tipo de restrição quanto ao seu acesso.

Solução: Restrição de acesso mediante dos privilégios do elemento se possível. Guardar informação noutro lugar físico seguro.

A19 – Apesar de a organização realizar backups diariamente, estes não são testados o que pode resultar numa falha de configuração ou num ataque de um vírus no momento em que o backup é realizado colocando em risco a segurança dessa informação.

Solução: Criação de backups em mais de um suporte e utilização de um computador para testes de backups estabelecendo um plano de teste com uma determinada periodicidade.

A21 – Não existem responsáveis pela segurança da informação na organização.

Solução: Identificar responsáveis e fornecer formação sobre os aspetos de segurança da informação necessários para desempenhar as suas funções.

A26(9) – Não são efetuadas medidas quanto a recolha de logs por parte de programas de desenvolvimento.

Solução: Após o trabalho realizado pelo *developper* devem-se verificar se não gravaram dados prejudiciais referentes a terceiros. Criar métodos de limpeza automática no final da sessão.

A26(10) – A organização deve recolher os dados estritamente necessários para o correto funcionamento do trabalho.

Solução: Pedir consentimento a terceiros para o uso dessa informação, criar formulários de recolha de dados apenas com a informação necessária.

Capítulo 5

Avaliação final

5.1 Perspetiva do avaliador

Depois de realizada a avaliação e o estudo da organização com base no trabalho efetuado é importante realizar um ponto de situação sobre as expectativas e resultados que obtivemos. Este trabalho pretendia responder a três pontos importantes atualmente para as empresas de desenvolvimento de software que são a obtenção de certificação, obter uma maior agilidade no seu processo de desenvolvimento e por fim corresponder a nova regulamentação de proteção de dados.

Desde o início, estes foram os principais objetivos definidos para a realização desta pesquisa, contudo existem outros pontos que estão subentendidos e que são importantes realçar como a criação de ferramentas de ajuda ao auditor quando este realiza as auditorias de avaliação à organização assim como evitar enormes custos para pequenas empresas, pois ao se fornecer uma solução única automaticamente resulta numa redução de custos.

Este capítulo serve como uma reflexão relativamente ao estudo que foi realizado entre metodologias ao longo da pesquisa que resulta num conjunto de materiais, produzidos com o intuito de servirem como uma solução específica para pequenas empresas de desenvolvimento de software. Como tal é importante descrever o que foi realizado percorrendo todos os pontos da pesquisa, demonstrando a perspetiva do avaliador e o seu grau de satisfação.

Começamos pelo modelo ITmark; como referido anteriormente, é um modelo de certificação que engloba uma série de componentes extremamente úteis para pequenas empresas de desenvolvimento de software. É constituído por três componentes, o CMMI que se preocupa com o processo de desenvolvimento de software e em criar uniformidade nas organizações, a ISO 27001 claramente preocupada com a segurança da informação, onde visualiza que procedimentos que são executados pela empresa e que por sua vez indica boas práticas. O último componente é o *Ten Squared* que avalia a gestão de negócio por parte da empresa. Comprova-se, portanto, como uma escolha de maior capacidade e solidez pois aborda os três pontos principais e que queremos cobrir.

O modelo ITmark é extremamente completo e flexível. À medida que a pesquisa foi realizada percebe-se claramente que apesar de ser um modelo recente e sem a mesma implementação e visibilidade como o CMMI, têm todas as condições para surgir como uma mais valia para o mercado

das pequenas empresas de desenvolvimento de software. A razão é muito simples: o custo de uma auditoria de CMMI é muito superior ao do ITmark e apenas avaliamos a questão do procedimento de desenvolvimento de software. No modelo ITmark estamos a avaliar três vertentes importantes da organização que definem muitas vezes o seu sucesso ou fracasso.

Com base nesta análise ao modelo verificamos que podemos abordar os três pontos a que pretendemos encontrar uma solução com este modelo. A metodologia foi dividida de acordo com estes três pontos e que permitiu tirar várias ilações e evidências de como o ITmark é importante para organizações que se encontram nestas condições e pretendem suprir estes requisitos.

O primeiro ponto focou-se essencialmente na questão da obtenção de certificação e agilidade do processo. A certificação atualmente é tida como uma característica que demonstra e garante a qualidade da empresa e assume-se como ponto de referência no que toca ao alcance de outros tipos de projetos com maior relevância e retorno. É também prestigiante para a empresa que conta com esta certificação o que transmite uma maior confiança no seu serviço aos seus clientes. Este ponto é claramente coberto pelo modelo ITmark pois sendo um modelo de certificação fornece um conjunto de requisitos que garantem a certificação, a que empresa têm de cumprir e implementar e atingir uma percentagem de cumprimento para assim passar na avaliação. Neste ponto o modelo cumpre; contudo, e quanto à segunda necessidade que era garantir agilidade no processo de entrega e desenvolvimento do software, ou seja, abordagem e implementação de movimentos ágeis foi necessário efetuar um refinamento.

O motivo deste refinamento ou adaptação surge por causa das características do modelo ITmark e dos movimentos ágeis não serem totalmente compatíveis inicialmente, pois o componente de avaliação dos processos de software, CMMI, é um modelo genérico que específica "o quê"e não o "como", daí a necessidade desta adaptação. A solução foi a escolha do Scrum, método mais comum e com maior sucesso do movimento ágil, com enorme capacidade de adaptação e que permitiu a realização desta adaptação.

O procedimento iniciou-se com a seleção das cerimónias Scrum e seus artefactos efetuando um mapeamento com as áreas de processo de software do ITmark. A seguir foram identificadas as capacidade de cobertura e as áreas de processo que não estavam claramente abrangidas. Para essas áreas de processo foram sugeridas oportunidades de melhoria das atividades que podem ser usadas no Scrum. O veredito quanto a este ponto é que é possível efetuar esta ligação e tornar a empresa certificada e ao mesmo com um processo rápido e eficaz. Este é um processo que já foi realizado em outros modelos que não tinha este detalhe, mas que serviram como base para a realização deste trabalho.

O terceiro ponto está ligado com o cumprimento da nova regulamentação de proteção de dados. Foi sem dúvida o mais desafiante e exigiu uma maior pesquisa pois apesar desta nova regulamentação ter um ano desde que foi aprovada não encontramos material suficiente para as características que pretendemos cobrir nos objetivos da dissertação.

Os objetivos passavam por capacitar a empresa em cumprir o novo regulamento geral de proteção de dados, mais especificamente nos departamentos de desenvolvimento de software, onde

grande parte das suas tarefas podem eventualmente envolver dados pessoais dos clientes e terceiros e por isso é importante criar e fornecer boas práticas para precaver das multas avultadas que as empresas podem sofrer assim como capacitar os elementos constituintes da empresa com estas valias reduzindo o risco de cometerem alguma infração.

O processo efetuado iniciou-se com um levantamento dos artigos constituinte do RGPD de forma a determinarmos as características e pontos necessário para cumprir a regulamentação. Feito este levantamento foi necessário encontrar uma forma para avaliar e conjugar em apenas uma solução. Como tal o modelo ITmark tem num dos seus componentes uma abordagem que consegue avaliar esta nova componente que é a ISO 27001, norma de avaliação de segurança de informação, fornece ainda medidas e ajuda a implementar um sistema de segurança de informação.

Com base na ISO 27001 foram determinados requisitos e identificados elementos de forma a cumprir os vários artigos do RGPD, o que resultou num mapeamento importante e que comprova que com a ISO 27001 conseguimos cobrir o RGPD. Contudo, e de forma a avaliarmos a empresa e o grau de cumprimento da norma e do RGPD, foi necessário efetuar um refinamento do guião das entrevistas da ISO 27001 onde passaram a ser integradas um conjunto de sub-questões da pergunta número 26 referente ao RGPD, resultantes do mapeamento efetuado entre a regulamentação e a norma sendo assim possível avaliar tanto a empresa quanto a nível de segurança de informação e ao nível do RGPD.

Depois da visualização do resultado, a conclusão que se retira é que é um a solução extremamente viável pois permite avaliar dois pontos críticos que são a segurança de informação e regulamentação de proteção de dados que se cruzam entre si e trazem enormes valias. Fica comprovado que o ITmark com a ajuda do seu componente consegue cobrir a questão do RGPD, consegue também avaliar o sistema de segurança de informação e ajuda na criação e implementação de ambos os componentes.

Conseguimos também determinar outro ponto importante, com a realização destes refinamentos e alterações a modelos existentes foi possível corresponder e criar soluções que de certa forma simplificam as avaliações tanto às empresas como aos auditores. Exemplo nas empresas é a solução encontrada que permite corresponder a todas as suas necessidades e cumprir com máximo de qualidade, sem custos elevados, sem a necessidade de efetuar inúmeras auditorias.

Quanto aos auditores foram criadas ferramentas que podem e ajudam claramente nas auditorias, como são os casos do mapeamento de cerimónias de Scrum com áreas de processo de software, que irá facilitar e reduzir o tempo dedicado a esta tarefa. Porque fica definida uma matriz que serve o auditor como um guia e automaticamente já sabe o que procurar. Um ponto que demonstra a vantagem deste estudo é o tempo que demora a realizar o mapeamento entre as áreas de processo e as cerimónias sem uma matriz já realizada e com a matriz já definida. O primeiro teve a duração de 4 horas sem matriz definida, com a matriz já definida reduziu o tempo para duas horas o que demonstra uma redução em cerca de 50 %. Quanto ao RGPD o auditor poderá efetuar a avaliação em conjunto com a ISO 27001, sem necessitar de efetuar ambas avaliações em separado.

Por fim o ITmark responde de forma positiva quanto aos objetivos pretendidos. Verificamos

que é um modelo flexível e adaptável a vários panoramas. Neste caso específico existem alguns pontos a ter em conta: a empresa que foi alvo deste estudo encontra-se num estado embrionário, não cumpre grande parte dos requisitos necessários em ambas as vertentes e seria preciso mais tempo para implementar este modelo totalmente. No RGPD o nosso foco é claramente o desenvolvimento de software e nos elementos ligados diretamente como departamentos, elementos, etc. Com isto pretende-se demonstrar que as perguntas não são aplicáveis a outros tipos de outro contexto que não esse.

Concluindo, a perspetiva quanto ao ITmark é positiva e recomendável, com este estudo temos matéria suficiente para comprovar exatamente que o modelo ITmark é o ideal para pequenas empresas que pretendam certificação e agilidade no processo de desenvolvimento de software e ao mesmo cumprirem a regulamentação. O ITmark fornece todas as ferramentas para iniciar ou acertar com os requisitos necessários de uma forma menos exaustiva e dispendiosa, mas ao mesmo tempo com um grande prestígio e qualidade que é obter a sua certificação. É também o modelo mais adequado para as empresas que pretendem dar inicio a uniformização do seu processo e que não tem nenhuma cultura e prática destas metodologias, pois é menos exaustivo e complexo quer para a organização assim como os seus elementos criando assim boas fundações para uma melhoria contínua.

5.2 Perspetiva da empresa avaliada

Depois de realizado o caso de estudo e a avaliação à empresa, foram identificadas as oportunidades de melhoria quanto aos processos de desenvolvimento de software, gestão de segurança de informação e RGPD. Estas oportunidades de melhoria foram apresentadas à empresa para obter uma opinião relativamente ao estudo efetuado, às oportunidades de melhoria levantadas e se a empresa futuramente teria o interesses em aplicar o estudo no seu processo organizacional.

Com base na apresentação das oportunidades de melhorias e identificação de lacunas relativamente à melhoria de processos de software, avaliação de segurança de informação e RGPD foi elaborada a seguinte opinião por parte da empresa:

> *"A empresa de momento encontra-se numa fase de reestruturação e redefinição do conceito da sua prestação de serviços. Por isso a normalização dos processos de desenvolvimento de software, gestão de segurança da informação e RGPD tornou-se uma das prioridades da empresa, visto que são processos cruciais para a melhoria da eficiência organizacional. O Duarte Gomes, ao longo do seu estágio curricular no departamento de Gestão de Projeto demonstrou sempre árdua dedicação e interesse na identificação de propostas de melhorias para ir de encontro a este objetivo. O estudo efetuado permitiu-nos identificar determinadas lacunas não só no desenvolvimento de software mas também na gestão de segurança da informação e RGPD. As propostas apresentadas revelam-se pertinentes e algumas delas também vão de encontro com as exigências legais inerentes ao Regulamento Geral de Proteção de Dados. A empresa claramente vê a implementação deste modelo como uma mais valia para o seu*

processo organizacional e prevê futuramente tomar diligências para a implementação destas mesmas oportunidades de melhoria." - Adaílson Júnior, orientador do estágio curricular.

5.3 Perspetiva de especialistas independentes

Este estudo tinha também por objetivo ajudar a reduzir o tempo que os auditores demoram a realizar a avaliação aos processos de software das empresas. Como resultado desse objetivo surgiu um ficheiro de Appraisal Assistant, com o pré-preenchimento das evidências necessárias para o cumprimento do modelo ITmark e cerimónias e artefactos do Scrum.

Com objetivo de verificar a importância do ficheiro de Appraisal Assistant produzido durante a dissertação, foi pedido a Pedro Castro Henriques, CEO da Strongstep, empresa única a nível nacional a implementar o modelo ITmark, para dar uma opinião relativamente a esta ferramenta de ajuda aos auditores.

Foi redigida a seguinte opinião:

"A ferramenta pode servir como um auto-diagnóstico, para as empresas fazerem uma auto-avaliação e saberem qual o seu ponto de partida numa fase inicial. Com esse ponto de partida as empresas, podem fazer um plano, com base no diagnóstico, e assim programar a implementação das melhorias de forma a estarem compliants. As empresas seguem depois uma lista de ações, utilizando uma ferramenta de gestão de projeto (por exemplo sharepoint ou um simples excel), com a lista dessas ações. Distribuem as ações no tempo, atribuem aos responsáveis. A meio do projeto usam a mesma ferramenta para fazer um novo diagnóstico, e verem o resultado. Com as ações identificadas nesse diagnóstico intermédio, podem ver o gap (distância ou ação necessária para cumprir com uma ou um conjunto de práticas). Nesta fase de implementação, seguem os gaps, e fecham as ações. Antes de chamarem o auditor externo para avaliação final usam a ferramenta ainda internamente para verem que estão compliants. A ferramenta ajuda a standardizar e a ser mais eficiente na avaliação, podendo se preparar em menos tempo, e realizar auditoria com mais qualidade, gastando também menos tempo na avaliação. Desta forma fica mais barato para a empresa comprar serviços de auditoria externa.Conclusão, a empresa assim poupa em 2 momentos, no momento da implementação interna da empresa, com a colaboração da equipa de engenharia e da qualidade. e também no momento da avaliação externa/auditoria.No contexto atual, é fundamental às empresas tornar-se mais competitivo, gastar o mínimo de recursos e de forma eficiente, tornando-se mais competitivo. A ferramenta mostra à empresa o seu gap para as boas práticas internacionais, ajudam a ter uma ideia do tempo necessário para implementar e permitir dividir por toda a equipa as tarefas, bem como ir seguindo o nível de compliance, para atingir a certificação/assessment com sucesso, tornando-se assim mais competitivos e evitando reinventar a roda." - Pedro Castro Henriques, CEO da Strongstep.

Capítulo 6

Conclusão e trabalho futuro

Para terminar é importante realizarmos uma retrospetiva do trabalho realizado ao longo da dissertação e elaborar conclusões sobre contribuições, dificuldades encontradas e trabalho futuro que poderá ser realizado. Durante esta dissertação pretendemos encontrar uma solução que correspondesse às necessidades que as pequenas empresas de desenvolvimento de software atualmente necessitam. Foram identificadas três necessidades que são a obtenção de certificação, maior flexibilidade e agilidade no processo de desenvolvimento de software e cumprimento com o novo regulamento de proteção de dados.

Com base nestes requisitos foi escolhido o modelo ITmark, modelo de certificação de processos de software constituído por 3 componentes, CMMI, ISO 27001 e *Ten Squared*, para a avaliação da empresa quanto à melhoria de processos de software, segurança de informação e gestão de negócio. Este modelo forneceu a base para iniciarmos a pesquisa efetuada no capítulo 2 onde procedemos à análise de cada componente, identificando os requisitos de avaliação, características necessárias para efetuar essa avaliação. É demonstrada também uma análise a explicar a finalidade de cada componente que irá ajudar a compreender o porquê da sua escolha e da sua importância para o estudo que foi realizado mais à frente na dissertação.

A partir desta análise e descrição dos componentes foram identificados os desafios que teríamos de responder de forma a cumprir com o objetivo proposto para esta dissertação. Esses desafios deram a origem a contribuições no modelo ITmark nos componentes de melhoria de processos e avaliação de segurança de informação que pode ser observado no capítulo 3 onde é realizado um refinamento em alguns componentes do modelo ITmark.

Por sua vez todo este processo foi testado num caso de estudo corporativo com o objetivo de verificar se metodologia desenvolvida ao longo da dissertação é adequada aos objetivos e desafios identificados assim como às necessidades que as pequenas empresas de desenvolvimento de software têm atualmente. Com base nessa análise efetuada à empresa, surgiram resultados como identificação de sugestões de melhorias e lacunas, onde depois foi realizado uma revisão dos elementos identificados durante a avaliação. Após esta avaliação foi fornecido um parecer com opinião da empresa onde foi realizado o caso de estudo sobre a avaliação realizada. Foi também fornecido uma opinião de um especialista independente, que visualizou o trabalho e determinou

a qualidade e importância que teria o uso das ferramentas desenvolvidas na dissertação para o mundo empresarial.

Este estudo quanto aos objetivos identificados inicialmente foi um sucesso pois com base no modelo ITmark e no seu processo de refinamento conseguimos cobrir todas as necessidades das pequenas empresas de desenvolvimento de software. Contudo a análise ficaria claramente mais completa com a realização da implementação do modelo, pois apesar da análise realizada à empresa, determinou-se que a empresa ainda não estaria preparada para uma avaliação final, necessitaria da implementação das oportunidades de melhoria quer a nível de processo de software assim como segurança de informação o que levaria ao uso de mais tempo para colocar a empresa num estado aceitável, contudo o levantamento destas lacunas deve-se claramente a aplicação do modelo e refinamento do modelo e dessa forma foi formada a base na empresa para assim implementarem um processo robusto.

6.1 Contribuições

Da dissertação resultaram contribuições importantes para a área de gestão e qualidade em melhoria de processos de software. A primeira contribuição foi a realização do mapeamento entre artefactos, cerimónias Scrum e áreas de processo do modelo ITmark. Esta tarefa permitiu cobrir dois pontos propostos da dissertação que são a obtenção de certificação e implementação de um processo de desenvolvimento de software mais ágil; é uma contribuição pois após a realização deste mapeamento resultaram sugestões de práticas e cuidados complementares à metodologia Scrum de forma a obter a total cobertura do modelo ITmark.

Deste mapeamento resultou também um ficheiro de *Appraisal Assistant* pré-preenchido com os artefactos e cerimónias Scrum de acordo com as áreas de processo ITmark, que serve como uma ferramenta de ajuda ao auditor nas avaliações. Quando realiza uma avaliação automaticamente irá ter uma base de evidências que facilitará o seu trabalho em tempo e procura, libertando o auditor para se focar na identificação de oportunidades de melhoria.

Na segurança de informação resultou também uma contribuição, no mapeamento entre RGPD e ISO 27001. Para efetuar esta avaliação o modelo ITmark conta com um guião de entrevistas onde corre todos os pontos necessário de segurança de informação para obter uma avaliação favorável, contudo não contemplava claramente os artigos do RGPD. Foi realizado então um refinamento e adaptação ao guião onde a pergunta ligada a nova regulamentação de proteção de dados foi reformulada, acrescentando perguntas importantes quanto ao RGPD, sempre com foco nos pontos que afetam desenvolvimento de software e todas as atividades ligadas a este processo.

Por fim, foi a utilização do modelo ITmark como uma solução única para cobrir as várias necessidades. Através deste modelo foi possível realizar a avaliação a três componentes importantes das empresas de desenvolvimento software sem efetuar múltiplas auditorias. Explorando os seus componentes e realizando um refinamento ao modelo foi possível determinar que o ITmark é extremamente flexível, capaz de se adaptar as diferentes necessidades e características das pequenas empresas, evitando custos elevados. Durante a pesquisa verifiquei que existiam outros modelos de

certificação e com mapeamento para métodos ágeis, mas que não estavam preparados para uma avaliação e cumprimento de RGPD. O ITmark com as suas características cobre os três pontos e realiza a avaliação a todos, equipa também as empresas com bases para a implementação de um processo ou ajuda a melhorar o processo existente evitando o caos organizacional e uma melhoria na performance da empresa.

6.2 Dificuldades

As principais dificuldades identificadas foram a falta de informação científica relativamente ao modelo ITmark. É um modelo recente e muitos dos estudos realizados não são publicados totalmente, não permitindo entender o seu funcionamento numa fase inicial. Apesar de demonstrar os seus componentes, não era fornecido a forma de como eram calculados e obtido os resultados da avaliação.

Esta dificuldade foi ultrapassada com ajuda de uma entidade independente que forneceu alguma documentação e explicação do funcionamento do modelo, mas sem poder publicar informação que não esteja atualmente disponível a todos.

A outra dificuldade encontrada foi o estado organizacional da empresa onde foi realizado o estudo, com o intuito de realizar o processo de certificação que não foi possível pois seria necessárias inúmeras alterações, assim como mais tempo para a realização desta atividade. Porque atualmente a empresa não conta com um processo de desenvolvimento de software uniforme assim como falta de inúmeras cerimónias e artefactos de Scrum.

6.3 Trabalho futuro

Quanto ao trabalho futuro, temos alguns pontos que seria interessante desenvolver e que poderiam servir como exemplo para empresas que se identifiquem com este panorama e necessidades.

O primeiro é o refinamento do guião de entrevista do ITmark, onde o objetivo seria incluir as perguntas de RGPD, nas questões obrigatórias. Como referido, o modelo ITmark fornece um guião onde são contempladas um conjunto de perguntas obrigatórias. Como a nova regulamentação de proteção de dados é extremamente importante para as empresas, as perguntas identificadas teriam de ser obrigatórias.

O segundo ponto seria completar o processo de auditoria de avaliação à empresa do caso de estudo corporativo, com base no modelo ITmark adaptado nesta dissertação terminando com o processo de certificação à empresa.

Anexo A

Guião de avaliação ITMark - Segurança da Informação ISO 27001

A1 - Existe um inventário básico de ativos (hardware e software)?

A2 - Cada ativo tem o proprietário identificado?

A3 - Há uma política de classificação da informação?

A4 - Existem procedimentos de classificação da informação?

A5 - Existem papéis e responsabilidades definidas para a gestão da segurança?

A6 - Os responsáveis de segurança receberam treino especializado?

A7 - Existe um perímetro físico de segurança definido?

A8 - Existem equipamentos para alimentação ininterrupta?

A9 - Existem mecanismos para a eliminação segura da informação?

A10 - Cada utilizador tem um identificador exclusivo?

A11 - São definidas permissões em função dos papéis e responsabilidades?

A12 - Os servidores locais são protegidos por firewalls?

A13 - Os equipamentos dos utilizadores são atualizados periodicamente?

A14 - Os servidores são atualizados periodicamente?

A15 - Existem mecanismos de proteção contra malwares?

A16 - Existem procedimentos de backup e recuperação de dados?

A17 - Um plano de backups é definido e executado?

A18 - As cópias de segurança são etiquetadas e armazenadas em lugares seguros (fora da organização se for necessário)?

A19 - Os backups são testados periodicamente para verificar sua correta geração e recuperação?

A20 – Os controlos da rede são configurados e implementados?

A21 - Foi identificado na empresa um responsável pela gestão da segurança?

A22 - Os funcionários assinam acordos de confidencialidade?

A23 - São assinados acordos de confidencialidade com clientes e fornecedores?

A24 - A empresa conhece a legislação que se aplica na sua região e nas regiões das empresas parceiras, clientes, fornecedores, etc?

A25 - A empresa verifica os direitos de propriedade intelectual (uso de cópias ilegais, etc.)?

A26 -A organização cumpre com os requisitos do novo regulamento geral de proteção de dados?

A27 - A organização cumpre os requisitos da LSSICE (Lei de Serviços da Sociedade da Informação e Comércio Eletrónico)?

A28 – Controlos de segurança dos sistemas de informação são verificados periodicamente na empresa para garantir o cumprimento das normas vigentes?

Anexo B

Refinamento do modelo ITMark para Scrum

ITmark Process Area	Goal	Specific Practice	Scrum	Satisfied if	Level of Implementation
Project Monitoring and Control	Monitor Project Against Plan	Monitor Project Planning Parameters	Daily Scrum Meeting/ Sprint Retrospective Meeting / Sprint Review Meeting	On release level, velocity, completed points, and total scope are monitored. On sprint level, task effort and remaining effort are monitored. Example:(use of Release Burndown Charts.)	Fully Implemented
		Monitor Commitments	Sprint Review Meeting/ Daily Scrum Meeting	Commitments to the plan are established during sprint planning meeting and monitored. (Example Release Burndown Charts and Daily Sprint Meetings and Sprint Review Meetings).	Fully Implemented
		Monitor Project Risks	Sprint Review Meeting/ Daily Scrum Meeting	In addition to standard agile practices, not only issues (actual impediments) but also risks (potential impediments) are proactively identified and their status updated by the team. (Example: keeping them together with the sprint backlog and reviewed/discussed in daily scrum meetings).	Largely Implemented
		Monitor Data Management			Not Implemented
		Monitor Stakeholder Involvement	Sprint Planning Meeting/Sprint Review Meeting	Stakeholder iterations are defined by Product owner. Normally happens when a major change is made in requirements and stakeholder approvement is needed. (Example: Documentation like minute meetings where stakeholder is documented as member of the meeting and his participation is documented, Release Burndown Charts)	Largely Implemented
		Conduct Progress Reviews	Sprint Review Meeting / Sprint Retrospective Meeting	A review is conducted with stakeholders and team where progress is reviewed to understand. "What has been made?" and "What needs to be done?". They count the sprint backlog to obtain the project progress (Example: Product Backlog and Backlog Refinement, Sprint Burndown Chart).	Fully Implemented
		Conduct Milestone Reviews	Sprint Review Meeting	A Sprint review is conducted with Product Owner, Team and Stakeholders where progress is reviewed to understand what user stories have been accomplished (Sprint Burndown Chart).	Fully Implemented

Figura B.1: Refinamento da área processo Project Monitoring and control do modelo ITMark com Scrum

ITmark Process Area	Goal	Specific Practice	Scrum	Satisfied if	Level of Implementation
Project Monitoring and Control	Manage Corrective Action to Closure	Analyse Issues	Daily Scrum Meeting/ Sprint Review Meeting	Daily scrum meeting is important to gathered and analyze issues. Satisfied by collecting information from dev team, about their impediments and problems during the development of product. (Example: Impediments collection, Issues are registered on a white board, flip chart or impediment list.)	Fully Implemented
		Take Corrective Action	Sprint Review Meeting	In Sprint Review Meeting after the collection of issues, some actions are taken to solve problems. This is made with stakeholder knowledge. The team could decide whether they take the corrective actions immediately or they fix it in an. (Example: Product Backlog Refinement).	Largely Implemented
		Manage Corrective actions	Sprint Review Meeting	All corrective actions are monitored until closing. The results are analyzed to determine their efficiency. (Example: Issues are registered on a white board, flip chart or impediment list.)	Fully Implemented

Figura B.2: Refinamento da área processo monitorização e controlo do projeto do modelo ITMark com Scrum

ITmark Process Area	Goal	Specific Practice	Scrum	Satisfied if	Level of Implementation
Planning Project	Establish Estimates	Estimate the Scope of the Project	Sprint Planning Meeting	Product owner and the other parts estimate the scope of project using the product backlog and the user stories. They Examine it and after their consensus and understanding on the subject they determine the Scope. (User Stories, Product Backlog, Backlog Grooming, Epics, DOD).	Fully Implemented
		Establish Estimates of Work Product and Task Attributes	Sprint Planning Meeting	To estimate the work product and divide tasks, product owner, team members and stakeholders define the division of user stories. They also select user stories and sized them using story sizing techniques and sprint planning. (Example: Poker Planning, Fibonacci Scale, Sprint Planning, Backlog Grooming, Release Planning).	Fully Implemented
		Define Project Lifecycle Phases	Sprint Planning Meeting	Scrum defines process which contains three phases. (Example: pre-game, development, post-game. Release Planning).	Fully Implemented
		Estimate Effort and Costs	Sprint Planning Meeting	In Scrum, estimations occur twice. The first estimation occurs during pre-game phase. The second estimation occurs at the beginning of each sprint. (Example: Story points, velocity and sprint buffer are rational for effort estimation.)	Partially Implemented

Figura B.3: Refinamento da área processo monitorização e controlo do projeto do modelo ITMark com Scrum

ITmark Process Area	Goal	Specific Practice	Scrum	Satisfied if	Level of Implementation
Project Planning	Develop a Project Plan	Establish the Budget and Shedule	Sprint Planning Meeting	Usually this selection takes place in sprint planning meeting with all the company constituents. Example (selecting all user stories and size, project shedule).	Partially Implemented
		Identify Project Risks	Daily Scrum Meeting /Sprint Planning Meeting/Sprint Retrospective Meeting	Risks are captured as impediments. They are registered on white-boards, flip charts, or impediments list. Risk assessment, categorization and prioritization occur in an informal manner. (Example: Release Planning Meeting, Sprint Planning Meeting, Daily Scrum Meeting).	Partially Implemented
		Plan Data Management	Sprint Planning Meeting	Suggestion (Define crucial information that needs to be documented, like (Product Backlog, product requirements, Project effort, Sprint Burndown charts, White-boards), and decide where to save it (place) and necessary resources	Partially Implemented
		Plan the Project's Resources	Sprint Planning Meeting	This is satisfied by selecting external factors like non-human, human and others are identified. Usually this selection takes place in sprint planning meeting with all the parts of project.	Fully Implemented
		Plan Needed Knowledge and Skills	Sprint Planning Meeting	At the start of a Scrum project, the knowledge and skills needed to perform the project are defined. Knowledge and skills which are not found in the organization are considered as impediments and are resolved during the daily and retrospective meetings Definition of training plans to develop the knowledge of the coworkers. (Technical debt)	Fully Implemented
		Plan Stakeholder Involvement	Sprint Planning Meeting	The scrum master is responsible for ensuring that all stakeholders involved in the project follow scrum rules and practices. Scrum defines roles, responsibilities, and involvement of the stakeholders during the project execution. (Example: Backlog Grooming and Team Agreements)	Fully Implemented
		Establish the Project Plan	Sprint Planning Meeting	During the Sprint Planning Meeting the product owner and Dev Team Collaborates to determine initial and on-going priorities for user stories, and provide estimates in the form of story points and/or effort. (Example: Product Backlog, User Stories)	Fully Implemented

Figura B.4: Refinamento da área processo planeamento do projeto do modelo ITMark com Scrum

ITmark Process Area	Goal	Specific Practice	Scrum	Satisfied if	Level of Implementation
Project Planning	Obtain Commitment to the Plan	Review Plans that Afect the Project	Sprint Planning Meeting/Sprint Retrospective Meeting	Normally satisfied when the stakeholders and team review the project plan. When something has changed in requirements, objectives, roles and directly affects the success of the project. The CMMI model does not mention clearly what should be reviewed	Partially Implemented
		Reconcile Work and Resource Levels	Sprint Planning Meeting	Work reconciliation occurs during the sprint planning meeting where the team along with the product owner define the work to be developed in the sprint.	Fully Implemented
		Obtain Plan Commitment	Sprint Planning Meeting	Commitment to the plan is obtained iteratively at the beginning of each sprint. (Example: In the sprint planning meeting, the team selects as much user stories as it believes it can complete by the end of the sprint.)	Fully Implemented

Figura B.5: Refinamento da área processo planeamento do projeto do modelo ITMark com Scrum

ITmark Process Area	Goal	Specific Practice	Scrum	Satisfied if	Level of Implementation
Requirements Management	Manage Requirements Manage Requirements	Understand Requirements	Sprint Planning Meeting	The product owner is present during the Sprint Planning Meeting and assists the team in understanding the user stories so that valid and sufficient tasks can be identified. (Example: User Stories, Backlog Grooming, Product Backlog, Epic)	Fully Implemented
		Obtain Commitment to Requirements	Sprint Planning Meeting	Product owner, agile team and stakeholders reach a consensus in the functionalities to be delivered at each sprint (Example: Backlog Grooming, Epics).	Fully Implemented
		Manage Requirements Changes	Daily Scrum Meeting	The product owner frequently changes the user stories in the product backlog and makes it ready for the next sprint. If a user that was already implemented changed, a new story is created and linked to its old story. The product owner and the team discuss the changes to the user stories in the sprint planning meeting. (Example: Backlog Grooming, Product Backlog, Epics)	Fully Implemented
		Maintain Bidirectional Traceability of Requirements	Sprint Review Meeting	We can identify the current sprint accomplishment, the ideal and finally what is left to finish. (Example: By using Sprint Burndown chart we can obtain a reading about the coverage of requirements, Backlog Grooming).	Fully Implemented
		Ensure Alignment Between Project Work and Requirements	Sprint Review Meeting	Scrum backlogs help to ensure constancy between plans and requirements. The sprint backlog helps to ensure that only the work that has been committed will be implemented. No activities are implemented that do not belong to a user story. The definition of done (DOD) supports constancy between work products and plans. (Example: Backlog Grooming)	Fully Implemented

Figura B.6: Refinamento da área processo gestão de requisitos do modelo ITMark com Scrum

Referências

[1] Georg Disterer. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 04(02):92–100, 2013.

[2] Rossana Ducato. Cloud computing for s-Health and the data protection challenge. *Smart Cities Conference (ISC2), 2016 IEEE International*, 2016.

[3] Amr Emam e Marian Tadros. A case study on the benefit of adopting agile & cmmi in small software organization. *TRI EXL*, 2015.

[4] Very Small Entities. TECHNICAL REPORT ISO / IEC TR Software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Management and engineering guide : Generic profile group : Entry profile. 2012, 2012.

[5] International Organization for Standardization e International Electrotechnical Commission.. Iso annual survey - iso 27001. Available at http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1Accessed last time in December, 2017.

[6] Hillel Glazer, Jeff Dalton, David Anderson, Mike Konrad, e Sandy Shrum. CMMI ® or Agile : Why Not Embrace Both ! *(CMU/SEI-2008-TN-003). Software Engineering Institut*, (November):48, 2008.

[7] ISO/IEC. ISO/IEC TR 29110-1) Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) Part 1:Overview. *ISO.org [Online]*, 4th Edition, 2016.

[8] ITMark. Itmark - certification scheme. Available at http://it-mark.eu/ Accessed last time in December, 2017.

[9] Jeff Dalton, Ross Timmerman, Laura Adkins, Kirk Botula, Neil Potter, Dan Torrens, Prabhakar S., e Margaret Tanner Glover. A Guide to Scrum and CMMI: Improving Agile Performance with CMMI. *CMMI*, página 130, 2016.

[10] KPMG. O impacto do regulamento geral de protecção de dados em portugal. Available at https://assets.kpmg.com/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf Accessed last time in December, 2017.

[11] Claude Y. Laporte, Simon Alexandre, e Alain Renault. The application of International Software engineering Standards in Very Small enterprises. *Software Quality Professional*, 10(3):4–11, 2008.

[12] Xabier Larrucea, Rory V. O'Connor, Ricardo Colomo-Palacios, e Claude Y. Laporte. Software process improvement in very small organizations. *IEEE Software*, 33(2):85–89, 2016.

[13] Anjali Mogre e Sujata Salunkhe. Effective cmmi implementation in agile environment with fresh team. *Atos, Mumbai, India*, 2014.

[14] Jornal Oficial, Comunidades Europeias, e Comunidade Europeia. (Texto relevante para efeitos do EEE). *Control*, 2015(8):48–53, 2015.

[15] L.E. Pelaez. Certificación de la calidad del proceso y producto : ruta para PyMES colombianas. *Revista Ventana Informatica Facultad de Ingenieria Universidad de Manizales*, páginas 41–61, 2011.

[16] Pordata. Empresas- pequenas e médias empresas. Available at https://www.pordata.pt/Subtema/Portugal/Pequenas+e+Médias+Empresas+(PME)-378 Accessed last time in December, 2017.

[17] Mary Luz Sanchez-Gordon, Antonio de Amescua, Rory V. O'Connor, e Xabier Larrucea. A standard-based framework to integrate software work in small settings. *Computer Standards and Interfaces*, 2017.

[18] Fernando Selleri Silva, Felipe Santana Furtado Soares, Angela Lima Peres, Ivanildo Monteiro De Azevedo, Ana Paula L F Vasconcelos, Fernando Kenji Kamei, e Silvio Romero De Lemos Meira. Using CMMI together with agile software development: A systematic review. *Information and Software Technology*, 58:20–43, 2015.

[19] Marcelo Silva e Jacques Brancher. Avaliação de segurança da informação usando o modelo itmark. *Journal on Advances in Theoretical and Applied Informatics*, 2(1):7–11, 2016.

[20] Luz Stella Valencia, Paula Andrea Villa, e Carlos Alberto Ocampo. Modelo de calidad de software. *Scientia et technica*, 15(42):172–176, 2009.