LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

A MATURIDADE E EFICIÊNCIA DOS PROCESSOS DA GOVERNANÇA DE TI BASEADAS NO COBIT 5: UM CASO DE ESTUDO DE UMA ORGANIZAÇÃO DO SETOR DA SAÚDE EM PORTUGAL

POR YOLANDA TATIANA SEBASTIÃO CAROLINO

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
DISSERTAÇÃO

A MATURIDADE E EFICIÊNCIA DOS PROCESSOS DA GOVERNANÇA DE TI BASEADAS NO COBIT 5: UM CASO DE ESTUDO DE UMA ORGANIZAÇÃO DO SETOR DA SAÚDE EM PORTUGAL

POR YOLANDA TATIANA SEBASTIÃO CAROLINO

ORIENTAÇÃO:

PROFESSOR DOUTOR SÉRGIO RODRIGUES NUNES

OUTUBRO-2018

Lista de Acrónimos e Siglas

ANF-Associação Nacional de Farmácias

AP- Administração Pública

ARS- Administração Regional de Saúde

CIO- *Chief Information Officer*

CISO- *Chief Information Security Officer*

CNCS/ GNC - Centro Nacional de Cibersegurança/ Gabinete Nacional de Segurança

CNPD – Comissão Nacional de Proteção de Dados

COBIT- *Control Objectives for Information and Related Technologies*

DPO- *Data Privacy Officer*

DSI- Direção de Sistemas de Informação

EA- *Enterprise Architecture*

eSIS- Ecossistema da Informação na Saúde

ENESIS- Estratégia Nacional para o Ecossistema da Informação em Saúde

GSS- Gestão de Serviço e Suporte

GTI- Governança de TI

ISA- *Information Systems Architecture*

ISACA- *Information Systems Audit and Control Association*

ISO/IEC- *International Organization of Standardization/International Electrotechnical Commission*

ITGI- *Information Technology Governance Institute*

ITIL- *Information Technology Infrastructure Library*

MS- Ministério da Saúde

SANS- *System Administration Networking and Security*

SIS- Sistemas de Informação em Saúde

SPMS- Serviços Partilhados do Ministério da Saúde

SNS- Serviço Nacional de Saúde

RNO- Responsável de Notificação Obrigatória

TI- Tecnologias de Informação;

UE – União Europeia

Agradecimentos

A finalização desta dissertação representa o término de mais uma formação académica e de um sonho esperado por muito tempo e que não chegaria até este nível se não fosse ajuda e colaboração de várias pessoas importantes que passarei a estender os meus sinceros agradecimentos.

Primeiramente ao Soberano Deus Jeová, por me ter concedido a dádiva da vida, por me ter permitido chegado até aqui e pelo dom da inteligência com que sempre me dotou. Agradeço aos meus pais, pela educação e transmissão dos valores morais e éticos desde o berço, obrigada ao meu pai por me apoiar sempre na formação académica e profissional, à minha mãe pelo conforto e apoio incondicional e também ao meu irmão Miguel pelos seus conselhos e sugestões.

Agradeço ao Professor Dr Sérgio Nunes, por aceitar o meu pedido para ser o meu orientador e acompanhar todo este trabalho e por indicar a organização para o estudo de caso. Agradeço aos Doutores Rui Gomes, Pedro Batista, Alfredo Ramalho e também ao Presidente da SPMS, o Dr Henrique Martins por colaborarem nas entrevistas. Ao Doutor Bruno Soares pelos contactos que forneceu.

Por fim a todos que direta ou indiretamente contribuíram para o desenvolvimento deste trabalho dando as vossas opiniões e críticas, agradeço de todo o coração.

Muito obrigada!

Resumo

A Governança de TI é uma área que está a ganhar muita atenção das comunidades académicas e empresariais. O interesse das organizações nesta área é cada vez mais visível uma vez que as organizações estão mais preocupadas em produzir valor para os seus *stakeholders*. Mas para que tal coisa aconteça é necessário o envolvimento de todos os interessados para a organização atingir os seus objetivos estratégicos e proporcionar resultados satisfatórios com o uso das TI. Para ajudar as organizações a terem uma boa governança de TI, existem diversas *frameworks* que são modelos de boas práticas que podem ser aplicadas pelas organizações.

Esta dissertação propôs-se a realizar um caso de estudo de uma organização do setor da saúde em Portugal, que na qual foi feito o estudo da adoção do Cobit 5. O estudo é exploratório e qualitativo e foi usada a estratégia de caso de estudo único tendo como principal método de recolha de dados as entrevistas e análise de documentos. Desta forma, o estudo mostra como a organização tem adotado o Cobit 5 para resolver problemas relacionados com a gestão de riscos e segurança da informação, governação bem como a gestão de serviço permitindo que os recursos tecnológicos da saúde tenham uma gestão segura.

Palavras-Chave: Governança de TI, Tecnologias de Informação, Cobit 5, ITIL, Gestão de Risco, Segurança da Informação, Cibersegurança, Gestão de Serviço e Suporte, Saúde, Arquitetura Empresarial.

Abstract

IT Governance is an area that is gaining a lot of attention from the academic and business communities. The interest of organizations in this area is increasingly visible as organizations are more concerned with producing value for their stakeholders. But for this to happen, it is necessary to involve all stakeholders in order for the organization to achieve its strategic objectives and to provide satisfactory results with the use of IT. To help organizations have good IT governance, there are a number of frameworks that are good practice models that can be applied by organizations.

This dissertation proposed to carry out a case study of a health sector organization in Portugal, in which the study of the adoption of Cobit 5 was carried out. The study is exploratory and qualitative, and the single case study strategy having as main method of data collection interviews and analysis of documents. In this way, the study shows how the organization has adopted the Cobit 5 to solve problems related to risk management and information security, governance as well as service management allowing the technological resources of health have a safe management.

Keywords: IT Governance, Information Technology, Cobit 5, ITIL, Risk Management, Information Security, Cybersecurity, Service and Support Management, Health, Enterprise Architecture.

Índice

Capítulo 1 -Introdução

As organizações não medem esforços em conseguir grandes investimentos para satisfazer os seus *stakeholders* e clientes e desta forma manter firme a sua posição no mercado. Um dos grandes objetivos das organizações é ter um bom serviço que lhes possibilite atingir os seus objetivos estratégicos. E os sistemas de informação ajudam na melhoria dos investimentos da empresa permitindo maior eficiência nas suas atividades (Ribeiro & Gomes, 2009 p.41).

É muito importante o papel das TI no desenvolvimento das organizações. Entretanto é importante saber como está o nível de maturidade das TI nas organizações. De acordo com Ribeiro & Gomes (2009, p.41), uma grande preocupação é perceber que tipos de metodologias ou ferramentas estão a ser adotadas para gerir as TI nas organizações.

Existem vários tipos de *frameworks* (Simonsson et.al, 2007 p.1277; Laersen et.al, 2006 p.2) que ajudam a medir os níveis de maturidade de governança de TI nas organizações para que estas alcancem seus objetivos. A maioria das empresas usa o Cobit 5 por uma ser uma *framework* que retrata aspetos sobre governança e gestão. O Cobit 5 permite gerar valor, mas esse valor só é obtido através da otimização dos riscos e recursos e pela realização de benefícios. O Cobit 5 é aplicável a todo tipo de organização independentemente do seu tamanho e setor (ISACA, 2012 p. 13).

1.1-Objetivos do Estudo

O objetivo principal deste trabalho é com base num estudo de caso exploratório perceber de forma detalhada o processo de adoção da *framework* Cobit 5 numa entidade de saúde portuguesa. A SPMS é a entidade escolhida para este objetivo e o estudo pretende descrever o programa que a mesma tem para a governança e gestão das TI

garantindo a melhoria contínua dos mais variados componentes da informação na saúde.

1.2- Estrutura da Temática

Esta dissertação está organizada do seguinte modo:

1º Capítulo faz a introdução geral do tema e aponta para os principais objetivos a serem abordados no caso de estudo;

2º Capítulo é o referencial teórico onde mostra literatura existente nesta temática;

3º Capítulo apresenta as opções metodológicas e a estratégia de investigação utilizada;

4º Capítulo retrata o estudo de caso da SPMS e mostra o programa da mesma entidade para implementar várias iniciativas com base o Cobit 5. Mostra os benefícios desta iniciativa e também faz uma análise das opiniões dos participantes na componente da discussão e os contributos deste tema;

5º Capítulo são as conclusões finais, limitações e proposta para trabalhos futuros.

Capítulo 2- Revisão de Literatura

2.1- Conceitos de Governança de TI

A governança de TI é um tema muito abordado a nível empresarial. Segundo o que mostra grande parte da literatura sobre esta temática, o seu objetivo principal é permitir que as organizações alinhem as suas estratégias de TI com o negócio (Simonsson & Johnson, 2017 p.1). Esta descrição é apoiada por vários autores. Entretanto uma das definições mais importantes da Governança de TI é a do ITGI que define "a governança de TI como um mecanismo da organização em que os Conselhos de Administração têm a responsabilidade de tomar a liderança máxima e é uma sub-área da governança empresarial. Consiste num conjunto de estruturas organizacionais que garantam o suporte da TI nos objetivos do negócio" (ITGI, 2003 p.10).

Existem outros conceitos sobre governança de TI que são os seguintes:

-A governança de TI é uma estrutura que abrange a gestão executiva e a gestão de TI e permite o controlo e a implantação de processos estratégicos de TI de formas a garantir um alinhamento com os processos de negócio (Van Greembergen, 2002 p.1).

-Governança de TI permite determinar estruturas e processos de tomadas de decisão, fornecendo orientações práticas para o uso eficaz das TI (Weil & Ross, 2004).

Existem muitas *frameworks* que dão suporte aos processos da governança de TI. Conforme será destacado mais adiante, o Cobit 5 é uma ferramenta de boas práticas e foca-se sobretudo em gerir e governar os processos de TI na organização (ITGI, 2007 p.5).

Segundo a definição do ITGI (2003,p.10), o Conselho de Administração tem a responsabilidade de garantir que a governação de TI seja aplicada eficazmente. Entretanto governação e gestão são conceitos diferentes. A gestão de TI foca-se na entrega eficiente de serviços de TI. A governança vai além disso, é mais profunda e se concentra nos resultados que a TI pode fornecer para atender as necessidades do negócio (Peterson, 2004).

Num projeto de governança de TI os resultados vão variando de acordo com as particularidades das organizações, mesmo que forem do mesmo setor (Van Grembergen, Haes & Guldentops, 2004 citados por Van Greembergen & De Haes, 2005).

2.2-A governança de TI nas organizações do setor da saúde

As tecnologias de informação tornaram-se um fator muito importante nas atividades do setor da saúde, porque ajudam a sustentar os seus objetivos estratégicos. É essencial o papel da TI nos cuidados da saúde, a TI e a componente da gestão é bastante importante para o setor da saúde em geral (Suomi, 2001).

Em muitos países, o setor da saúde tem enfrentado vários tipos de pressões que na verdade não diferem muito. Esses desafios incluem: falta de recursos humanos e financeiros, falta de sensibilização das pessoas aos problemas de saúde e doenças novas. Embora hajam soluções, a grande preocupação é saber como geri-las (Suomi, 2000).

O principal desafio destas organizações é agregar valor e ter bons investimentos de TI. Algumas pesquisas mostram que sobretudo os hospitais desconhecem as práticas de governança de TI. Existe pouco pensamento estratégico e por sua vez gera menos desempenho da governação de TI na saúde (Suomi & Tähkäpää, 2004).

Embora existam vários desafios, a governança de TI tem contribuído para a melhoria na prestação dos serviços de saúde. As TI no setor da saúde são mais do que uma área de suporte técnico. As TI têm evoluído de forma significativa no setor da saúde. Atualmente têm contribuído para tratamentos de saúde modernos, telemedicina e tratamentos de saúde virtuais (Suomi & Tähkäpää, 2004).

A *ehealth* é um dos principais elementos que por meio da governança de TI pode-se criar valor para a organização e cobrir as necessidades dos *stakeholders* (Kozina & Sekovanić, 2015 p.205). A *ehealth* é vista como aplicação da TI aos cuidados e sistemas de saúde. Essas aplicações contribuem para a inovação dos sistemas de saúde e melhoram a qualidade de vida (European Comission, 2012 p.3).

A *ehealth* contribui para uma boa qualidade dos tratamentos de saúde moderna. Isto significa um melhor atendimento aos utentes e melhor controlo das informações (Kropf & Scalzi, 2015).

Ao implementar projetos de governança de TI na saúde, é necessário o envolvimento de todos os conselhos da saúde. Isso exigirá mudanças na gestão e na cultura organizacional. Além do compromisso, a *ehealth* também exige que todas as

organizações capitalizem investimentos juntamente com outros interessados (Suomi & Tähkäpää, 2004).

Em países como a Inglaterra e outros da União Europeia, a *ehealth* não tem grandes investimentos, porque normalmente os serviços de saúde nesses países são fornecidos e prestados por terceiros como por exemplo os fundos centrais e públicos (Suomi & Tähkäpää, 2004). Contudo a *ehealth* é um fator que proporciona ambientes rentáveis e retornos de investimentos o que garante que os hospitais e outras entidades adiram a soluções da saúde eletrónica (Suomi & Tähkäpää, 2004).

Em muitas organizações da saúde, a governança de TI permite alinhar as estratégias de TI com os objetivos das mesmas. Mas para garantir a melhoria contínua, estas estratégias precisam estar bem-definidas, planeadas e monitorizadas de formas a responder aos desafios crescentes no setor da saúde (Suomi & Tähkäpää, 2004).

2.3- O Cobit 5

As organizações fazem grandes esforços para garantir a otimização dos custos relacionados com as TI, procuram manter o seu nível de risco aceitável bem como cumprir leis e regulamentos (ISACA, 2012 p.13).

O "**Cobit 5** facilita as empresas a criar o melhor valor da TI, mantendo o equilíbrio e otimizando os níveis de risco e uso de recursos" (ISACA, 2012 p.13, citado por De Haes & Van Greembergem, 2013). O Cobit (*Control Objectives for Information and Related Technologies***)** foi inicialmente desenvolvido pelo ISACA (De Haes & Van Greembergen, 2013). O Instituto de Governança de TI (ITGI) fundado pelo ISACA lançou a terceira edição do Cobit. A quarta edição foi lançada em 2005 e foi revisada como edição 4.1 em 2007. Lançado em 2012, o Cobit 5 é a mais recente versão (Pasquini & Galiè, 2013).

2.3.1- O Modelo de Maturidade do Cobit 5

Segundo o ISACA (2012, p. 42), os seis níveis do Cobit 5 são os seguintes:

-0 Processo Incompleto- Os resultados do processo não são conhecidos, não há nenhum indicativo da realização dos seus objetivos.

-1 Processo Concluído- Este processo alcança os objetivos.

-2 Processo Gerido – Executa-se o processo e seus resultados são geridos, controlados e monitorados.

-3 Processo Estabelecido- Define-se todos os mecanismos usados para alcançar os seus resultados.

-4 Processo Previsível – Este processo funciona dentro dos padrões específicos para atingir os objetivos.

-5 Processo Otimizado- Este processo está ser otimizado e preparado para executar os objetivos planeados.

2.3.2- Os Princípios do Cobit 5

Segundo o ISACA (2012), os princípios do Cobit 5 são os seguintes:

1-Conhecer as necessidades dos interessados: as empresas estão preocupadas em gerar valor para os seus *stakeholders* (ISACA, 2012 p.17). Este princípio mostra que o Cobit 5 fornece todos os mecanismos necessários para que o valor seja agregado através do uso da TI. A essência da governação é definir como as necessidades dos interessados serão preenchidas e estabelecer processos de negócio (ISACA, 2012 p. 17).

2-Cobrindo a empresa num todo: Conforme o ISACA, este princípio mostra que o Cobit 5 trata de todos os processos da empresa. O Cobit é abrangente e permite a integração da governança de TI dentro da governança empresarial. Concentra-se em

todas funções necessárias para gerir informações empresariais e tecnologias relacionadas e trata de todos os aspetos da organização (ISACA, 2012 p.23).

3-Aplicando uma estrutura única e integrada: Por ser abrangente, o Cobit alinha-se com outros padrões e estruturas relevantes. Ele está totalmente integrado com toda estrutura ISACA. Depois de vários anos de investigação, o ISACA desenvolveu padrões como Cobit 4.1, VAL IT, Modelo de Negócio para a Segurança da Informação (BMIS), e o *IT Assurance Framework* (ITAF) entre outros. O Cobit 5 está alinhado a todos estes (ISACA, 2012 p.25; Oliver & Lainhart, 2012).

4-Permitindo uma abordagem holística: este princípio mostra que para uma governação ser eficaz necessita de uma abordagem holística. Esta componente está relacionada com os elementos da empresa (pessoas, estruturas organizacionais e tecnologias). Para isso o Cobit5 fornece facilitadores que ajudam as organizações a alcançar estes objetivos. (ISACA, 2012 p.27; Oliver & Lainhart, 2012). Estes facilitadores são:

-Princípios, políticas e *frameworks*: fornecem instruções para o dia-a-dia das operações da gestão (ISACA, 2012 p.27; Oliver & Lainhart, 2012);

-Processos: definem uma série de práticas a realizar para atingir e produzir os resultados respetivos tendo em mente os objetivos relacionados à TI (ISACA, 2012 p. 27; Oliver & Lainhart, 2012);

-Estruturas Organizacionais: são as estruturas que tem como função a tomada de decisão e dar o sustento necessário aos processos de governação (ISACA, 2012 p. 27; Oliver & Lainhart, 2012);

-Cultura, ética e comportamento: são as ações comportamentais de indivíduos que garantem o sucesso da organização nas atividades de governação e gestão (ISACA, 2012 p. 27; Oliver & Lainhart, 2012);

-Informação: é o recurso mais importante da organização que permite que suas atividades sejam governadas e geridas (ISACA, 2012 p. 27; Oliver & Lainhart, 2012);

-Serviços, aplicações e infraestrutura: são todos os serviços que mantêm o bom funcionamento da organização (ISACA, 2012 p. 27; Oliver & Lainhart, 2012);

-Pessoas, Habilidades e Competências: são todos recursos humanos necessários que executam as atividades com sucesso permitindo melhores tomadas de decisões (ISACA, 2012 p. 27; Oliver & Lainhart, 2012).

As dimensões comuns dos facilitadores são as seguintes:

***-Stakeholders*:** desempenham um papel importante no facilitador e manifestam interesse no facilitador (Oliver & Lainhart, 2012);

-Goals: são os resultados do facilitador que agregam valor na execução desses objetivos. As categorias desses objetivos são:

Qualidade intrínseca: os facilitadores fornecem resultados confiáveis e precisos (Oliver & Lainhart, 2012);

Qualidade Contextual: os resultados do facilitador são apropriados de acordo com o seu contexto (Oliver & Lainhart, 2012);

Acesso e Segurança: os facilitadores são fáceis de aceder quando necessários e seguros (Oliver & Lainhart, 2012).

-Ciclo de Vida: os facilitadores têm um ciclo de vida, desde o início até uma vida operacional/ útil até a eliminação. Isto se aplica às informações, estruturas, processos, políticas e assim por diante. As fases do ciclo de vida consistem em Planear, Desenhar,

Construir/Adquirir/Criar/, Implementar, Usar/Operar, Avaliar/Monitorar, Atualizar/Descartar (Oliver & Lainhart, 2012).

-**Boas Práticas**: Exemplificam como implementar melhor o facilitador e quais produtos de trabalho são requeridos. O Cobit 5 dá exemplos de boas práticas para os facilitadores como por exemplo os **processos.** Para os demais facilitadores, orientações de outros padrões ou *frameworks* podem ser utilizados (Oliver & Lainhart, 2012).

5-Separando a Governação da Gestão: Este princípio mostra que o Cobit 5 separa as atividades de governança e gestão. A governação certifica-se de como as necessidades dos *stakeholders* são atendidas e a gestão trata da execução das atividades sob a direção da governança para alcançar os objetivos da empresa. O Cobit5 divide as funções de governança e gestão de TI em duas vertentes: na governança temos cinco processos baseados no domínio *EDM (Evaluate, Direct and Monitor*) e na gestão temos 4 processos definidos no domínio PBRM *(Plan, Build, Run and Monitor).* Os quatro domínios são: *Align, Plan and Organise (APO)* - orienta como a TI pode ser utilizada na organização para esta alcançar os seus objetivos e gerar benefícios; *Build, Acquire and Implement (BAI)* - descreve como os requisitos de TI podem ser implementados dentro dos processos de negócio da empresa*; Deliver, Service and Support (DSS)* - aborda aspetos da entrega de TI e os processos de suporte que garantem a execução efetiva destes resultados e *Monitor, Evaluate and Assess (MEA)* - verifica se o sistema atual de TI cumpre com os requisitos regulamentares (ISACA, 2012 p. 31; Khanyile & Abdullah, 2012).

2.3.3- Integração Cobit 5 e EA

A arquitetura empresarial refere-se ao uso de modelos necessários para gerir e desenvolver a organização e tem uma noção completa de seus processos de negócio, sistemas de informação e infraestrutura tecnológica (Niemi, 2006).

Assim como o Cobit 5 é uma *framework* para a gestão e governação dos processos de negócio, o EA possibilita uma estrutura para as empresas gerirem dentro da arquitetura ou modelo operacional para atender a visão, missão e metas dos negócios da empresa (Lane, 2014).

Ao referirmos sobre EA no contexto do Cobit 5 existe uma arquitetura considerada como arquitetura-chave que é o *The Open Group Architecture Framework (TOGAF).* Nesta *framework* a governação da EA permite o alinhamento com os objetivos da empresa e dos *stakeholders*, permite definir responsabilidades, melhor controlo dos riscos e a criação de valor. Isto está totalmente relacionado com o Cobit 5 sendo que o mesmo permite a criação de valor através da realização de benefícios e otimização dos riscos (Lane, 2014).

O EA está completamente integrado ao Cobit 5. No domínio APO (alinhar, planear e organizar) há um processo que é o **gerir a arquitetura empresarial** (APO03) que define uma arquitetura empresarial central consistindo em várias camadas como processos de negócio, informações, dados e tecnológicas para realiza-los de forma eficiente. Por outro lado, dentro do domínio EDM (*evaluate, diret and monitor*), a EA é ligada ao processo de otimização de recursos e as atividades associadas (EDM04). O Cobit 5 além de integrar com a estrutura ISACA, integra-se ao *TOGAF for EA* permitindo a governança e gestão da arquitetura empresarial fornecendo uma estrutura global para a empresa (Lane, 2014).

A *information systems architecture* (ISA) é um tópico associado ao conceito de arquitetura empresarial. Descreve o papel do planeamento e recursos dos sistemas de informação e o suporte que estes podem dar nos processos de negócio da organização (Wardle, 1984 p. 205).

A definição de arquitetura de SI é baseada nos conceitos seguintes: arquitetura de negócios, arquitetura tecnológica, arquitetura de informação e aplicacional. A definição destes parâmetros serão discutidos no estudo de caso.

2.3.4- O Cobit 5 para a gestão de serviço e suporte de TI

O Cobit 5 tem um papel na gestão de serviços de TI. O domínio DSS02 permite **gerir solicitações e incidentes** o que implica a priorização de solicitações, incidentes e serviços tendo por base a definição do acordo de nível de serviço e da urgência do negócio (Tucker, 2014).

A TI deve estar habilitada para manter esses serviços em funcionamento por dar suportes aos utilizadores de forma centralizada permitindo que eles sempre reportem os seus problemas que afetam as suas tarefas relacionadas com as TI. Esses serviços de suporte têm várias denominações como *call center, helpdesk ou servicedesk.* O principal objetivo destes serviços é dar suportes aos utilizadores garantindo a eficiência organizacional. O *helpdesk* é geralmente o meio que pela qual os utilizadores têm contacto com a equipa de TI e portanto deve dar sempre uma melhor visão aos utilizadores pela maneira como são resolvidos os seus incidentes e pela qualidade dos resultados. O Cobit 5 fornece boas práticas nesse serviço por definir o desenho e classificação desses incidentes; gravar e priorizar as solicitações e incidentes; investigar, diagnosticar e alocar os incidentes; resolver e recuperar incidentes; fechar as

solicitações de serviço e incidentes e produzir relatórios (University of South Africa, 2017).

Nessa vertente o Cobit 5 alinha-se ao ITIL. O ITIL foca-se principalmente na gestão de serviços e trata da gestão de riscos, gerir relacionamentos com clientes, gerir incidentes e problemas, gerir a continuidade entre outros (White & Greiner, 2017). O Cobit e o ITIL são *frameworks* que fornecem uma visão completa para a governação e gestão de serviços de TI.

2.3.5- O Cobit 5 para a Gestão de Risco e Segurança da Informação

A avaliação e a gestão de riscos fazem parte da segurança de TI em qualquer organização e garantem o sucesso da mesma (Ahmed, 2017).

Existem muitas *frameworks* que cobrem o risco de TI de uma organização, como o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), (ERM-*Enterprise Risk Managment*) para a gestão de riscos empresariais, o RIMS *(Risk Management Society's),* o RMM (*Risk Maturity Model*), a ISO /IEC 27005 (*International Organization for Standardization /International Electrotechnical Commission*), *Information Technology-Security Techniques*- gestão de risco e segurança da informação e a ISO 31000. O Cobit 5 é a única *framework* que é globalmente reconhecida para fins de governação e gestão de risco (Ahmed, 2017 p. 1).

2.3.5.1- Perspetivas de Risco baseadas no Cobit 5

Perspetiva da Função de Risco: Esta perspetiva mostra os passos que as organizações podem seguir para ter uma boa gestão de risco, assim como uma boa gestão e governança. Isto também é ilustrado de como os facilitadores contribuem para tal

(Ahmed, 2017, p. 1). Por exemplo: que **Processos** serão essenciais para suportar a gestão de riscos (Ahmed, 2017);

-Que tipo de **Estruturas Organizacionais** serão necessárias para dar sustento a este programa (Ahmed, 2017; ISACA, 2013a).

Perspetiva de Gestão de Risco: Especifica como os facilitadores do Cobit 5 ajudam no processo da gestão de risco. Estes processos incluem identificar, analisar, corrigir e reportar os riscos. A gestão de riscos é aplicada nas vertentes do Cobit 5 que são: a componente da governança (*Evaluate, Direct and Monitor* (EDM)) e a componente da gestão (*Align, Plan and Organize* (APO)), que são os processos de **Garantir a Otimização de Risco (EDM03)** e **Gerir Riscos (APO12)** (Ahmed 2017, p. 2; ISACA, 2013a).

O processo de governança (EDM03) garante que as organizações conseguem otimizar os seus riscos e alinhá-los ao uso da TI e as falhas de TI são mitigadas e corrigidas (Ahmed, 2017, pág. 2). O processo de gestão (APO12) permite relacionar a TI à gestão de risco e com o ERM e medir os benefícios da gestão de risco empresarial relacionados com as TI (Ahmed, 2017 p.3).

Na segurança da informação, os processos APO13 gerem a segurança, o DSS04 gere a continuidade e o DSS05 gere os serviços de segurança e desta forma permitem definir e monitorizar a gestão da segurança no geral (ISACA, 2014 p.28). Quando as organizações possuem uma excelente estratégia de risco, um bom plano de gestão de risco e meios financeiros para corrigir os riscos, as probabilidades de terem excelentes resultados é sempre maior. O Cobit 5 fornece processos que dão suporte a gestão de risco (Ahmed, 2017, p. 3).

2.3.5.2- Cenários de Risco do Cobit 5

"Um **Cenário de Risco** é definido como sendo uma ocorrência de acontecimentos que ao longo do tempo vão afetando as operações da empresa quer positiva ou negativamente" (ISACA, 2013a). Existem dois tipos de abordagens de risco:

-Abordagem *top- down*: utiliza os objetivos globais do negócio e faz uma análise dos riscos relevantes que impactam os objetivos do negócio (ISACA *Journal*, 2011 p.1; ISACA, 2013a).

-Abordagem *Bottom-up*: utiliza um conjunto de cenários específicos que são personalizáveis e compatíveis à própria empresa (ISACA *Journal* 2011, p.1; ISACA, 2013a).

2.3.5.3-Estrutura do Cobit 5 para o Risco

O Cobit 5 define orientações para a governança e gestão de risco, com objetivo de suprir as estratégias da empresa. Isto permite perceber a aplicação dos facilitadores do Cobit 5 para o risco, permite uma governança e gestão de riscos eficientes, usa os cenários e procedimentos para ajudar a gestão a dar respostas significativas e interliga os cenários de risco com os facilitadores na mitigação dos mesmos. (Ahmed, 2017 p.3).

O *Cobit 5 for Risk* fornece procedimentos que incluem diversas categorias de riscos para as organizações utilizarem para mitigar os seus riscos. Dentre vários tipos de riscos, os cenários do Cobit 5 incluem riscos como roubos, sabotagens, espionagem industrial e outros. (Ahmed, 2017 p. 3).

2.3.5.4- Alinhamento do Cobit 5 for Risk com outras estruturas

Segundo o ISACA (2014), o Cobit 5 na vertente do risco alinha-se com outros padrões e estruturas:

-ISO 31000: 2009 (Focada na gestão de riscos): o *Cobit 5 for risk* abrange todos os aspetos especificados pela ISO 31000. E o Cobit 5 vai muito mais além, porque todos aspectos não definidos pela ISO 31000, tais como a governança dos riscos são cobertos pelo Cobit para o risco (ISACA, 2014 p.27; Ahmed, 2017 p. 4).

-ISO 27005: 2011 (Focada na gestão de risco e segurança da informação): o Cobit 5 trata dos princípios da ISO 27005. O que difere o Cobit 5 da ISO 27005 é pelo facto do Cobit5 para o risco atender áreas não definidas pela ISO 27005 como por exemplo a governança de riscos e também por abordar vários tipos de categorias de risco. Por outro lado, a ISO 27005 tem por objetivos tratar da gestão de riscos e segurança da informação (ISACA, 2014 p. 27; Ahmed, 2017 p. 4).

Na segurança da informação, o Cobit5 alinha-se com seguintes padrões: Modelo de Negócios para Segurança da Informação (BMIS) – ISACA; Padrão de Boas Práticas para Segurança da Informação (ISF); ISO / IEC 27000 Séries; NIST SP 800-53a; Indústria de Cartões de Pagamento (PCI), Padrão de Segurança de Dados (DSS) (ISACA, 2014 p. 31).

2.3.5.5- Aplicações e Benefícios do Cobit 5 para o Risco e Segurança da Informação

Num programa de gestão de risco e segurança, os conselhos de administração devem dar sempre o suporte e apoiar estas iniciativas, as estruturas organizacionais devem ser indicadas para dar o sustento necessário. A gestão de risco deve fazer parte das atividades da organização e deve haver sensibilizações e consciencializações no sentido de disseminar uma cultura consciente (Ahmed, 2017).

Quando aplicados estes passos as organizações obtêm benefícios como: mais conhecimento sobre a gestão de risco e melhor perceção por parte das organizações; são fornecidos um conjunto de orientações sobre como gerir e mitigar os riscos e como

obter melhores investimentos com as práticas de gestão de risco; a organização consegue agregar valor o que proporciona uma redução de custos (ISACA, 2013b p.10). Na segurança destacam-se os seguintes benefícios: a segurança da informação integra-se por completo nas atividades da empresa; os resultados positivos derivados da segurança da informação aumentam a satisfação do cliente; a empresa cria linhas de defesa, deteção, recuperação e reduz os custos (ISACA, 2014 p. 29).

2.3.5.6- Aplicação do Cobit5 à Governança de Cibersegurança

Na governança cibernética, **os *stakeholders* tem necessidades distintas**. Portanto as empresas devem saber o quais são as suas reais necessidades e dos seus *stakeholders* e integrarem essas necessidades a nível do seu alinhamento estratégico mas como parte essencial na sua governança (ISACA, 2013c p.57).

A cobertura da empresa no geral é muito difícil alcançar devido a complexidade da TI. Este princípio não trata de todos os tipos de ataques. Com base numa abordagem sistémica pode-se criar uma gestão focada nas estruturas de ataques e violações (ISACA, 2013c p.58).

Para **criar estrutura única** para governar a segurança cibernética, é necessário alinhá-la com outras estruturas de governança empresarial como por exemplo: a ISO 27032, Tecnologia da Informação e Segurança Técnica - fornece diretrizes para segurança cibernética; ISO 27001 ou Instituto Nacional de Padrões e Tecnologia (NIST) SP 800-53; Controlos críticos pelo SANS (Top 20); Continuidade das operações, continuidade de serviço e gestão de emergências / medidas associadas a segurança, por exemplo, ISO 22301, ISO 27031 (ISACA, 2013c p.58).

A separação entre a governança e a gestão é um aspeto muito importante da cibersegurança. O fato de serem operações diferentes, a gestão das atividades de

cibersegurança deve ser uma atividade separada da governança de segurança cibernética (ISACA, 2013c p.58).

2.3.5.7-Gestão de Cibersegurança

Os facilitadores do Cobit 5 influem a maneira como a segurança cibernética é gerida e abordam o seu alinhamento com outras práticas de governança cibernética (ISACA, 2013c p.71).

1.Políticas, Princípios e *Frameworks*: este facilitador ajuda a tomar decisões para melhorar a relação com os interessados descrevendo requisitos para proteger-se dos ataques. É muito difícil elaborar um conjunto de políticas porque os ataques não são previsíveis. É importante a empresa considerar a adoção de controlos nas políticas para a segurança cibernética dos seus recursos (ISACA, 2013c p.78).

2.Processos: Segue a lógica do modelo do Cobit 5. Por exemplo o processo APO01 (gerir a *framework* de gestão de TI) - serve para monitorar a conformidade da segurança cibernética, o DSS02 (gerir solicitações e incidentes) - permite integrar as respostas de incidentes com a gestão de incidentes num todo/gestão de crises. Na gestão da cibersegurança, os conselhos de administração e outros processos organizacionais devem ter um funcionamento excelente para que possam conduzir a segurança cibernética no nível desejável (ISACA, 2013c p.90,92).

3.Estruturas Organizacionais: Neste facilitador são designados normalmente os responsáveis da área da segurança que cuidam do programa da segurança. Nesse caso, os gestores assumem responsabilidades mediante o seu perfil (ISACA, 2013c p.93).

4.Cultura, Ética e Comportamento: Os ataques cibernéticos constituem desafios que comprometem a cultura da organização. Cada vez que uma empresa é afetada por ataques, provoca uma sensação de insegurança, o que acaba por influenciar nas relações

que a empresa tem mantido com os clientes. A adoção de controlos poderá contribuir para uma boa cultura organizacional (ISACA, 2013c p. 96).

5.Informação: O principal recurso que deve ser protegido dos ataques cibernéticos é a informação. Este facilitador é aplicável a todos os interessados como gestores e utilizadores da informação. A informação deve estar protegida garantindo uma boa segurança em toda a organização (ISACA, 2013c p. 103).

6.Serviços, Aplicações e Infraestruturas: Este facilitador especifica e identifica os requisitos de serviço e metas para a gestão da segurança da informação como por exemplo: arquitetura de segurança, conscientização de segurança, avaliações de segurança, sistemas adequadamente protegidos e configurados, proteção adequada contra *malware*, ataques externos e tentativas de invasão (ISACA, 2013c p.110).

7.Pessoas e Competências: É importante que a equipa da segurança cibernética possua as habilidades desejadas. A formação é essencial para a segurança e deve estar disponível em todos os departamentos. As pessoas são treinadas para adquirir competências em todos os contextos (ISACA, 2013c p.114, 117).

Controlos de Segurança Cibernética: são definidos como um conjunto de soluções que a empresa decide adotar, mas tudo depende do cenário e categoria de risco. Esses controlos são parte da governança e gestão cibernética e devem estar em conformidade com os requisitos do Cobit 5 (ISACA, 2013c p.72).

Auditoria de Cibersegurança: O processo de auditoria é importante para perceber o nível de maturidade da organização em termos de segurança. Estas revisões requerem investigações mais profundas e seus objetivos devem estar bem definidos (ISACA, 2013c p. 121).

Capítulo 3 - Metodologia e Questão de Investigação

Neste tema será utilizada a **metodologia qualitativa e um estudo de caso como estratégia de investigação.**

A abordagem ideal para este trabalho é a qualitativa porque o objetivo principal do estudo é explorar detalhadamente a adoção do Cobit 5 numa organização da saúde. A pesquisa qualitativa tem como objetivos entender como estão relacionados determinados pontos e os princípios que governam tais aspetos, permitindo investigar e perceber a opiniões das pessoas (Kaplan & Maxwell, 2005 p.30).

A investigação qualitativa é destinada a fazer estudos aprofundados sobre determinado tópico de interesse, e normalmente o método de recolha de dados é feito através de entrevistas em que o objetivo é saber as opiniões e pontos de vista dos participantes do estudo, e que na qual eles partilham seus relatos e expetativas. Além das entrevistas, a investigação qualitativa permite que o investigador obtenha informações por meio de análises de documentos, observações e perceber como determinado assunto afeta as atividades dos participantes (Maxwell,1996).

Uma vez que adoção do Cobit 5 na SPMS envolve um setor grande e vão sendo aplicadas um conjunto de iniciativas, este estudo pretende responder a seguinte pergunta: Como as organizações podem mitigar as falhas e riscos de TI utilizando de forma eficaz as diretrizes do Cobit 5 para a Gestão de Risco e Segurança da Informação?

3.1- Recolha de Informação

3.1.1- Estudo de Caso

Optou-se pelo estudo de caso como estratégia de investigação que segundo Yin (1983, p.3) tem a finalidade de "compreender diversos aspetos da vida real em um contexto específico". O estudo de caso também ajuda a ter uma compreensão completa de "fenómenos sociais e complexos" (Yin, 1983 p.3). Foi utilizada a estratégia de **estudo de caso exploratório** por ser o mais adequado para o tema uma vez que o mesmo pretende explorar de forma mais estruturada o projeto de adoção do Cobit 5.

3.1.1.1- Elaborando o estudo de caso

Inicialmente foi feita uma investigação sobre a organização. Pesquisou-se os possíveis participantes e levou-se em conta pormenores como o perfil profissional e o grau de conhecimento sobre a matéria.

As **entrevistas** foram semiestruturadas com perguntas abertas e foi elaborado um guião único de entrevista (Anexo 1) tendo por base a revisão da literatura e os documentos analisados. As entrevistas duraram no geral cerca de 45 minutos a 1 hora. A primeira entrevista foi feita junto do antigo Diretor de SI da SPMS via *Skype*. Optou-se por esta entrevista porque ele liderou o projeto na altura e por ser perito nesta matéria. A segunda entrevista foi feita junto do Presidente do Conselho de Administração da SPMS e optou-se por isso porque os Conselhos de Administração são normalmente os que assumem a liderança e tomam as decisões nestes projetos. A terceira entrevista foi feita ao novo Diretor de SI que atualmente coordena o núcleo da Cibersegurança e foi complementada com uma quarta entrevista que contou com a participação do Diretor responsável pelo núcleo do eSIS, isto porque o programa de formação, gestão e reforço

de competências atualmente está dividido e coordenado por estes Diretores. As 3 últimas entrevistas foram realizadas presencialmente na SPMS com a particularidade de que a última entrevista contou com a presença de dois Diretores estando um deles em videoconferência. Aos entrevistados foram atribuídos os seguintes códigos: **Diretor1** (Diretor de SI), **PCA** (Presidente do Conselho da Administração), **Diretor3** (Diretor de SI-Núcleo da Cibersegurança) e **Diretor4** (Diretor de SI-Núcleo do eSIS).

Foram pesquisados **documentos** pertencentes à organização que retratam especificamente o projeto de adoção do Cobit 5. Documentos como: O Caderno de Encargos da SPMS, Plano Sectorial das TIC- Ecossistema Português de *Health*-Sistemas de Informação em Saúde e *Cybersecurity Match Supply And Demand in Portuguese HealthCare Sector – Industry Collaboration* – são documentos que mostram a adoção do Cobit para as estratégias de cibersegurança em Portugal. O documento Estratégias das TIC 2020 para a transformação da informação digital na Administração Pública - mostra que um dos eixos estratégicos para o setor da saúde é a adoção de um modelo de Governação de TI para o Ministério da Saúde. Estes e outros documentos foram úteis para a realização deste tema.

Realizou-se a **Triangulação** que segundo Denzin (1978 p. 28, citado por Jick (1979), p.602), é definida como "a combinação de vários métodos de estudo para entender o mesmo fenómeno". A triangulação, segundo Smith (1975, p. 23) é uma estratégia que usa múltiplas referências para perceber a posição concreta de um objeto. Neste caso, o processo de triangulação foi utilizado para relacionar o estudo de caso com a literatura e com as entrevistas a fim de identificar aspetos que se assemelham e diferem uns dos outros para se ter a ideia concreta do estudo e sugerir algumas melhorias que poderão ser os contributos deste tema.

Capítulo 4- Adoção do Cobit 5:Um Estudo de Caso

4.1- Caracterização da Organização

A SPMS (Serviços Partilhados do Ministério da Saúde) criada em 2010 é uma entidade pública portuguesa do setor da saúde. A sua principal missão é prestar serviços a todas as entidades do setor da saúde em Portugal, tais como o Serviço Nacional da Saúde, o Ministério da Saúde e outras entidades do setor da saúde (SPMS, 2016a p. 1). Segundo o Diretor 3 as delegações da SPMS estão situadas em Lisboa e no Porto e a organização passou por uma nova reestruturação. Atingiu uma dimensão maior e conta com mais de 400 colaboradores. A DSI atualmente está dividida por 3 núcleos liderados por 3 Diretores, sendo o Diretor 3 um deles. Estes núcleos estão subdivididos em 15 unidades de coordenação, 5 para cada núcleo e cada Diretor coordena um núcleo específico. Por outro lado existem funções de suporte que são transversais a toda DSI.

Além de supervisionar as TI da saúde pública portuguesa, a SPMS já conta com participações a nível Europeu. Segundo o Diretor3, as iniciativas da SPMS são de facultar serviços "*cross-border*" e a troca de sumário clínico nos países da UE. Por exemplo se um estrangeiro estiver em Portugal, os sistemas informáticos portugueses fornecem as informações do país de origem deste utente. Ou se o utente português for atendido em França, os sistemas informáticos franceses devem estar capacitados para fornecer a informação do resumo clínico do utente Português em França e assim a SPMS consegue produzir, fabricar e suportar os SI para estes *stakeholders*.

4.2- A Governação das TI no setor da saúde em Portugal: Situação Atual e Futura

A SPMS é a supervisora do Modelo de Governação do setor da saúde. Desde 2011, supervisiona as operações relacionadas com a manutenção das TI do Ministério da

Saúde e garante o funcionamento dos Sistemas de Informação na Saúde em alinhamento com os SI da Administração Pública. A SPMS é o CIO do MS e tem como função fornecer todas as informações de TI aos utentes/cidadãos, profissionais de saúde e gestores (SPMS, 2017a p. 9).

A nível do planeamento do SIS, a SPMS alinha os processos de TI com as estratégias de saúde local, nacional e internacional. A nível estratégico de TI, a SPMS alinha-se com a estratégia a nível da Europa, interministerial das entidades do SNS e outros intervenientes (SPMS, 2017a p.9).

O programa da SPMS para a melhoria contínua visando as boas práticas de governação e gestão de TI está em desenvolvimento. Tem como objetivo a definição de estruturas organizacionais para possibilitar a participação dos *stakeholders* do eSIS, estando em alinhamento com o Cobit 5. Pretende-se a colaboração dos todos os membros a nível estratégico que são os órgãos máximos das Instituições do MS (a Tutela, o Presidente do Conselho de Administração da SPMS, o Diretor Geral da Saúde e o Presidente do Conselho Diretivo) integrados na **Comissão de Acompanhamento do eSIS**, e a nível tático que refere-se aos Diretores de SI vinculados à **Comissão de Acompanhamento TIC**. A SPMS continuará como responsável pela Governação de TI no MS (SPMS, 2017a p. 10; ENESIS, 2017).

4.2.1-Descrição e Diretrizes do Modelo de Governação

O Modelo de Governação estabelecido pela SPMS e pelo CNCS está previsto no Despacho nº8877/2017 do mês de Outubro (Artigo 3). Faz um resumo de todos os procedimentos e objetivos que devem ser cumpridos na componente da segurança e na gestão de risco. A SPMS é responsável por manter a segurança de todos os recursos tecnológicos, realização de operação, manutenção e recuperação das infraestruturas. As

ações de formação são muito importantes para contribuir para uma cultura consciente e definir as diretrizes para o combate de ataques (Artigo 3, Despacho nº 8877/2017).

Todas as organizações devem reportar o seu desempenho à SPMS e esta reporta ao CNCS. Este modelo de governação pretende alinhar as estratégias das TI do MS com as estratégias da saúde e com as estratégias de TI da AP (Artigo 3 Despacho nº8877/2017; SPMS, 2016b p. 19). É importante a colaboração de todos *stakeholders* no sentido de haver partilhas de responsabilidades, os utentes também são beneficiados com acesso à informação. A SPMS está estabelecendo parcerias com instituições internacionais de pesquisa sobre matérias de segurança permitindo um alinhamento entre as práticas do Cobit 5 e as práticas de segurança da informação (Artigo 4, Despacho nº8877/2017).

4.2.2-Responsabilidades das Entidades

As entidades abrangidas neste programa devem cumprir com todos os requisitos estabelecidos no Modelo de Governação; devem participar ativamente no ato de partilhas de boas práticas; devem designar um CISO *(Chief Information Security Officer)* e um CSO *(Chief Security Officer).* Caso surjam situações que comprometam à segurança dos seus dados devem reportar aos seus superiores e devem cooperar com a SPMS na implementação dos padrões de cibersegurança (Artigo 5, Despacho nº8877/2017).

4.3- Análise dos Resultados

4.3.1-Enquadramento, Objetivos e iniciativas

O Diretor4 relatou que além do Cobit 5 o trabalho está ser feito também com base no ITIL sobretudo em áreas como a GSS. O Cobit vai sendo implementado de acordo as necessidades, nível de conhecimento e maturidade interna e externa. A responsabilidade

da DSI é de trabalhar nas diferentes unidades de coordenação otimizando e melhorando a prestação de serviços com bases estas boas práticas. Além disso este programa abrange a todas as entidades da saúde e tem sido feito um trabalho na área de governação.

Os Diretores (com os códigos Diretor3 e Diretor4) caracterizam o nível de conhecimento da equipa de TI nesta área como baixo, sendo que o programa ainda não está avançado e está numa fase inicial. A equipa de cibersegurança na SPMS é pequena, são poucas pessoas na equipa certificadas na área e um dos Diretores tem certificação formal em Cobit 5 para a segurança e uma certificada em arquitetura empresarial.

Segundo o Diretor3, o objetivo ao adotar o Cobit tem a ver com a necessidade de governação uma vez que a entidade atingiu uma grande dimensão. Este crescimento interno, a constante reorganização das unidades de coordenação, das funções e dos processos levou a SPMS a procurar uma *framework* para a governação e gestão interna da entidade. E também o Cobit permite a SPMS dar instruções a nível externo para as demais entidades do eSIS.

Segundo o Diretor4, o Cobit e o ITIL permitem governar de forma eficiente a complexidade dos Sistemas de Informação da Saúde a nível interno e externo. Com base nas boas práticas dessas *frameworks* é possível dar eficiência em áreas como a gestão de serviço e suporte, gerir problemas, gerir relacionamentos com as entidades definir a gestão e liderança com papéis diferentes, a gestão da segurança e arquitetura empresarial.

Segundo o PCA, o modelo de governação foi um dos objetivos alcançados e dá instruções de quem governa a área da segurança, quais são as responsabilidades da

SPMS e das entidades. As circulares normativas emitidas pela SPMS também transmitem alguma histológica do ponto de vista da governação.

Para o Diretor1 é a importância de gerar a criação de valor por meio da otimização dos recursos, mitigação dos riscos e realização de benefícios. Os fatores que estiveram na base desta adoção segundo o Diretor1 foram a necessidade da gestão de risco, garantir a segurança e a privacidade dos dados.

Além disso, um outro objetivo é a adoção e partilha de práticas internacionais (ENESIS, 2017). A Resolução do Conselho de Ministros aprovou a Estratégia Nacional para o Ecossistema da Informação em Saúde 2020 que garante a entrega de benefícios e a criação de valor através dos vários elementos do SIS (ENESIS, 2017). Encontra-se disponível no Despacho n.º 3156/2017.

As iniciativas que estão em curso são:

-Reforço e capacitação dos recursos humanos (Gestão das competências) - tem como objetivo formar e capacitar as pessoas de acordo com seus perfis por exemplo administrativos, gestores, clínicos e não clínicos e os tecnológicos (ENESIS, 2017);

-Melhoria dos SI na área da segurança- este programa baseia-se nas boas práticas do Cobit 5, ITIL e ISO 27001 com objetivo de melhorar questão da segurança da informação da saúde (ENESIS, 2017);

-Melhor prestação a nível da entrega de serviços- em Junho de 2017, a SPMS desenvolveu o Modelo de Gestão de Serviço e Suporte (figura 1, Anexo 2) baseado no Cobit 5 (aplicado para as tarefas de *governance* e também para a gestão e organização dos processos de TI) e ITIL (em que seguiu-se as práticas para uma melhor gestão de serviços) com objetivo de proporcionar melhores serviços aos *stakeholders* (ENESIS, 2017). No dia 1 de agosto do mesmo ano, entrou em curso o *Portal Easy Vista*, a nível

do eSIS para facilitar o reporte de problemas e incidentes (Circular Normativa nº6/2017). Os técnicos de TI estão a ser formados principalmente em ITIL no sentido de poderem trabalhar com este modelo (SPMS, 2017b).

-**Definir uma arquitetura central para o eSIS**: o Diretor4 disse que este trabalho está ser feito a nível do eSIS e da SPMS. Estão a ser definidas um conjunto de regras e políticas de forma transversal para as entidades e está a se fazer um levantamento de todos os ativos e das arquiteturas para se trabalhar de forma integrada e ver os impactos que podem ser gerados. A nível do sistema hospitalar a arquitetura é global que também está a ser implementada.

Nesse âmbito está ser desenvolvida uma **arquitetura de SI para o eSIS** com base nas seguintes dimensões: **arquitetura de negócio**: que identifica os componentes dos SI que suportam o negócio; **arquitetura aplicacional:** implementa as aplicações necessárias que dão suporte ao negócio; **arquitetura da informação:** refere-se a gestão dos ativos físicos e lógicos da organização e **arquitetura tecnológica**: que suporta os dados, aplicações e processos de negócio e implementa serviços que são as infraestruturas da organização. A nível do eSIS esta arquitetura supre os objetivos atuais e futuros das TI (ENESIS, 2017).

Segundo o Diretor4 uma outra dimensão dessa arquitetura é mais aplicacional e tecnológica com base na arquitetura empresarial que está ser desenvolvida internamente e estão a ser criadas condições para o desenvolvimento dos sistemas e implementa-la de forma lógica.

4.3.2-A SPMS antes do Cobit 5

Segundo o PCA era mais confuso o papel da SPMS em relação à tutela e aos fornecedores. O Cobit ajuda a perceber o papel de cada pessoa e o que esperar de cada

nível de responsabilidade. Por exemplo ao referir-se nos Despachos da tutela, ficou claro de que devia haver um sinal claro da parte do governo a dizer que o assunto é importante e que a SPMS é a entidade responsável pelo programa e que todas as entidades deviam obedecer as suas instruções. E desta forma o Cobit ajudou a explicar ao mais alto nível de hierarquia as questões tecnológicas. Foram feitas várias investigações e leituras sobre o tema e ficou claro que sem o envolvimento do topo há coisas que não vão funcionar.

O PCA partilhou a opinião dos Diretores (Diretor3 e Diretor4) de que o projeto está numa fase inicial. "*Para mim são ideias e elas vão impregnando a maneira de pensar das pessoas. O mais importante numa framework desta, conforme aprendi não é seguir aquilo à risca é ter a noção de que há níveis de responsabilidades, de desempenho e interesse e esses níveis não se devem confundir mas estão interligados"*.

O PCA esclareceu o papel dos Conselhos da Administração nestes programas. As iniciativas devem sempre partir de alguém do Conselho de administração porque há coisas que não estão no topo das preocupações das pessoas, e a segurança é um destes aspetos. "*O grande problema é que no caso português temos uma grande maturidade tecnológica, mas temos poucas pessoas, as pessoas têm muitas prioridades e a segurança não é prioridade. Estão mais preocupadas com o entregar o serviço e portanto tem de ter alguém que se preocupe com estes pontos"*.

4.3.3- Reestruturação do Organograma

O organograma da SPMS (figura 2, Anexo 2) sofreu uma nova reestruturação. Segundo o Diretor3, a segurança foi sempre uma preocupação. Mas não havia uma área dedicada para a segurança, uma vez que havia um núcleo que fazia a articulação do pensamento e iniciativas estratégicas de todo eSIS e abrangia a articulação com os *stakeholders* que é

o **Núcleo do eSIS** e existe até agora e as responsabilidades de segurança estavam dentro deste núcleo. A componente operacional estava mais focada nas operações, ou seja as equipas estavam mais focadas a fazer e a suportar a manutenção operacional dos sistemas.

Com a nova reestruturação que houve em 2017, foi criado o **Núcleo da Cibersegurança** que faz a governação e gestão da segurança e permite enviar diretrizes para fora.

Segundo o Diretor3 o que falta ainda é ter a nível do núcleo e das equipas operacionais um *Security Operations Center* (SOC) e uma equipa de respostas aos incidentes. O catálogo de serviços do núcleo de cibersegurança é muito a base de articulação/governação. Esta componente é suportada com base numa *framework* interna em que existe um repositório documental e rico autonomizado a nível de pensamento estratégico e com base nisso a SPMS tem sido capaz de informar as entidades e outros *stakeholders* que devem políticas de segurança e privacidade de dados e nomear responsáveis de notificação obrigatória. Este repositório deu a evidência de que este pensamento deve existir em todas as entidades e não só na SPMS. O núcleo permite uma governação concreta e garante que as políticas sejam implementadas.

Um outro aspeto que falta conforme o Diretor3 *"é ter um braço operacional no núcleo da cibersegurança, este núcleo promove, articula e põe várias equipas em contacto e faz muito trabalho de awareness. Quanto ao reporte de incidentes fazemos a ponte do que acontece aqui na SPMS e nas entidades com o CNCS aquém reportamos."*

4.3.4-Principais Desafios

Um dos desafios segundo o Diretor1 é a necessidade de todos os *stakeholders* passarem a trabalhar nesta *framework* e reverem-se nela.

Segundo um relatório feito pela IDC *Health Insigths*, as organizações do setor da saúde foram vítimas de vários ataques cibernéticos, ocorridos nos anos de 2013 e 2014 (Konschak et. al, 2015, p. 1, citado por Gomes & Soares, 2016 p.2). Um destes é o famoso ataque *Wannacry*, que assolou vários hospitais da Inglaterra por exemplo. Este ataque ocorreu em 12 de Maio de 2017 e é uma espécie de *ransomware* que bloqueia o acesso do utilizador aos dados e pede resgate para restaurar o acesso (Circular Normativa nº3/2017). O PCA disse que "*houve vários ataques noutros países, tivemos um incidente que não foi nada extraordinário, estamos mais ou menos seguros. Não tivemos os mesmos os problemas que tiveram os ingleses. Estou a falar do ataque WannaCry que ocorreu em Maio de 2017, os hospitais ingleses ficaram parados durante vários dias".*

Houve também a necessidade das entidades terem suas informações seguras. Nesse caso, o **Ministério da Saúde** tinha como objetivo agregar valor à proteção de seus recursos. Resumindo para garantir a **criação de valor,** considerou-se dois importantes fatores que são: **a otimização dos riscos e a gestão da segurança** (Gomes & Soares, 2016 p.5). A SPMS levou conta duas situações:

-***AS-IS***: Para garantir uma boa governança e gestão, as organizações precisam ter uma excelente estrutura que possibilite a partilha de boas práticas. Este programa está ser desenvolvido tendo em mente três componentes a saber **pessoas, processos e tecnologias** (Gomes & Soares, 2016 p.5).

-***TO-BE***: É necessário um programa de gestão de riscos que possibilite a partilha de boas práticas de governança e gestão em todo o setor da saúde (Gomes & Soares, 2016 p.5).

Outros desafios verificados são a necessidade de uma governança abrangente e uma arquitetura a nível do eSIS que fosse comunicável (ENESIS, 2017).

4.4- Caracterização do Projeto de Adoção do Cobit 5

O projeto do Cobit 5 está ser usado para questões de governação e gestão dos SI na saúde e alinha-las aos objetivos relacionados a gestão de risco e segurança da informação. O programa de gestão de risco e segurança da informação foi liderado pelo Diretor1 que era o Diretor de SI da organização na altura. As equipas do projeto segundo o Diretor1 estão formadas da seguinte forma: do lado da SPMS estão o Responsável TIC, o Comité de Risco e Segurança da Informação e o Gestor de Segurança e Privacidade e Continuidade da Informação. Do lado do eSIS estão a Equipa de Coordenação do eSIS (SPMS), a Comissão de Acompanhamento TIC do eSIS e o grupo de trabalho do eSIS responsável pela gestão de risco e segurança da informação (Gomes, 2016a).

Segundo o PCA este programa já tem uns 3 anos e os documentos feitos na altura continuam válidos e agora é necessário passar da teoria para a prática. Ele prossegue *"uma coisa é estruturarmos os documentos e a forma de pensar sobre a cibersegurança de maneira teórica e outra com os recursos e equipas que existem, com os hospitais e as ARS implementa-las de facto".* Ele explicou que em 2017, muito antes do ataque *Wannacry* foi proposto da parte da SPMS à tutela (Ministério da Saúde) o 1º Despacho sobre notificações de risco e incidentes de segurança e "*desta forma o Despacho foi estruturado segundo a lógica do Cobit 5 em que deve estar envolvida a tutela no topo, os Conselhos de Administração e depois as demais entidades e é nesta fase em que nos encontramos" (PCA).* Quatro dias depois do ataque, foi escrita a proposta de Despacho e só foi assinado pela tutela em Outubro um Despacho mais forte sobre as estratégias da

saúde para a cibersegurança. O despacho foi publicado e a SPMS passou a implementa-lo e segundo o PCA "*contactamos presidentes dos hospitais para eles nomearem um CISO, ou seja, um responsável pela segurança, estamos a fazer um levantamento da arquitetura dos sistemas como um requisito obrigatório previsto no despacho. No fundo essa determinação da tutela permitiu-nos ter uma força organizacional para exigir um comportamento mais compliant com as regras de cibersegurança" (PCA).* Houve uma formação do Cobit na SPMS em que o Presidente, Coordenadores, os Responsáveis de TI e os Diretores de TI dos hospitais e das ARS na altura fizeram e nesta formação ficou claro de que há temas que devem ser discutidos a nível do Conselho de Administração e não com o Diretor de SI.

4.4.1- Adoção da Framework Cobit 5

Esta *framework* (figura 3, Anexo 2) tem como objetivo: compreender a relação entre os objetivos estratégicos da organização com os objetivos do Risco e Segurança de SI; os objetivos do SIS e a sua relação com os objetivos da gestão de Risco e Segurança; os cenários de riscos relevantes para o eSIS; aplicação dos facilitadores na vertente do risco e segurança de SI e compreender o funcionamento das operações de segurança de SI (SPMS, 2017c p. 7). Foi feita uma adaptação das regras e normas previstas no domínio da Segurança da Informação. Estas regras começaram a ser seguidas pela SPMS e estendeu-se a todas as organizações do eSIS (Gomes, 2016a).

***-Framework Cobit 5-* Objetivos dos SI associados ao Risco e Segurança:** Os objetivos do risco e da segurança têm como finalidade **gerar benefícios** e **criar valor** na entidade e permitem definir métricas comuns a todas as entidades do eSIS, desta forma foram definidos os cenários de risco mais relevantes para o eSIS (pode-se

confirmar as palavras de Ahmed, 2017 p.3 visto que o *Cobit 5 for risk* cobre vários cenários expressos na tabela 1, anexo 2) (Gomes, 2016a).

***-Framework Cobit 5-* Operações de Segurança.**

-Procedimentos/Processos: são todos os procedimentos operacionais especificados na gestão de risco e segurança da informação. Estes requisitos estão em conformidade com a implementação de normas ISO relacionadas a saúde (Gomes, 2016a).

-Tecnologia: são todos ativos tecnológicos como *hardware*, *software*, redes e os componentes da segurança que fazem parte das arquiteturas (Gomes, 2016a).

-Pessoas: são todos os recursos humanos que fazem parte desta vertente, ou seja, o risco e segurança da informação (Gomes, 2016a).

4.4.2- Facilitadores

Os facilitadores são os seguintes (tabela 2, Anexo 2): **1.Princípios, Políticas e *Frameworks***: são todos os princípios e políticas que as organizações devem obedecer e encontram-se no Anexo 2, tabela 3.

2.Processos: Os processos estão a ser implantados em duas vertentes: **a governança e a gestão** (tabela 4 do Anexo 2)**.** Na governança temos o domínio "***Avaliar, Direcionar e Monitorizar"*** permitindo que a *framework* de segurança da informação esteja alinhada as estratégias da saúde. Será necessário *garantir a manutenção da framework de governance, garantir a entrega de benefícios e o* ***processo de garantir a otimização dos riscos***. Na gestão, temos a fase ***Alinhar, Planear e Organizar*** todas as atividades que serão executadas. Estas atividades envolvem *planear a arquitetura, gerir os riscos, orçamentos e custos e todos os recursos materiais e humanos* para implementar as práticas de saúde eletrónica (estes pontos estão confirmados por Ahmed (2017, p.2) em que os processos (otimizar os riscos e gerir os riscos) são geridos nos domínios EDM03

e APO12 pelo *Cobit 5 for risk).* Segue a fase de ***Construir, Adquirir e Implementar*** as soluções eletrónicas. Para isso é necessário assegurar uma eficiente *definição de programas, definir padrões e mecanismos necessários para a prestação de serviços de saúde*. A fase de ***Entrega e Suporte*** tem como objetivo iniciar o programa e dar o suporte necessário, assegurando a *gestão de operações, serviços, problemas e incidentes*. E a fase de ***Monitorar e Avaliar*** tem como objetivo verificar se todas as etapas estão em conformidade com a legislação. Esta iniciativa deverá obedecer a legislação que fornece informações sobre a proteção das informações da saúde e são conjunto de leis nacionais que estão sendo partilhadas com todo o setor como o RGPD (Carrasqueiro, 2017 p. 21).

3. Estruturas Organizacionais: Foram definidas as seguintes estruturas locais:

-Conselho de Administração: É o Responsável Máximo pelo programa de governação e gestão incluindo o risco e cibersegurança (Gomes, 2016a).

-Comité de Segurança da Informação: É a estrutura responsável que se certifica que a entidade no geral aplique as boas práticas especificadas neste programa (Gomes, 2016a).

-Coordenador de Segurança: Assegura que os sistemas de informação sejam geridos de forma contínua. Esta área está subdividida em 4 partes: **Gestor de Segurança de Informação**, **Gestor de Segurança de Operações**, **Gestor de Segurança do Desenvolvimento Informático e Gestor de Segurança Física e Ambiental** e pode-se confirmar a teoria do ISACA (2013c, p.93) porque estes gestores são responsáveis pela gestão da segurança da informação na sua área de atuação. As tabelas 5 e 6 do Anexo 2 descrevem o nível de poder/autoridade e de responsabilidade destas Estruturas Organizacionais para o programa (Gomes, 2016a).

4.**Ética, Cultura e Comportamento:** foi definido um modelo com o objetivo de promover a melhoria no **Programa de Cultura** e **Segurança.** A SPMS tem realizado vários *workshops* não só para transmitir guias de boas práticas da segurança, mas também com objetivo de incentivar uma cultura desejável no setor (Gomes, 2016a, tabela 7 Anexo 2).

5.Informação: Os artefactos da informação estão definidos nas vertentes da segurança e do risco conforme a tabela 8 do Anexo 2.

6. Serviços, Infraestruturas e Aplicações: Foram definidos os principais serviços que deverão ser prestados neste contexto (ver tabela 9, Anexo 2).Na vertente da segurança, os serviços de arquitetura de segurança, consciencialização e avaliações de segurança são expressos pelo ISACA (2013c, p.110).

7. Pessoas e Competências: Segundo o Artigo 9 do Despacho nº8877/2017, as entidades estão apostar cada vez mais no investimento dos seus quadros de forma a habilitá-los na matéria de cibersegurança, por meio da formação sobre o projeto do Cobit5.Por meio de parcerias com universidades públicas e institutos de investigação, e as vezes com seus próprios recursos, a SPMS garante formação de qualidade para os seus quadros sobre Cobit 5 *Foundation,* Cobit 5 para a Gestão de Risco e Segurança, Arquitetura Empresarial, Auditoria e Controlo de Sistemas e Transformação Digital. Estas formações também estendem-se a todas instituições do eSIS e está disponível para todos os profissionais da saúde incluindo TIC, Clínicos e não Clínicos, Administrativos e de Gestão (SPMS, 2017d p.11).

4.4.3- Legislação e Regulamentos

Segundo o Diretor3 tem-se feito ao nível de privacidade e proteção de dados (RGPD) algumas ações de formação e *awareness* a nível interno. Dentro do organograma da

SPMS existe um núcleo dedicado a **privacidade e proteção dos dados na área jurídica** que trabalha de forma articulada com o núcleo de cibersegurança.

As entidades são orientadas a serem mais autónomas por exemplo devem criar o seu DPO (*Data Privacy Officer*) e terem as suas próprias políticas. A SPMS tem tido muito trabalho, fruto das dúvidas que os utilizadores têm sobre a proteção dos seus dados no SI, porque em muitos casos os sistemas utilizados por vários cidadãos e em algumas entidades são fornecidos pela SPMS. A equipa de privacidade de dados tem tido muito trabalho e trata do que vai responder. A nível da segurança, a SPMS bem como outros ministérios têm tido alguma participação, antes de a legislação sair os ministérios fornecem sempre algum comentário antes ser aprovada.

O Diretor3 citou o exemplo da Resolução do Conselho de Ministros 41/2018. Resumidamente esta norma fornece detalhes técnicos que as infraestruturas e os SI devem ter para estar em conformidade com o RGPD. Por exemplo uma base de dados para estar em conformidade com o RGPD deve registar todos os acessos que lhe são feitos. Se o programador XPTO ou algum administrador alterou a célula de uma determinada tabela isto deve estar registado. A princípio esta norma estava para ser implementada em 6 meses. Mas todos os ministérios optaram por 1 ano e meio adaptar todas as suas infraestruturas e sistemas para estar em conformidade com o RGPD e depois faz-se algum *awareness* por exemplo são emitidas notícias no *site* da SPMS e as entidades são orientadas a fazerem o mesmo.

O Diretor3 também relatou que eles têm reformulado algum clausulado nos contratos. A SPMS trabalha com várias empresas prestadoras de serviço, em muitos casos alguns dos sistemas não feitos pela SPMS mas por programadores de empresas que são contratadas. Nestes contratos são postos 2 clausulados que referem aspetos importantes

a nível de RGPD e as demais organizações são orientadas para fazerem o mesmo. As organizações podem também consultar a CNPD para mais informações.

4.5- Análise dos Impactos e Benefícios do Cobit 5

4.5.1.- Benefícios do Cobit 5

Segundo o Diretor4 os benefícios são muitos. Permite ganhos de eficiência, orientar e gerir melhor as organizações e um melhor planeamento estratégico. Quando as coisas estiverem mais estruturadas e maduras, permitirá um melhor serviço aos clientes finais (utentes). Estes benefícios assemelham-se aos benefícios destacados pelo ISACA (2013b p.10). Do ponto de vista interno, permite gerir uma DSI grande com base nas práticas do Cobit especificamente nas áreas de GSS, segurança, arquitetura empresarial e planeamento estratégico. As boas práticas do Cobit darão as ferramentas necessárias para a entidade atingir este rumo.

Para o Diretor1 foi mais fácil ter o controlo das atividades. Antes do Cobit 5 não era possível acompanhar todas as atividades porque eram muitas, com o Cobit foi possível acompanhar, avaliar, monitorizar, planear e corrigir as atividades de *governance*, no fundo os processos de *it governançe*.

Para o Diretor3, o ITIL é a *framework* que melhor complementa o Cobit. O Cobit5 tem ajudado a nível operacional na abordagem de processos da gestão de serviço e suporte e a nível da governação o Cobit 5 ajuda a perceber o papel do acionista, a visão do negócio e como isto articula com os processos de suporte das operações da gestão diária, está alinhado à *framework* interna de segurança da SPMS e com a arquitetura empresarial.

Embora os benefícios da adoção têm sido notáveis, não há resultados estruturados porque o programa ainda não foi executado por completo. Por exemplo ainda não

existem resultados das ações do núcleo da Cibersegurança. O Diretor3 explicou que ainda estão fazer trabalho de *awareness* e sensibilização e ainda não passaram para a implementação de pontos de controlo, portanto não estão a medir com base em métricas sustentáveis. "*Temos poucos pontos de controlo a parte do circuito que montamos, temos um programa de notificação obrigatória por causa da responsabilidade que temos com o CNCS aquém reportamos. Ainda temos poucos incidentes quer da nossa parte, quer da parte das entidades que reportaram. São métricas muito generalizadas para dizer que já temos respostas derivadas das ações do nosso núcleo".* O entrevistado propôs um plano futuro que será visto mais adiante o que permite também ajudar as organizações a corrigir as falhas de segurança.

Outro aspeto é que ainda não foi feita uma análise estruturada do desempenho das entidades na área da cibersegurança. O Diretor3 explicou que tem recebido algumas evidências, as entidades fornecem exemplares a explicar se têm ou não políticas de segurança. Em outros casos a SPMS faculta os seus em *templates* para as organizações que não possuem e assim elas vão adaptando conforme a sua realidade. Segundo o Diretor3 os resultados são positivos, algumas entidades têm um grau de maturidade muito superior ao da SPMS em termos segurança interna. Outras tem a maturidade muito baixa e a SPMS tem tido dificuldade em fazer com que as mesmas prestem atenção ao assunto.

Todos os entrevistados salientaram que o Cobit 5 tem servido para formação de pessoas. O PCA explicou que houve 2 seções de formação para os chefes máximos, conselhos de administração para eles entenderem a importância da *framework*. Houve formações em Lisboa e no Porto em que foram abordadas temáticas de governação.

4.5.2- Impactos na governação e gestão das Infraestruturas de TI

Segundo o Diretor1, com o Cobit 5 foi feita a governação e gestão dos ***assets*** que são os ativos ou as infraestruturas da organização. Ele explicou que por ser uma ferramenta de alta gestão, o Cobit 5 permitiu-lhe fazer a gestão em várias dimensões tais como a gestão da arquitetura, gestão da aquisição, gestão da estratégia e principalmente a gestão de risco e da segurança. Concluindo ele disse que "*o Cobit permitiu fazer uma combinação destes parâmetros e gerar benefícios, ao mesmo tempo em que se vai se mitigando os riscos e racionalizando os resultados" confirmando a teoria do* ISACA, 2012 p. 13 de que o Cobit permite gerar benefícios através da otimização dos riscos.

Para o PCA, é necessário dinheiro no investimento de novas infraestruturas. A organização não tem tido dinheiro para pensar nas infraestruturas de forma estratégica. Ele explicou que são situações diferentes: "*uma coisa é comprar uma infraestrutura por que está acabar, ou é necessária, ou porque temos problemas de espaço de "storage" ou porque a máquina de 9 anos foi a baixo"*. Ele explicou que há pouco dinheiro para investir nas infraestruturas o que acaba por não sobrar tempo para o pensamento estratégico.

Segundo o Diretor3, o Cobit tem ajudado numa lógica de repensar todo o ecossistema infraestrutural de forma estratégica de como pode ser montado um sistema hospitalar no geral, ou seja os SI que dão suporte ao atendimento assistencial ao hospital e aos utentes sobretudo nos cuidados sub-primários. Este pensamento de como estruturar uma solução integrada em que uma parte são os SI da SPMS mas também como serão suportados em termos de infraestruturas, redes, segurança, governação e suporte, as boas práticas do Cobit têm sido uma mais-valia.

Para o Diretor4 o Cobit serve de guia área de GSS. Esta área está assente no núcleo do eSIS e está a ser reestruturada quer do ponto vista interno e externo e mapeada com base nos princípios e políticas Cobit/ITIL e permite estabelecer pontos de contacto com os *stakeholders*. Todas as componentes de serviço como a gestão de serviço, dos ativos, de problemas, incidentes, bases de dados de conhecimento estão assentes nos processos que vão sendo gradualmente implementados com base nestas práticas. Por exemplo já existe um gestor de serviço e era algo que não existia, haverá um gestor de problemas e incidentes e com base no Cobit já é possível definir papéis e responsabilidades para as pessoas e mapear os processos e políticas. Estes aspetos podem relacionar-se com a teoria de Tucker (2014), que mostra que o Cobit 5 fornece boas práticas relacionadas à gestão de serviço e suporte.

4.5.3- Impactos nas Perspetivas dos stakeholders da saúde

Para o PCA e o Diretor4, os impactos são positivos. O PCA disse que há um reconhecimento por parte dos *stakeholders*, eles vêm que a SPMS tem as ideias bem arrumadas para a cibersegurança e isto dá-lhes algum sentimento de segurança. Por exemplo a SPMS celebrou um acordo para a cibersegurança com a ANF e estes se comprometeram em seguir as orientações da SPMS. Também o Diretor do CNCS afirmou que a saúde tem as estratégias bem montadas para a cibersegurança para aquilo que pretende fazer. Foi também assinado um protocolo de cibersegurança com o Centro Hospitalar Universitário de Coimbra.

Para o Diretor4, os *stakeholders* também se beneficiam deste programa. Com base no Modelo de Governação foi criado um conjunto de grupos, um conjunto de organismos de gestão e liderança para os conselhos da administração e a tutela e depois ao nível da

gestão e operacional. As políticas a serem criadas foram um conjunto de grupos de trabalhos, de comissões que permitem governar e definir por um lado a mudança e o acompanhamento no eSIS. São grupos que trabalham em áreas como planeamento estratégico (macro), nas questões operacionais e na gestão. E desta forma, os *stakeholders* participam nos fóruns e levam para as suas entidades as boas práticas que são difundidas nestas áreas (segurança, arquitetura empresarial, formação das pessoas). Este programa permite uma articulação com os *stakeholders* porque eles normalmente reportam problemas e acabam por se beneficiar dessas boas práticas.

4.5.4-Pontos Positivos e Negativos da Adoção

Segundo o Diretor1, o ponto positivo é que o projeto permite estabelecer políticas de segurança; construir um modelo de risco e transversal; a criação de estruturas organizacionais; a possibilidade de gerir novas iniciativas como a mudança e a gestão, gestão da estratégia e a gestão da arquitetura empresarial, gestão de risco e segurança, gestão da inovação e das competências, gestão de serviços de TI e gestão dos fornecedores e permite uma melhor governação e gestão.

O ponto negativo apontado pelo Diretor1 é que o Cobit 5 é uma *framework* um bocado disruptiva, o que obriga a que as pessoas tenham formações constantes para que possam trabalhar de forma diferente e contribuir para o desempenho da mesma. Assim foram necessárias formações variadas para que as pessoas estivessem à altura de trabalhar com o Cobit.

Para o PCA, o ponto negativo é que as pessoas ficam presas demais a *framework* do Cobit. Se algo não foi feito ou dito a nível do negócio, as TI não fazem nada. Ele explicou que quando o pessoal da TI vem com uma ideia nova, com uma nova tecnologia, se a pessoa que estiver no negócio não conhecer as potencialidades das TI

acaba por não tomar as decisões necessárias. Isso cria uma dependência muito negativa. Desta forma ele concluiu o seguinte " *mesmo quando o chefe máximo não tiver uma opinião formada sobre o assunto as decisões devem ser tomadas"*. O PCA não destacou aspetos positivos.

Para o Diretor3 o ponto positivo é o fato de haver repetições nos resultados, a certeza de que se as coisas forem feitas da mesma forma poderão ter os mesmos resultados dando garantias de eficácia. O ponto negativo é que se as atividades forem feitas com base em processos informais e não estiverem documentados constituirão um grau de dificuldade. É necessário haver tempo, recursos e energia para trabalhar e robustecer os processos ou muitas vezes pedir ajudas. O entrevistado ressaltou que é importante ter a noção de como as coisas devem ser feitas e analisá-las com base numa lógica de como se devia fazer visto que os processos têm *inputs*, *outputs* e responsabilidades.

4.5.5- Benefícios do Modelo GSS

Segundo o Diretor3 esta é a área que mais tem-se beneficiado e está alinhada com todo o modelo estruturado baseado em normas de gestão e governação (Cobit) e gestão de incidentes e serviços (ITIL). Este modelo visa melhorar a prestação e a entrega de serviços de TI alinhando com as estratégias do negócio proporcionando benefícios a vários *stakeholders* (utentes, profissionais de saúde, gestores). Facilita a comunicação de reporte de incidentes e pedidos resultando em ganhos de eficiência. Permite obter registos estruturados destes incidentes possibilitando melhores tomadas de decisão (ENESIS, 2017). Com base neste modelo, está ser desenvolvido um processo de notificação obrigatória. O Diretor3 explicou que a equipa estava a desenvolver de forma separada todo o processo de notificação obrigatória abstraído dos modelos desenhados para a GSS. Foram feitas as correções e agora os processos de notificação obrigatória

usam a mesma plataforma e estão alinhados à GSS só que são mais específicos para a segurança.

4.5.6- Adaptação à Mudança

Os Diretores (Diretor1 e Diretor3) compartilharam o mesmo ponto de vista de que não está ser fácil. O Diretor1 disse que esta questão é difícil de responder porque os colaboradores ainda estão a adaptar-se. O Diretor3 explicou que depende muito da área. Em áreas como a GSS, os resultados têm sido mais notáveis do que nas áreas técnicas como a manutenção e infraestrutura. Na GSS já se está robustecer o modelo, rever os processos e adicionar pontos de controlos e a melhorar a parte que está a ser trabalhada com o Cobit e ITIL. Em outras áreas como a manutenção fez-se algum trabalho de documentar alguns processos mais ainda não está a ser sentido, ou seja não há mentalidade de que "*estamos a trabalhar sob processos" (Diretor3).*

4.6-Recomendações do Projeto: Programa de ativação de Boas Práticas

Para partilhar as suas boas práticas com as entidades, a SPMS utilizou o programa de boas práticas, ou seja os **Kits de Ativação** (figura 4 do Anexo 2). Este programa de ativação de boas práticas está disponível para as entidades do SNS (Centros Hospitalares, Hospitais, ARS e os SPMS). Os resultados do grau de maturidade das organizações são apresentados no *dashboard security* e é um passo para se iniciar as auditorias, conforme ilustrado na figura 5 do Anexo 2 (Gomes & Soares, 2016 p. 8).

Segundo o Diretor1, a SPMS criou Kits de ativação que contêm recomendações e foram usados para partilhar com outras organizações que possuem características e contextos semelhantes as suas boas práticas para que estas organizações pudessem adotar.

O PCA disse que ainda não falaram com nenhuma organização similar. No caso dos hospitais e cuidados sub-primários, foram emitidas as *guidelines*, quatro normas de segurança que podem ser vistas no *site* da SPMS explicando as funções de cada um. Sobre os *kits* de ativação, o PCA relatou que foram enviados e feitas as sensibilizações e agora resta saber se as organizações os usam. As organizações devem reportar o seu desempenho enviando à SPMS os documentos analisados, discutidos e aprovados pelos conselhos de administração.

Para o Diretor3, os *assessments* são uma componente do programa de ativação. Em termos de partilha com as entidades, tem-se feito a aplicação de políticas de segurança de informação aprovadas pela SPMS. A organização já tem uma política de *backups*, de controlos de acesso e isto vai permitir adotar controlos nestas políticas e pode-se relacionar com a teoria do ISACA (2013c, p. 78) que mostra que as organizações podem aplicar controlos críticos nas políticas para reforçar a cibersegurança dos seus ativos. As organizações deverão dizer se têm processos associados a estas políticas e vão se adotando os controlos para estabelecer métricas e fazer uma gestão destas políticas.

4.6.1-Controlos Críticos de Cibersegurança

A SPMS está a adotar os CIS (Controlos Críticos de Cibersegurança- *Controls for Effective Cyber Defense Version 6.0*) que estão num formulário (figura 6, Anexo 2). São os 20 controlos do SANS e este ponto confirma a teoria do ISACA (2013c, p.58). Com estes procedimentos, as organizações podem ter uma noção clara sobre os controlos, e decidir quais devem adotar para as suas necessidades. A explicação detalhada destes controlos encontra-se num manual intitulado *CIS Controls Version 7*, disponível em https://www.cisecurity.org/critical-controls.cfm (Gomes & Soares, 2016 p.9).

4.6.2- Perspetivas e Planos Futuros

O Diretor1 foi mais positivo e relata que *"nós temos dado formação aos Conselhos de Administração e aos Diretores de Informática para isso mesmo, para adotarem o Cobit, e neste sentido o setor da saúde já começa estar muito avançado*".

A perspetiva do PCA foi negativa, porque não há técnicos suficientes, a Administração Pública não está contratar informáticos. Existe uma grande escassez de quadros e profissionais de TI principalmente nos hospitais públicos e mesmo na SPMS. Ele explicou que *"não adianta falar do Cobit quando temos problemas mais graves para resolver, isso é que nos preocupa. É claro se houver direções fortes, departamentos musculados com técnicos importa sim falar".*

O PCA ressaltou a importância de haver a componente da governação no âmbito hospitalar. Os dirigentes dos hospitais normalmente têm cursos relacionados a gestão mais não têm bases sobre governação de TI, porque as pessoas têm várias preocupações como medicamentos, despesas e compras e não dão importância à governação. Desta forma faz sentido haver esta componente no setor hospitalar porque "*se os cursos gerais de administração hospitalar tiverem e devem ter uma área de TI forte e dentro desta área tiver aspectos relacionados à governação, não só falar de software, hardware provavelmente será muito bem-vindo" (PCA).*

Planos Futuros para o Projeto de Adoção Cobit 5

Diretor3: Melhorar a capacidade de resolução e resposta dos incidentes:" quanto a resolução e resposta dos incidentes nós fazemos um trabalho de insistência junto das equipas de suporte, não temos uma equipa autónoma que ajuda a resolver os problemas, ou seja não temos a capacidade operacional de ajudar. Temos este plano em marcha que é melhorar a nossa capacidade de resolver estes problemas".

Diretor3: Fomentar práticas para a gestão da inovação: "ainda não temos um programa estruturado mas temos como objetivo este ano fazer um programa relativo à gestão da inovação no SNS e na SPMS".

Diretor3: Implementação de pontos de controlo e capacidade de mitigar os riscos e falhas de segurança: "temos como objetivo implementar pontos de controlo e já poderemos no próximo ano ter a capacidade de ter um circuito de feedback para verificar se há melhorias ou retornos positivos das ações do núcleo de cibersegurança.

Diretor3: Medir o grau de maturidade: "temos como meta começar a medir para ver em que nível estamos. Quando tivermos processos definidos, começaremos a medir para ver se conseguimos evoluir o nosso grau de maturidade dentro do Cobit."

Diretor4: Consolidação das diferentes áreas: "temos como planeamento a evolução dos processos, políticas e as boas práticas relativamente ao *roadmap* do Cobit. Na área de GSS vamos implementar a gestão de processos, problemas entre outros. Vamos melhorar as áreas como a gestão do planeamento estratégico, arquitetura empresarial e sobretudo na consolidação do Modelo de Governação".

4.6.3- Lições Aprendidas

O PCA explicou que as ideias têm de ser trabalhadas e divulgadas e não apenas estar na mente do Diretor. Ele explicou que o que não correu bem é que os documentos não foram trabalhados com os vários membros da Direção. É importante haver mais intercâmbio com os funcionários, especialmente com o pessoal das TI porque são estes que fazem a segurança, mantêm o *hardware,* fazem o software e há grande necessidade deste pessoal trabalhar na elaboração dos artefactos e dos documentos. Embora os documentos estejam bem elaborados teoricamente mais não têm aplicação prática.

Os entrevistados (Diretor1 e PCA) concordaram que as pessoas dos Conselhos de Administração devem liderar este projetos, e esta concordância é confirmada pela definição de Governança de TI do ITGI (2003, p.10). "*Para estes tipos de iniciativas deve-se ter a liderança das pessoas dos Conselhos de Administração, porque muitas vezes as pessoas das TI não facilitam esta adoção, elas não têm uma visão da organização num todo" (Diretor1).* O Diretor1 explicou que o pessoal da TI muitas das vezes não se revê nessa *framework,* e não percebem os benefícios que a mesma pode

trazer. Nesse caso a SPMS tem dado cursos de formação sobre o Cobit que estão a decorrer até agora a fim de se criar esta mentalidade.

O PCA explicou que muitas vezes os hospitais têm dificuldade em perceber que devem enviar alguém do Conselho de Administração e não da informática. Mas ele ressaltou que tem estado a melhorar a cada dia, alguns dirigentes já percebem que os SI são estratégicos e devem ser acompanhados ao nível do Conselho de Administração, embora alguns ao receberem notificações da SPMS reencaminham para o Diretor de Informática. Entretanto alguns já estão mais interessados com a informática no geral e com a cibersegurança em particular. Ele concluiu o raciocínio dizendo que eles estão mais preocupados com a cibersegurança do que as vezes com temas operacionais tais como o funcionamento do sistema achando que cabe apenas na responsabilidade do Diretor de TI.

Segundo o Diretor4, um dos aspetos é a complexidade da gestão da mudança. " *Muitas vezes somos demasiado ambiciosos e queremos atingir resultados muito rápidos e não é fácil trabalhar com um conjunto de pessoas que não estão habituadas em muitas áreas a trabalhar com processos e políticas claras".* Ele concluiu que mais vale ir devagar e de forma segura do que definir objetivos demasiado ambiciosos e não alcançar. Ele também explicou que *frameworks* como o Cobit e o ITIL são muitos bons teoricamente, o mais difícil é adaptar as regras, as boas práticas com a realidade concreta de cada organização. Portanto não necessariamente deve ser seguido tudo o que lá está porque nem sempre faz sentido o que gera maus resultados, mostrando uma opinião similar ao PCA.

O Diretor3 compartilhou a mesma visão e explicou que "*há uma falta de capacidade de traduzir a teoria em prática não que a teoria esteja errada. Uma implementação pouco*

experiente da teoria nem sempre leva aos resultados desejados. É importante ter a maturidade certa para saber como traduzir a teoria para prática".

4.7.-Discussão e Síntese do Estudo de caso com a Literatura e as Entrevistas

Este capítulo mostra os pontos semelhantes e diferentes entre estudo de caso com a literatura e os comentários dos entrevistados.

Pontos Similares

Os objetivos do modelo de governação da SPMS são similares aos objetivos da governança de TI descritos por Simonsson & Johnson (2017, p.1). Neste modelo inspirado no Cobit 5, a SPMS garante a participação de todas organizações, alinha as estratégias de TI com a AP e com os objetivos da saúde, e permite um alinhamento das práticas do Cobit 5 a nível local, nacional e internacional. A SPMS é o CIO do MS e responde pela estrutura da Governança de TI na saúde.

Suomi & Tähkäpää (2004) afirmaram que as organizações da saúde têm pouco conhecimento sobre práticas de governança de TI. O PCA comentou esta afirmação dizendo "*as organizações não têm conhecimento nenhum. Elas têm uma prática de gestão rudimentar (elementar) no geral e gestão de TI pior ainda, não há gestão em muitos hospitais e sim administração",* mostrando uma opinião contrária a de Suomi (2001) de que deve haver a componente da gestão na saúde. Existe diferença entre gestão e administração hospitalar. "*A administração hospitalar é robusta. Deve haver 3 ou 4 hospitais em que as práticas de gestão de TI são maduras consistentes que seguem regras e lógicas que podem ser encaixadas na framework do Cobit, de resto são práticas generalizadas, porque ainda não estão conscientes de como governar as suas tecnologias" (PCA).*

Os facilitadores ajudam as organizações a atingir os seus objetivos (ISACA, 2012; Oliver & Lainhart, 2012). Os Diretores (Diretor1 e Diretor3) explicaram que os processos são um dos facilitadores mais trabalhados. O Diretor3 deu 3 motivos que mostram que os processos têm tido mais atenção: o Conselho entende que a organização atingiu uma grande dimensão em que a formalização e a sustentabilidade dos processos é determinante e isto implica a necessidade de haver processos claros e definidos. Segundo, a SPMS passou por uma reestruturação e a nível dos Departamentos, Direção e Coordenadores sentem que já não é possível garantir uma articulação apenas com mecanismos informais. São necessários processos claros que garantam que os produtos criados estejam articulados a outros. E terceiro a nível das equipas devido aos acréscimos e transições de responsabilidades e pela diversidade de produtos que são feitos. Estes motivos mostram que a ausência de processos definidos costumam ser um entrave.

O Diretor3 relatou que alguns cenários de risco estão minimamente desenvolvidos. Está a ser desenvolvida uma ferramenta para a análise de riscos e está ser revisada. As análises de riscos não foram feitas para todos temas. O Diretor3 explicou que estão ser feitas na lógica *top-down*, ou seja a nível do negócio, que catálogos de serviços são mais vitais não para a organização toda. Estas análises ainda são experimentais e estão a ser feitas com base na lógica dos serviços prestados pela DSI, e quais destes serviços parecem ser mais vitais para os *stakeholders*. Por exemplo fez-se para a prescrição eletrónica de receitas e para 2 temas que pareciam mais críticos e os cenários de riscos foram selecionados na lógica *top-down,* confirmando a teoria do ISACA *Journal* (2011, p.1) porque essas análises foram feitas numa lógica de se perceber quais serviços seriam críticos para os *stakeholders* externos.

O Diretor1 comentou a teoria do ISACA (2014) de que o Cobit 5 alinha-se com outras *frameworks e* este alinhamento está especificado na *framework* da gestão de risco e segurança. Esta adoção canaliza orientações para utilização de outros *standards* e práticas como ISO 20.000, Arquitetura Empresarial e a ISO 27.001. O Cobit fornece guias para a adoção das práticas da gestão de serviço, de segurança, arquitetura empresarial, gestão da inovação e foi possível dar um salto para adotar todas estas práticas que não são do Cobit mas que ele faz referência. Por exemplo usa-se a ISO 27.000 para a segurança porque o Cobit fornece guias, assim como para melhorar a gestão de serviço dos utilizadores o Cobit pede para usar a ISO 20.000. "*O Cobit é uma framework que faz a junção e orquestração dessas boas práticas*" (Diretor1).

O PCA fundamentou a teoria de Ahmed (2017) mostrando que o conselho de administração da SPMS tem dado apoios sobretudo na área da segurança. A SPMS conseguiu vários orçamentos para a cibersegurança no verão de 2017. Promoveu-se uma articulação com a Agência Europeia um evento da Cibersegurança em Novembro e foram convidados vários membros do Governo. E sempre que há pedidos de compras relacionadas com a cibersegurança normalmente são bem-vindos dependendo das disponibilidades financeiras.

Segundo Ahmed (2017), é muito importante num programa de governação e gestão de TI haver a disseminação de uma cultura consciente para os todos os níveis e departamentos. As opiniões dos entrevistados confirmaram este ponto embora houve pequenas diferenças nos comentários. Segundo o PCA, a nível interno esta disseminação ainda não foi muito abrangente. Houve uma formação para os dirigentes intermédios mais é necessário uma sensibilização mais alargada para garantir que todos os colaboradores tenham noção sobre o Cobit porque nem todos conhecem.

O Diretores (Diretor3 e Diretor4) ressaltaram que há resultados positivos a nível externo. O Diretor3 relatou que já têm feito muito trabalho de *awareness*, consciencialização e sensibilização a nível das equipas. Ele explicou que não consegue medir os impactos resultantes desta contribuição, mas os resultados são positivos porque muitas dessas sensibilizações não eram feitas. A SPMS tem conseguido fazer com que as entidades façam-lhes chegar o seu planeamento estratégico a nível de SI. Eles têm sensibilizado as tutelas sobre o que são responsabilidades partilhadas e o diferencial de alocação que põem em causa estas responsabilidades. Apesar de haver resultados positivos, existem entidades mais sensibilizadas do que outras porque nem todas têm a *awareness* completa e nem estão totalmente conscientes do papel do Cobit 5 para a governação dos SI no MS.

O Diretor4 disse que de forma geral as entidades já percebem o que é o eSIS. Muitos profissionais dos Hospitais e das ARS estão formados e certificados com o Cobit 5 formações estas patrocinadas pela SPMS. Ele partilhou o ponto vista do Diretor3, dizendo que há níveis de maturidades diferentes. Alguns hospitais já têm um Modelo de Gestão de serviço e suporte, políticas de gestão de risco e segurança claramente mapeadas com os processos do Cobit. Algumas instituições estão a implementar o Cobit, outras ainda não começaram e outras não têm recursos. Nas reuniões que têm sido promovidas conforme o Modelo de Governação e nos fóruns ENESIS tem-se promovido vários debates relacionados com o Cobit 5.

Um outro aspeto final ressaltado pelo Diretor4 "*é a estimulação dentro do modelo das competências alguns perfis e responsabilidades que os profissionais devem ter de acordo com os princípios do Cobit"*. Ele concluiu que sim que de forma geral as organizações conhecem o Cobit e participam no modelo de governação, confirmando as

palavras de Suomi & Tähkäpää (2004) de que deve haver colaboração de todos os conselhos da saúde no programa de governação.

Pontos Diferentes

Dois entrevistados responderam que não foram feitas as auditorias de cibersegurança e isto difere da teoria do ISACA (2013c p. 121), embora este seja um requisito do modelo de governação previsto no Artigo 7 do Despacho 8877/2017. O PCA comentou que foram feitas algumas auditorias nos *datacenters* e fez-se auditorias de desempenho em 17 hospitais na área do *software* SONHO. O objetivo ainda este ano é promover exigências de que se façam auditorias de cibersegurança cumprindo esta norma do Despacho.

O Diretor3 explicou que "*tem-se feito assessments técnicos com softwares próprios que fazem o varrimento de vários temas. Leva-se uma pendrive e coloca-se com a colaboração dos colegas da entidade e o software varre o sistema e verifica vulnerabilidades de portos abertos, firewalls com exceções e faz testes automáticos"* (Diretor3). Segundo Diretor3 ainda não se realizou esta atividade porque as políticas e processos ainda não estão maduros. Este ano a SPMS começou a divulgar as suas políticas e as entidades deviam ter as suas e darem a conhecer à SPMS. A SPMS ainda está a desenvolver processos internos de cibersegurança como é caso da ferramenta de análise de risco e também processos de gestão de acesso. Desta forma ele concluiu que só faz sentido fazer auditoria só se houver algum *standard* que permita auditar.

Embora os Conselhos de Administração são os que tomam a decisão máxima em programas de governação e gestão das TI conforme o ITGI (2003 p.10), ainda existe um nível de conhecimento baixo nessa área. O PCA relatou que foi feito um "*Conselho de Administração Especial*", foram adotadas algumas políticas e conversou-se sobre o

assunto. Mas como Conselho de Administração eles não têm tido muita conversa sobre Cobit, governança e cibersegurança. Dentre os variados temas que eles tratam como medicamentos, compras e comunicação, quando chegam no assunto das TI nem sempre descem no nível seguinte são as operações, serviços e segurança. Normalmente estes assuntos são mais abordados nas conversas que os diretores de TI têm tido com o Presidente.

4.7.1- Recomendações e Sugestões

-Necessidade de uma mentalidade estratégica nos investimentos de TI: Para criar esta estrutura mental, a Governança de TI deve estar alinhada ao planeamento estratégico da organização. Este pensamento estratégico deve começar no topo e nos diretores de TI conforme o PCA "*se conseguirmos que os nossos dirigentes e diretores de TI pensem estrategicamente mas sobretudo metodologicamente a sua estratégia melhor".*

-Os Conselhos de Administração devem ter competências sobre temas relacionados a governança de TI e *frameworks*: Estas temáticas devem estar no topo das conversas do Conselho de Administração para que as decisões certas sejam tomadas. O PCA explicou que muitos hospitais ainda tem problemas em perceber esses assuntos são da responsabilidade do Conselho. O motivo pode ser a falta de habilidades que os Conselhos de Administração têm sobre o Cobit, portanto os Conselhos de Administração devem ter bases sólidas nestas temáticas. O Presidente falou sobre a necessidade de haver mais técnicos de TI para cuidarem da segurança. Esta preocupação pode ser reportada à tutela.

É importante que seja disseminada **uma cultura consciente a nível interno.** Embora os dois Diretores salientaram que há resultados positivos a nível do eSIS, o PCA explicou

que nem todos os colaboradores da SPMS conhecem a *framework*. A DSI pode providenciar formações específicas sobre o Cobit a nível dos departamentos para que os demais funcionários tenham a noção das novas políticas e processos estão sendo implementados e que poderão ter impactos nas suas atividades no futuro.

Sugere-se e recomenda-se a DSI a **criação de uma equipa interna na DSI dedicada nos aspetos relacionados e governação e *frameworks***. Embora estes temas sejam importantes, um dos Diretores afirmou não foi investido muito tempo neste trabalho. Esta equipa pode ajudar a DSI a como adotar estas *frameworks* e no desenvolvimento organizacional da entidade. Esta equipa poderá assegurar como as práticas do Cobit podem ser úteis para uma necessidade específica, que boas práticas do Cobit 5 podem ser úteis para o Departamento. A criação desta equipa seria uma grande ajuda nestas reflexões.

4.7.2- Análise Crítica

Esta secção refere-se a uma análise da investigadora consoante o material pesquisado e pelas entrevistas realizadas.

O primeiro ponto a ressaltar é que a SPMS ainda não tem um programa estruturado a nível de governação e gestão espelhada no Cobit 5. O projeto encontra-se numa etapa inicial, mas a *framework* tem sido útil em fornecer ideias de como estruturar as componentes de uma forma lógica. É evidente que o Cobit 5 atende as necessidades de qualquer organização, mas um ponto interessante neste estudo é pelo fato do Cobit 5 ser uma *framework* que além de facilitar o trabalho que tem sido desenvolvido pela SPMS, acaba também por orientar um conjunto de organizações que embora estando no mesmo setor têm características, maturidades e contextos diferentes.

Pode-se afirmar que esta adoção está a ter um efeito positivo na reestruturação da SPMS. A SPMS fez um novo planeamento estratégico e segundo o PCA, o Cobit ajudou a organizar os objetivos em camadas começando da camada de negócio até a tecnológica. Segundo um dos Diretores, a SPMS teve um crescimento muito acelerado e gerou um aumento das atividades nas áreas de coordenação. Por exemplo a nível interno já se consegue transmitir orientações mais específicas sobre segurança às equipas que estão a desenvolver e a manter produtos nos Sistemas de Informação e permite mais eficiência na execução das atividades.

Foi também interessante perceber que a SPMS tem uma responsabilidade bastante abrangente não só no ecossistema da saúde português mas também a nível Europeu e nesta ótica o papel do Cobit 5 é bem visível no que toca a transmissão de boas práticas. Todas estas responsabilidades constituem desafios para a SPMS levar a cabo a sua missão e objetivos.

Particularmente na DSI, a criação dos núcleos é vantajosa porque permite melhor eficiência no trabalho a nível da governação e do Cobit 5. Estes núcleos permitem dar um acompanhamento mais focado nas atividades e facilita na gestão permitindo a SPMS divulgar as boas práticas a nível nacional e internacional.

O projeto ainda não foi executado na sua totalidade mas um dos entrevistados acredita que a estratégia está bem definida e poderá ter muitos êxitos no futuro principalmente na componente da segurança uma vez que vivemos num cenário de crise informática sujeito a ciberataques sucessivos. Entretanto os benefícios são visíveis. Permite mapear o trabalho que tem sido feito a nível operacional em áreas como a segurança, arquitetura empresarial, gestão das competências e na gestão de serviço e suporte. A macro estrutura do Cobit permitirá a SPMS adotar normas, políticas para a governação e o

alinhamento das TI com o negócio. A consolidação de todas as áreas permitirá a evolução de processos e políticas robustas e gerir melhor os recursos do eSIS possibilitando uma melhoria no desempenho dos sistemas de informação na saúde.

4.7.3-Resposta à Questão de Investigação

A questão de investigação é a seguinte: Como as organizações podem mitigar as falhas e riscos de TI utilizando de forma eficaz as diretrizes do Cobit 5 para a Gestão de Risco e Segurança da Informação? O primeiro passo é a adaptação de regras e políticas existentes na vertente da segurança e gestão de risco (Gomes, 2016a). Segundo a Sonda S.A, uma empresa da América Latina do setor das TI, é necessário integrar os objetivos de TI com as necessidades da sua organização, porque as políticas de TI serão mais eficazes se estiverem dentro dos objetivos do negócio. Um segundo fator é que as organizações podem mitigar os riscos implementando controlos adequados mas que devem estar em conformidade com o Cobit 5. As organizações podem fazer testes para verificar os controlos mais adequados para os cenários de risco (ISACA, 2013c p.72), e segundo a Sonda S.A, as empresas podem usar dados para medir o seu desempenho para verificar os impactos dos riscos e incidentes. Segundo Espirito Santo (2010 p.5), os pontos de controlo devem ser adotados. Identificados os impactos dos riscos, estes pontos podem ser implementados para reduzir ao máximo os riscos porque nunca se sabe ao certo se os riscos foram mitigados. Segundo a Sonda, um último passo é rever as políticas que mitigam os riscos. O gestor de TI deve estar atento às atualizações de novos processos que vão fazendo parte do negócio. É necessário que a equipa de gestão de risco seja treinada para estarem a par destes novos processos.

Capítulo 5-Conclusões

Esta dissertação teve como foco principal estudar a *framework* da governança de TI que é o Cobit 5. Da revisão da literatura conclui-se que a governança de TI é uma ferramenta bastante indispensável para as organizações. As organizações só poderão ter sucesso se incorporarem as TI dentro dos seus processos de negócio. Quando estes itens operam em conjunto as organizações conseguem alcançar os seus objetivos e ter vantagens competitivas. O Cobit 5 é uma *framework* robusta e reconhecida a nível internacional e ajuda as organizações a alcançar os seus objetivos. A grande vantagem do Cobit 5 é que ele é adaptável à situação de qualquer empresa e fornece princípios e políticas que ajudam a gerir e governar os processos de negócio e tem a TI como um meio de gerar valor ao negócio.

No estudo de caso, a SPMS está a levar a cabo um programa visando a governação e gestão das TI para a saúde usando o Cobit 5. A SPMS elaborou um modelo de governação, e com base nesta estratégia tem permitido a participação de todos as organizações da saúde e dos outros *stakeholders* o que permite também divulgar boas práticas a nível internacional.

Por ser uma *framework* abrangente o Cobit 5 alinha-se com outras *frameworks*, e nesse sentido a SPMS está a implantar várias iniciativas em áreas já mencionadas. Conclui-se que cada uma dessas iniciativas contribui para a melhoria contínua reforça o modo como a entidade tem dado eficiência ao trabalho feito nestas áreas como a resolução de incidentes, a implementação de práticas de segurança e de risco e os *stakeholders* têm tirado vantagens destas boas práticas. Permite que governação dos sistemas de informação da saúde seja mais abrangente e coerente.

Conclui-se que os Conselhos de Administração devem tomar as lideranças nesses programas, e para tal é necessário que os membros dos Conselhos de Administração tenham as competências necessárias nesses temas para que haja o alinhamento e o valor seja criado. Das entrevistas concluiu-se que o Cobit 5 ajuda na pensar de forma estratégica de como montar as ideias que por sua vez devem obedecer uma sequência lógica. A SPMS é uma entidade vasta e gere as TI de um setor muito grande e complexo. Os entrevistados mostraram que o Cobit ajuda numa lógica de pensamento de como governar esta complexidade e ajuda a organizar as ideias de como alocar as atividades. Também conclui-se que devido a implantação de novos processos fica difícil gerir a mudança porque nem todos facilmente adaptam-se a novos processos e políticas, portanto se houver dificuldades neste aspeto, não se consegue chegar aos resultados desejados. Portanto ao definirem-se metas e objetivos é necessário haver uma preparação em toda empresa começando do topo até as equipas sobre a evolução de novos processos e políticas de modos que haja mais comprometimento por parte das pessoas. Por outro lado a organização deve ser realista ao estabelecer estas metas tendo em mente de que poderá haver resistências por parte de alguns funcionários e/ou departamentos.

Um aspeto importante a ter em conta são os cenários de risco do Cobit 5. Sendo uma *framework* que alinha a TI com o negócio, ele fornece bases que ajudam a ter uma visão completa da empresa. É aconselhável que as empresas optem sempre pela abordagem *top-down*, não que a *bottom-up* seja menos importante. A vantagem da abordagem *top-down* é o seu foco nos detalhes que impactam os objetivos da empresa, e no caso da SPMS ajuda a refletir os objetivos do negócio. De acordo com Neto (2010) as organizações devem perguntar-se: Quais são as prioridades da nossa empresa? O que

pensa a alta gestão, os nossos *stakeholders* sobre o que são riscos e percebermos que controlos podemos usar para reduzi-los? Estes riscos devem suportar ou não as necessidades do negócio? Questões desta natureza ajudam as empresas a terem um mapa geral das suas necessidades prioritárias. Já a abordagem *bottom-up* é muito mais simples porque só analisa os riscos tendo em conta o seu grau de impacto sem levar em conta aspetos importantes.

Conclui-se que o Cobit 5 tem beneficiado a SPMS na forma como diversas áreas são geridas e governadas como o planeamento estratégico, a segurança, arquitetura empresarial entre outras. E nesse caso para que a evolução da organização seja significativa na *framework* as iniciativas em andamento serão melhor trabalhadas com objetivo de obter processos claros e definidos.

Desta forma, a dissertação ajuda as organizações a terem em atenção os problemas mais críticos do seu setor e que não necessariamente devem aplicar todas regras especificadas pelo Cobit 5. Um aspeto que foi concluído por 2 entrevistados é que estas *frameworks* e os *standards* são bons na teoria mas que na prática nem sempre os resultados são compatíveis com a realidade. Portanto é necessário ter a maturidade certa para se perceber quando é que faz sentido aplicar determinada prática do Cobit.

5.1- Limitações, Estudos Futuros e Contributos para o Conhecimento

Limitações: Durante a elaboração da dissertação foram encontradas algumas limitações, pelo facto de haver pouca informação relacionada com as temáticas à governança de TI e o Cobit 5 destacando a aplicabilidade para o sector da saúde particularizando a realidade portuguesa.

Dado que o programa da SPMS encontra-se numa fase inicial, acredita-se que a organização ainda não tem um nível de maturidade suficientemente bom em termos

Cobit 5 e governação. Há ainda pouco conhecimento sobre a matéria sendo que não foi possível ter acesso em algumas respostas.

Estudos Futuros: Visto que existe pouca informação sobre a temática, académicos e investigadores podem pesquisar os variados motivos que levam as organizações da saúde a terem debilidades nas questões de governação e gestão e que facetas podem ser melhoradas com base nos vários métodos de investigação.

Organizações de setores diferentes podem investigar como os Kits de ativação podem ser úteis para o seu setor. Os programas de ativação e os controlos críticos de cibersegurança são excelentes campos de investigação para os académicos e investigadores, e o caso da SPMS é uma referência para as indústrias que futuramente tiverem projetos similares. Membros destas organizações podem por meio de inquéritos, entrevistas e outras formas metodológicas para explorar como a SPMS está aplicar os requisitos do Cobit 5 para a cibersegurança, gestão de serviço e suporte e arquitetura empresarial e definirem os seus próprios mecanismos para as suas necessidades específicas e podem consultar os manuais que o ISACA tem disponibilizado para a gestão de risco, segurança da informação e cibersegurança baseadas no Cobit 5.

Esta dissertação e os aspetos focados para estudos futuros poderão dar um excelente contributo para a comunidade académica, científica e empresarial. Para os académicos/investigadores ajuda a fomentar mais estudos relacionados a esta temática para o setor da saúde e outros setores e para os profissionais ajuda explorar como proteger-se dos ataques que impactam as suas tarefas e assim definir os princípios adequados alinhando-os com as práticas do Cobit 5, como podem ter um modelo que permita a partilha de incidentes e uma arquitetura para as necessidades dos SI no seu sector.

Referências Bibliográficas

Ahmed, H. (2017). COBIT 5 for Risk. A Powerful Tool for Risk Management GEIT, COBIT 5 Assessor, ISO 20000 LA, ISO 27001 LA, ISO 27032 Lead Cybersecurity Manager ISO 38500 Lead IT Corporate Governance Manager, Lean Six Sigma Green Belt .COBIT Focus, pp.1-4.

Carrasqueiro, S. (2017). Report on The establishment of a platform for the sharing of national eHealth strategies. Joint Action to support the eHealth Network. *Co-founder by the Health Programme of the European Union*, pp. 21.

Carrasqueiro, S. & Dias, A. (2017). Programa de Melhoria de Gestão do Serviço TI do eSIS – Ecossistema de Informação da Saúde. 14ª Conferência Anual itSMF Portugal, Tendências da Gestão de Serviço TIC no Contexto da Inovação. *Reitoria da Universidade Nova de Lisboa*.

Circular Normativa nº3/2017. Medidas Excecionais de Segurança.

Circular Normativa nº6/2017. Disponibilização do novo canal de comunicação para os profissionais de TI. Abertura do Portal Self- Service Easy Vista, 1 de Agosto de 2017.

De Haes, S. & Van Greembergem, W. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Article in* · DOI: 10.2308/isys-50422, Vol. 27, *Journal of Information Systems Spring 2013*, pp. 307–324.

Denzin, K. (1978). The Research Act, 2d ed. *New York*: McGraw-Hill, pp.28.

Despacho n.º 3156/2017 Estratégia Nacional para o Ecossistema de Informação de Saúde 2020 — ENESIS 2020. *Diário da República*, 2.ª série — N.º 74 — 13 de abril de 2017.

Despacho nº8877/2017. Modelo de Governação relativo à implementação da política de cibersegurança da saúde. *Diário da República*, 2.ª série — N.º 194 — 9 de outubro de 2017.

ENESIS. (2017). Estratégia Nacional para o Ecossistema da Informação na Saúde.

Espírito Santo, A. (2010). Segurança da Informação. Departamento de Ciência da Computação - *Instituto Cuiabano de Educação (ICE) Caixa Postal 78.065-130 – Cuiabá – MT – Brasil*, pp.5.

European Commission. (2012). Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions eHealth. Action Plan 2012-2020: *Innovative healthcare for the 21st century*, pp.3.

Gomes, R. (2015). Ecossistema Português de *Health*. Sistema de Informação de Saúde, Governança e Gestão, Instituto de Ciências Sociais e Políticas: A Gestão do Risco e Segurança.

Gomes, R. (2016a). Cibersegurança no Estado e *Ransoware* - Programas de melhoria contínua para a Gestão de Risco e Segurança.

Gomes, R. (2016b). Risk Managment and Data Protection. Serviços Partilhados do Ministério da Saúde, E.P.E. Serviço Nacional da Saúde.

Gomes, R. & Soares, B. (2016). Cybersecurity Match Supply And Demand in Portuguese HealthCare Sector – Industry Collaboration. Centeris 2016 - Conference on Enterprise Information Systems / PROJMAN 2016. International Conference on Project Management / HCIST 2016. *International Conference on Health and Social Care Information Systems and Technologies*, pp. 2-9.

ISACA *Journal*. (2011). Análise de cenários de TI em gestão de riscos corporativos. Volume 2, *EUA*, pp.1.

ISACA. (2012). Cobit 5, A Business Framework for the Governance and Management of Enterprise IT- COBIT. An ISACA Framework. *3701 Algonquin Road, Suite 1010 Rolling Meadows*, IL 60008 USA.COBIT® 5, ISBN 978-1-60420-237-3. *Printed in the United States of America*, pp. 13-31.

ISACA (2013a). Cobit 5 for Risk © 2013 ISACA. All rights reserved.

ISACA. (2013b). Cobit 5 for Risk – Cobit 5. An ISACA Framework. 3701 *Algonquin Road, Suite 1010 Rolling Meadows*, IL 60008 USA ISBN: 978-1-60420-458-2 pp. 10.

ISACA. (2013c). Transforming Cybersecurity: Using COBIT® 5. 3701 *Algonquin Road, Suite 1010 Rolling Meadows*, IL 60008 USA, ISBN: 978-1-60420-342-4, pp. 51-123.

ISACA. (2014). Trust in, and value from Information Systems. Basic Foundational Concepts Students Book: Using *COBIT® 5*. 3701 *Algonquin Road, Suite 1010 Rolling Meadows*, IL 60008 USA, pp. 28-31.

ITGI. (2003). Board Briefing on IT Governance. *3701 Algonquin Road, Suite 1010Rolling Meadows, IL 60008 USA*, 2nd Edition, ISBN 1-893209-64-4. *Printed in the United States of America*, pp.10.

(ITGI). (2007). COBIT, 4th Edition. *3701 Algonquin Road, Suite 1010 Rolling Meadows*, IL 60008 USA. *Printed in the United States of America*, pp.5.

Jick, T. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. Qualitative Methodology, Vol. 24, No.4. Published by: Jonhson Graduate School of Managment, Cornell University. Stable URL: http://www.jstor.org/stable/2392366. *Administrative Science Quartely*, pp.602.

Kaplan, B. & Maxwell, J. (2005). Qualitative Research Methods for Evaluating Computer Information Systems, p.30.

Khanyile, S. & Abdullah, H. (2012). COBIT 5: an evolutionary framework and only framework to address the governance and management of enterprise IT. *University of South Africa*, pp.3-4.

Konschak, C., Gomez, J., & Anderson, P. (2015). Cyber-Security In Healthcare - Understanding the New World Threats, *White Paper*, pp. 1.

Larsen, M., Pedersen, M., & Andersen, K. (2006). IT Governance – Reviewing 17 IT Governance Tools and Analyzing the Case of Novozymes A/S", *Proceedings of the 39th Hawaii International Conference on System Sciences* 0-7695-2507-5/06/$20.00 (C) 2006 IEEE, pp.2.

Lane, M. (2014). Enterprise Architecture and Cobit5. Disponível em https://www.orbussoftware.com/blog/enterprise-architecture-and-cobit-5/ Último acesso dia 29/10/2018.

Kozina, M. & Sekovanić, I. (2015). Using the Cobit 5 for E-health Governance. *Central European Conference on Information and Intelligent Systems Faculty of Organization and Informatics University of Zagreb Pavlinska 2, 42000 Varaždin, Croati*a, pp.205.

Kropf, R. & Scalzi, G. (2015). IT Governance and Information Governance Winter, *Journal of Healthcare Information Managment*, Volume 29 / Number 1.

Martins, H. (2017). Caminhos dos Hospitais: Os Desafios da Cibersegurança na Saúde. Serviços Partilhados do Ministério da Saúde, E.P.E. Instituto Português de Oncologia de Coimbra.

Maxwell, J.A. (1996). Qualitative Research Design: An Interactive Approach (*Sage Publications, Thousand Oaks, CA*).

Neto, M. (2010) Governança, Riscos, *Compliance*, Segurança, Forense, Resposta à Incidentes. Disponível em http://mzillo.blogspot.com/2010/09/top-down-ou-bottom-up.html . Último acesso 28/10/2018.

Niemi, E. (2006). Enterprise Architecture Benefits: Perceptions from Literature and Practice. First published in the Proceedings of the 7th IBIMA Conference Internet & Information Systems in the Digital Age, 14-16, Brescia, Italy. *University of Jyväskylä, Finland,* pp.1.

Oliver, D. & Lainhart, J. (2012). COBIT 5: Adding Value Through Effetive GEIT, Vol 46 Nº 3 .*EDPACS THE EDP Audit, Control, And Security Newsletter.*

Pasquini, A & Galiè, E. (2013). COBIT 5 and the Process Capability Model. Proceedings of FIKUSZ '13 Symposium for Young Researchers. Improvements Provided for IT Governance Process Conference Proceedings compilation © Obuda University Keleti Faculty of Business and Management. *Published by Óbuda University* http://kgk.uni-obuda.hu/fikusz, pp. 67-76.

Peterson, R. (2004). "Integration Strategies and Tactics for Information Technology Governance," Strategies for Information Technology Governance, edited by W. Van Grembergen. *Idea Group Publishing*, pp. 37-80.

Relatório da Sonda, S.A. 8 Passos para uma mitigação de riscos eficiente em TI. Disponível em https://blog.sonda.com/mitigacao-de-riscos/.Último acesso 19 de Novembro de 2018.

Ribeiro, J. & Gomes, R. (2009). IT Governance using COBIT implemented in a High Public Educational Institution – A Case Study. School of Technology and Management Polytechnic *Institute of Viana do Castelo Avenida do Atlântico, Viana do Castelo* – Portugal ISSN: 1790-5117, ISBN: 978-960-474-088-8, p.41.

Simonsson, M., Johnson, P., & Wijkström, H. (2007). Model-based IT governance maturity assessments with COBIT. Department of Industrial Information and Control Systems, KTH, *Royal Institute of Technology, Osquldas väg 12, 10044, Stockholm, Sweden*, pp.1277.

Simonsson, M. & Johnson, P. (2017). Assessment of IT Governance: A Prioritization of Cobit - KTH, Paper #151, *Royal Institute of Technology Osquldas* väg 12, 7 tr, S-100 44 Stockholm, Sweden, pp.1.

Smith, W. (1975). Strategies of Social Research: The Methodological Imagination Englewood Cliffs, NJ: *Prentice Hall*, pp.23.

SPMS. (2016a). Caracterização da Empresa. Serviços Partilhados do Ministério da Saúde, pp. 1-3.

SPMS. (2016b). Plano Setorial TIC 2020 Ministério da Saúde. *Draft* para discussão 2016, pp.19.

SPMS. (2017a). Estratégia TIC 2020. Estratégia para a Transformação Digital na Administração Pública: Plano Setorial TIC da Área Governamental da Saúde Versão 1 pp. 9,10.

SPMS. (2017b). SPMS aposta novo sistema de gestão de serviço e suporte ao utilizador. Disponível em http://spms.min-saude.pt/2017/07/. Último acesso dia 28/10/2018.

SPMS. (2017c). Concurso Público com Publicação no Joue para a Celebração de Acordo. O Quadro para a Prestação de Serviços de Cibersegurança para a área da Saúde. *Ref UAQT2017002 Caderno de Encargos SPMS*, pp. 7.

SPMS. (2017d). Relatório de Monitorização do Plano de Atividades, Investimento e Orçamento, p.11.

SPMS. (2018).Organograma Reestruturado da SPMS. Disponível em http://spms.min-saude.pt/organograma/ Acesso dia 15/11/2018.

Suomi, R. (2000). Leapfrogging for modern ICT usage in the health care sector. Paper presented at the *Proceedings of the Eighth European Conference on Information Systems, Vienna*.

Suomi, R. (2001). Streamlining operations in health care with ICT. In T. A. Spil & R. A. Stegwee (Eds.), *Strategies for Healthcare Information Systems*. Hershey, PA: *Idea Group Publishing*, pp. 31-44.

Suomi, R. & Tähkäpää, T. (2004). Governance Structures for IT in the Health Care Industry, Chapter XIV.

Tucker, G. (2014). The future of Service Managment. Disponível em https://www.itsminfo.com/category/cobit/ . Último acesso dia 28/10/2018.

University of South Africa. (2017). DSS02 – Manage service requests and incidents. Disponível em https://www.coursehero.com/file/31730424/DSS02-Manage-service-requests-and-incidentspdf/. Último acesso 28/10/2018.

Van Grembergen, W. (2002). Introduction to the minitrack IT governance and its mechanisms. University of Antwerp (UFSIA) Belgium. *Proceedings of the 35th Hawaii International Conference on System Sciences* (HICSS-35í02) IEEE, 0-7695-1435-9/02 $17.00, pp.1

Van Grembergen, W., De Haes, S. & Guldentops, E. (2004). "Structures, Processes and Relational Mechanisms for IT Governance," Strategies for Information Technology Governance, edited by W. Van Grembergen, *Idea Group Publishing*, pp. 1-37.

Van Greembergem, W. & De Haes, S. (2005). Measuring and Improving IT Governance Through the Balanced Scorecard. Information Systems Audit and Control Association, *Information Systems Control Journal*, Volume 2.

Wardle, C. (1984). The Evolution of Information Systems Architecture. AIS Electronic Library (AISeL). Metropolitan College, Boston University. *ICIS 1984 Proceedings. 4.* http://aisel.aisnet.org/icis1984/4, p.205.

Weill, P. & Ross, W. (2004). IT governance – How top performers manage IT decision rights for superior results. Harvard Business School Press. *International Journal of Electronic Government Research*, 1(4), pp.63-67.

White, S.K & Greiner, L. (2017). What is ITIL? Your Guide to the Infrastructure Library. Disponível em https://www.cio.com/article/2439501/itil/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html. Último acesso 28 /08/2018.

Yin, R. (1983). Case Study Research: Design and Methods. Second Edition, Thousand Oaks London New Deihl, Volume 5: *Sage Publications*, pp. 3.

Anexos 1: Guião de Entrevista

Caracterização dos Entrevistados		
Nome	**Código de Entrevista**	**Função/Cargo**
Rui Gomes	Diretor1	Diretor de SI da SPMS (2015-2017); Diretor de SI do Centro Hospitalar Universitário de Coimbra (2017-atualmente)
Henrique Martins	PCA	Presidente do Conselho de Administração (2013-atualmente)
Pedro Batista	Diretor3	Diretor dos SI Financeiros na SPMS (2012-2017); Diretor dos SI-Núcleo da Cibersegurança (2017-atualmente)
Alfredo Ramalho	Diretor4	Diretor dos SI na SPMS- Núcleo do eSIS

Âmbito: Esta entrevista faz parte da elaboração do meu Trabalho Final de Mestrado no Curso de Gestão de Sistemas de Informação no ISEG. O objetivo é estudar a adoção do Cobit 5 na SPMS. Uma vez que um dos principais desafios para as organizações do setor da saúde é gerir as suas infraestruturas de TI, este estudo pode ajudar as organizações a se concentrarem nos aspetos críticos e garantirem o sucesso.

Questões aos entrevistados

Parte 1: Caracterização do Projeto Cobit 5/ Objetivos Estratégicos/ Finalidade e Desafios/GSS/Arquitetura

1-Descreva sucintamente como foi o projeto de adoção do Cobit 5 na organização. **(Diretor1, PCA)**

2- Quais são os objetivos estratégicos que tinham em mente ao adotar o Cobit? **(Todos responderam)**

3- Há quanto tempo está a decorrer o projeto do Cobit 5? **(PCA)**

4- Como está constituída a equipa do projeto? **(Diretor1)**

5- Como caracteriza a entidade antes do Cobit 5 e agora? **(PCA e Diretor3**)

6- Que desafios a organização enfrentou antes de começar a adotar a *framework?* **(Diretor1, PCA)**

7- Que aspetos positivos e negativos tem verificado? **(Diretor1, PCA e Diretor3)**

8- Quais os facilitadores do Cobit 5 estão a ser mais trabalhados? **(só para o Diretor1 e Diretor3)**

9- Qual é o nível de conhecimento do Conselho de Administração tem sobre o Cobit 5 aplicado na vertente da gestão de risco e da segurança? **(só para o PCA)**

10- Qual é nível de conhecimento que a equipa de TI tem sobre o Cobit 5 aplicado na vertente da gestão do risco e da segurança e não só? **(só para o Diretor3 e Diretor4)**

11- Que suporte o Conselho de Administração tem dado para esta iniciativa? **(só para o PCA**)

12- O Modelo de Gestão de Serviço e Suporte já encontra-se em curso? **(Diretor3 e Diretor4**)

13- Consideram que a Arquitetura de Referência para o SIS já está formalizada? **(Diretor3 e Diretor4)**

Parte 2: Cenários de Risco/ Auditoria/ Legislação

1-Em qual das abordagens de cenários de risco, os cenários de risco da SPMS enquadram-se (*Top-Down ou Bottom- up*)? Porquê? **(só para o Diretor3)**

2- Já foram feitas auditorias na componente da cibersegurança? Se sim quais os resultados? **(PCA e Diretor3)**

3- Que legislações estão usar para orientar na segurança, privacidade e proteção dos dados? **(só para o Diretor3)**

Parte 3: Benefícios/Resultados/ Alinhamento e Impactos/Ações de Formação

1-Como o Cobit 5 teve impacto:

a) No Planeamento Estratégico da Organização? **(PCA)**
b) Na governação e gestão das infraestruturas de TI? **(Todos responderam)**
c) Nas perspetivas dos *stakeholders* da saúde? **(PCA e Diretor4)**

2- Como este projeto do Cobit 5 tem contribuído para uma cultura consciente? Acredita que todas as instituições do eSIS já percebem o que é o Cobit e porque está a ser adotado? (**PCA, Diretor3 e Diretor4**)

3- E como tem sido a adaptação da organização a esta mudança? (**Diretor1 e Diretor3**)

4- Uma vez que as organizações do setor da saúde ainda têm pouco conhecimento sobre as práticas de governança de TI, como nesse caso a SPMS aproveitou as boas práticas do Cobit 5 para melhorar a prestação de seus serviços? **(Diretor1 e PCA)**

5- Como o Cobit 5 tem permitido a implementação de práticas como:

a) Arquitetura Empresarial; **(Diretor3/Diretor4**)
b) Gestão de Serviço; (**Diretor3/Diretor4**)
c) Gestão da Inovação; **(Diretor3)**
d) Gestão de Fornecedores (não foi respondida)
e) Gestão da Estratégia (não foi respondida)
f) Gestão das Competências **(Diretor3/Diretor4**)

6-Que benefícios o Cobit está a trazer para os Sistemas de Informação da Saúde? **(Diretor4)**

7- Este projeto já permite mitigar as falhas de risco e corrigir as falhas de segurança? **(só para o Diretor3)**

8- Que avaliação faz do desempenho das organizações na componente da segurança? (**só para o Diretor3**)

Parte 4: Recomendações/Lições Aprendidas/ Planos e Perspetivas Futuras

1-Que recomendações a SPMS tem deixado para as organizações com características similares e diferentes as vossas? **(Diretor1, PCA, Diretor3)**

2- Quais são as lições aprendidas? **(Todos responderam)**

3- Que planos têm com o Cobit 5 dentro do próximo ano? **(Diretor3 e Diretor4)**

4- E quais para as perspetivas para o setor da saúde? **(Diretor1 e Diretor2).**

Anexo 2: Figuras e Tabelas

1.FIGURAS

Conforme o estudo de caso, o Modelo de Gestão de serviço e suporte foi desenvolvido pela SPMS para melhorar a prestação dos serviços na saúde. Este modelo foi desenvolvido com base as boas práticas do Cobit 5 e ITIL. Tem como objetivo principal criar uma estrutura que facilite o suporte técnico aos utilizadores e entidades de formas a minimizar o grau de insatisfação e melhorar a qualidade da prestação de serviços. Esta figura mostra o funcionamento do Modelo Gestão de Serviço e Suporte.

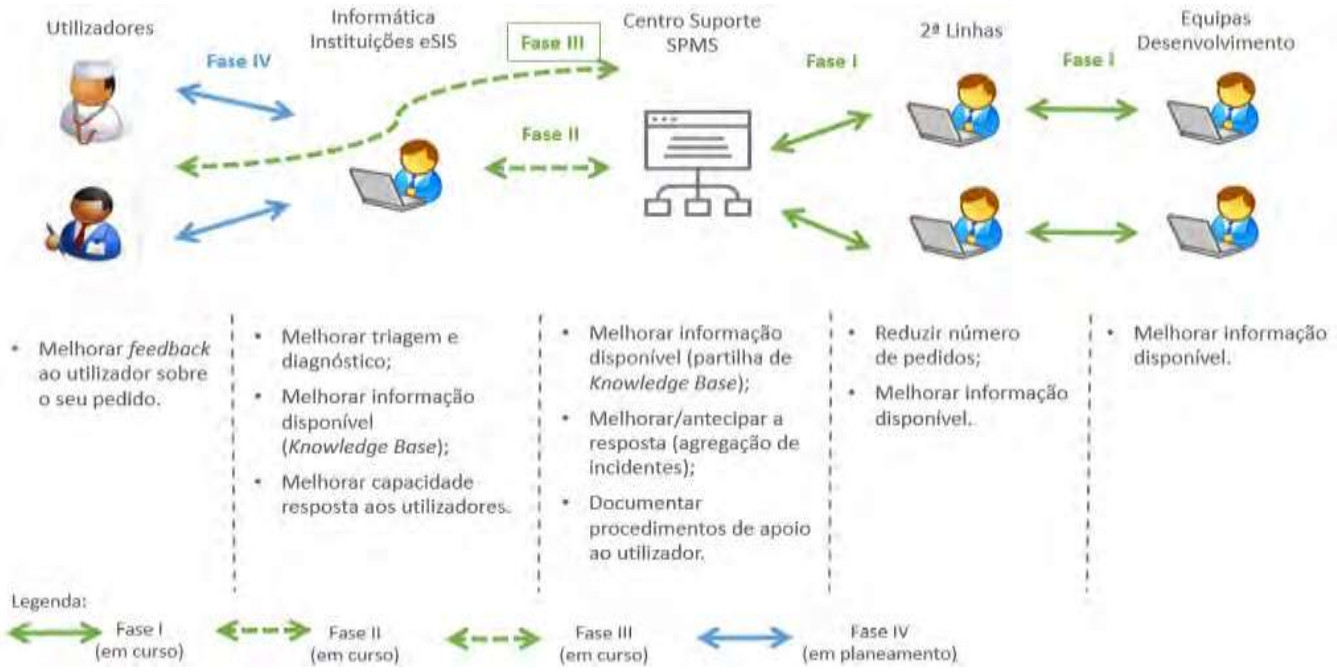

Figura 1- Modelo de Gestão de Serviço e Suporte
Fonte: Carrasqueiro & Dias, 2016

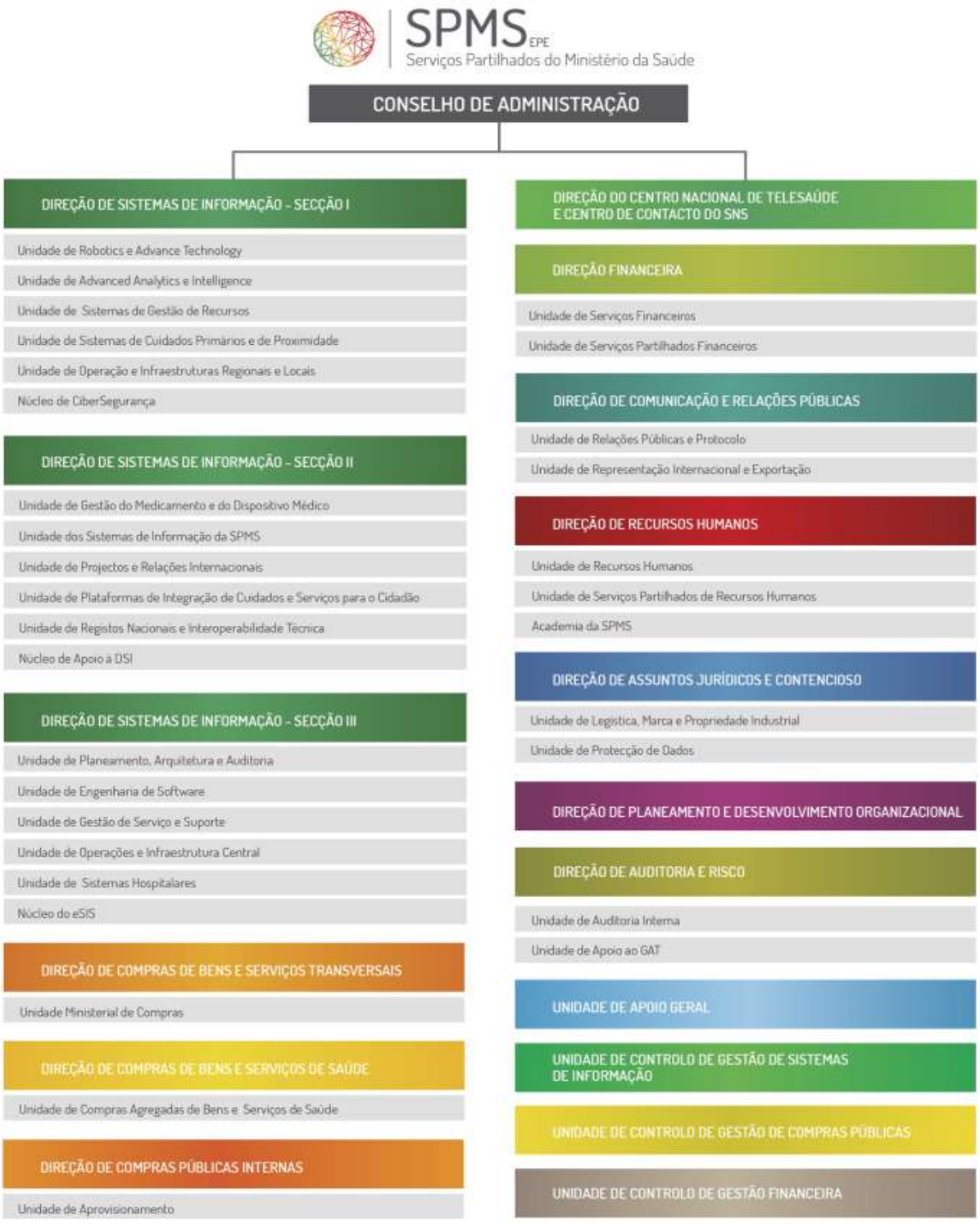

Figura 2- Organograma da SPMS. Fonte: SPMS, 2018.

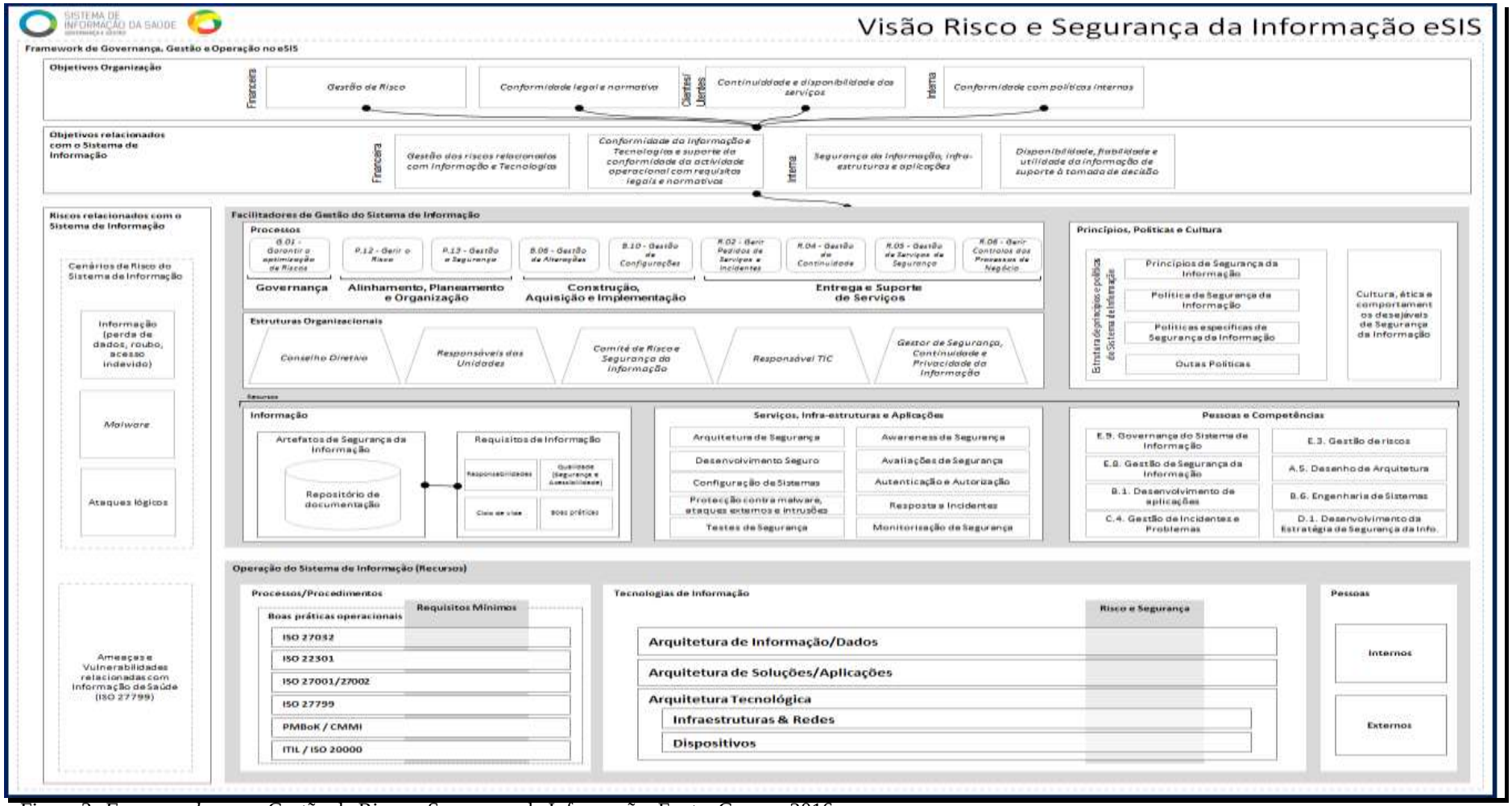

Figura 3- *Framework* para a Gestão de Risco e Segurança da Informação. Fonte: Gomes, 2016

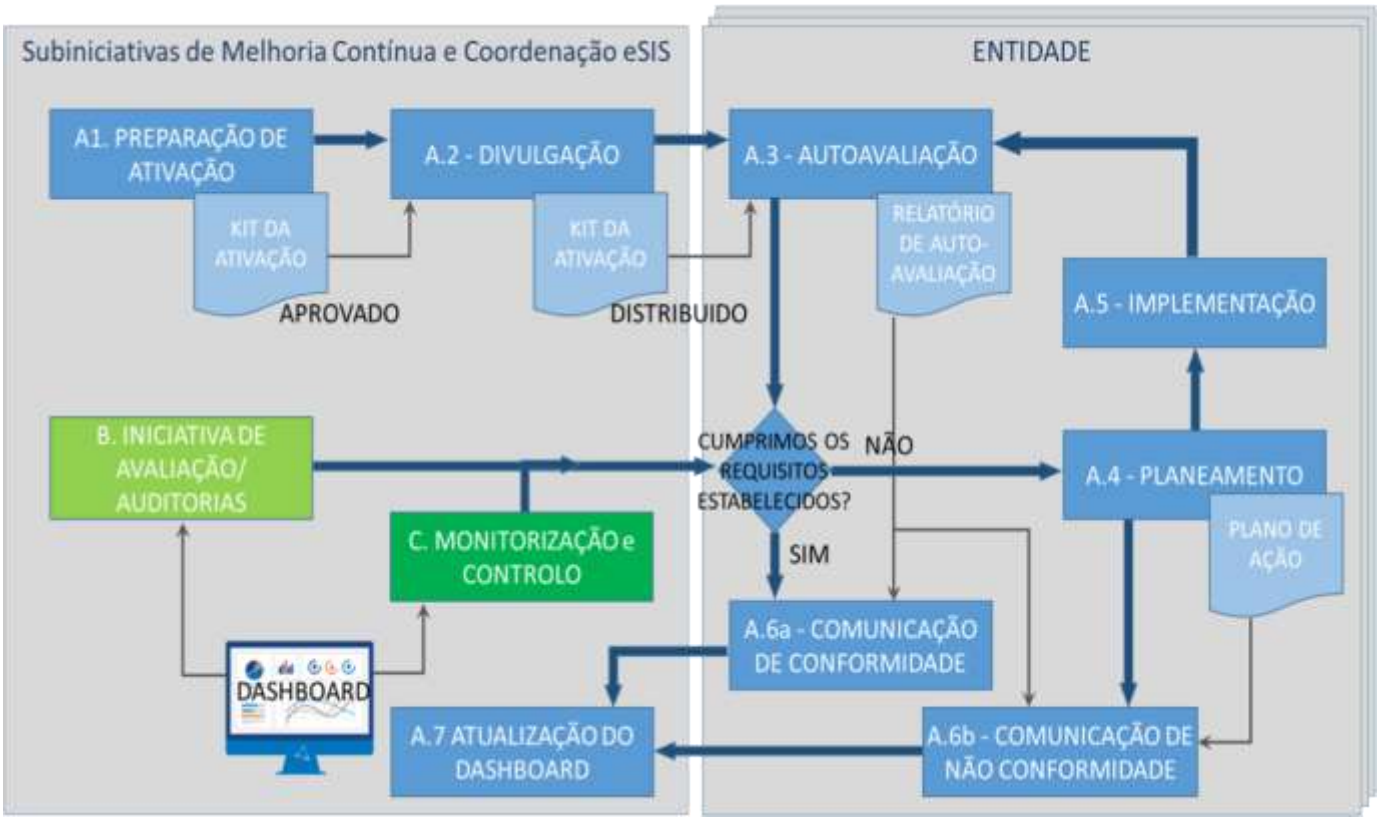

Figura 4- Programa de Ativação para a Partilha de boas práticas. Fonte: Martins, 2017.

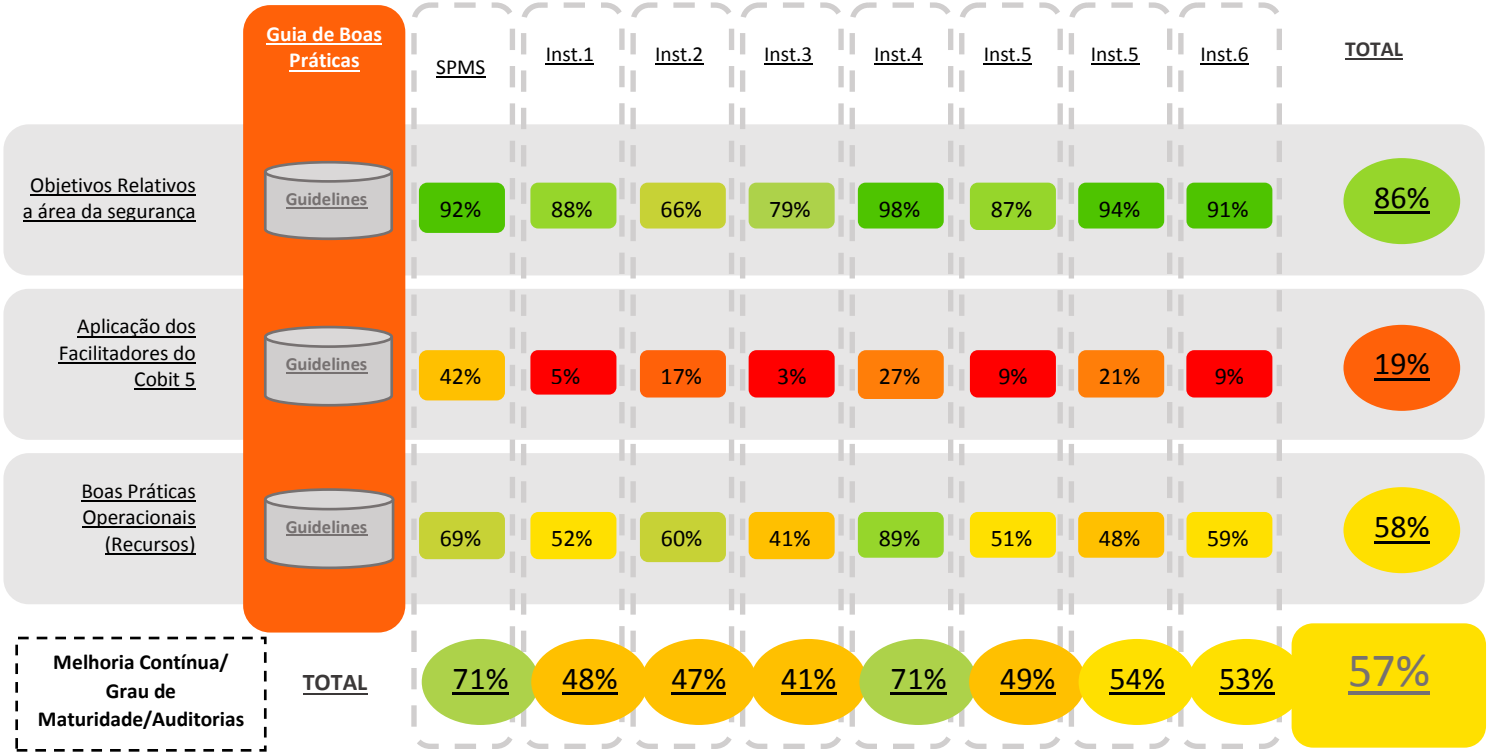

Figura 5- Ilustração dos resultados da maturidade das organizações no *dashboard*. Fonte: Gomes, 2016b. *OBS: Os dados não são reais*.

Based on "The Center for Internet Security Critical Security Controls for Effective Cyber Defense Version 6.0. SANS". Disponível em https://www.cisecurity.org/critical-controls.cfm

Controlo de Segurança Crítica # 1: Inventário de Dispositivos Autorizados e Não Autorizados	Controlo de Segurança Crítica # 2: Inventário de Software Autorizado e Não Autorizado	Controlo de segurança crítico # 3: configurações seguras para hardware e software	Controlo de Segurança Crítica # 4: Gestão Contínua de Vulnerabilidade
Controlo de Segurança Crítica # 5: Uso Controlado de Privilégios Administrativos	Controlo de Segurança Crítica # 6: Manutenção, Monitoramento e Análise de Registros de Auditoria	Controlo de Segurança Crítica # 7: Proteções de Navegador de Email e Web	Controlo de Segurança Crítica # 8: Defensas de *Malware*
Controlo de Segurança Crítica # 9: Limitação e Controlo de Portas de Rede	Controlo de Segurança Crítica # 10: Recurso de Recuperação de Dados	Controlo de segurança crítico # 11: configurações seguras para dispositivos de rede	Controlo de Segurança Crítica # 12: Defesa de Fronteira
Controlo de Segurança Crítica # 13: Proteção de Dados	Controlo de segurança crítico # 14: Acesso controlado com base na necessidade de saber	Controlo de segurança crítico # 15: Controlo de acesso sem fio	CCS eSIS#16: Account Monitoring and Control
Controlo de segurança crítico # 17: implementar programas de treinamento de cibersegurança	Controlo de Segurança Crítica # 18: Segurança do Software de Aplicação	Controlo de Segurança Crítica # 19: Resposta e Gestão de Incidentes	Controlo de segurança crítico # 20: testes de penetração e exercícios de equipa vermelha

Figura 6- Controlos Críticos de Cibersegurança. Fonte: Gomes, 2015

2. TABELAS

Tabela I- Cenários de riscos e segurança dos Sistemas de Informação na saúde.

CATEGORIA DE RISCO	CENÁRIOS DE RISCO
Informação (perda de dados, acesso indevido e roubos)	Perda parcial de informação devido a *hardware* danificado por colabores internos Difícil acesso aos dados devido ao corrompimento da base de dados Perda de dados sensíveis/confidenciais devido a existência de ataques lógicos Informação sensível/confidencial divulgada devido ao descumprimento das orientações do tratamento da informação
Malware	*Malware* existente em servidores operacionais críticos *Laptops* infetadas com *malware*
Ataques Lógicos	Utilizadores não autorizados tentam aceder aos sistemas Ataque DoS (*denial- of- service*) provoca paragem do sistema Modificação no *site* da Organização *(Defacement)* Espionagem industrial Ataques de vírus e *Hackers*

Fonte: Gomes, 2016a

Tabela II- Facilitadores Cobit 5.

Facilitadores Cobit 5 para o eSIS
1.Processos Que modelo central para os Processos de Risco e Segurança da Informação deve ser adotado no eSIS? Que processos críticos podem ser alcançados a curto prazo?
2.Estruturas Organizacionais Quais são as principais estruturas organizacionais no eSIS para sustentar o Risco e a Segurança? Qual é o nível de autoridade destas EO? **3. Cultura, Ética e Comportamentos** Que princípios culturais e éticos são aceitáveis para os Riscos e Segurança da Informação no eSIS? E para a Gestão da Mudança?

4. Princípios, Políticas e *Frameworks* Que princípios, politicas e *frameworks* orientarão o Risco e a Segurança de Informação e que todas as organizações deverão seguir?
5. Informação Quais os principais artefactos relacionados com o Risco e Segurança da Informação do eSIS?
6. Serviços, Infraestruturas e Aplicações Que serviços podem ser prestados para a segurança das componentes tecnológicas?
7. Pessoas e Competências Que competências relacionadas ao risco/segurança deverão ser adquiridos pelos quadros do eSIS?

Fonte: Gomes, 2015

Tabela III- Políticas adotadas no Sistema de Informação na Saúde

Políticas de Segurança da Informação	Políticas de Aquisição desenvolvimento, infraestruturas e aplicações
Políticas de Controlo de Acesso	Políticas e gestão de programas e projetos
Políticas de Segurança Física e Ambiental	Políticas de Gestão de Fornecedores
Políticas de Gestão de Incidentes	Políticas de Conformidade
Políticas de Continuidade do Negócio e Recuperação de Desastres	Políticas de Gestão de Recursos
Políticas Utilização e Recursos Informáticos	**Políticas de Gestão de Riscos**

Fonte: Gomes, 2015. Obs: *as políticas em negrito são as principais*.

Tabela IV- Processos do Cobit 5.

***Governança* (EDM)** ❖ **Avaliar, Direcionar e Monitorizar** Garantir a manutenção e definição da *framework* de *Governance* (EDM01) Garantir a entrega de benefícios (EDM02) **Garantir a otimização dos riscos (EDM03)** Garantir a otimização de recursos (EDM04) Garantir a transparência para os *stakeholders* (EDM05)
Gestão ❖ **Alinhar, Planear e Organizar (APO)** Gerir a *Framework* de Gestão de TI (APO01) Gerir a Estratégia (APO02) Gerir a Arquitetura Empresarial (APO03) Gerir a Inovação (APO04) Gerir o Portfolio (APO05) Gerir Orçamentos e Custos (APO06) Gerir os Recursos Humanos (APO07) Gerir as Relações (APO08) Gerir Acordos de Serviços (APO09) Gerir Fornecedores (APO10) Gerir a Qualidade (APO11) **Gerir o Risco (APO12)** **Gerir a Segurança (APO13)**
❖ **Construir, Adquirir e Implementar (BAI)** Gerir Programas e Projetos (BAI01) Gerir as Alterações(BAI06)

Gerir a Definição de Requisitos (BAI02) Gerir a Aceitação e Passagem de Alterações (BAI07) Gerir a Identificação e Construção de Soluções (BAI03) Gerir Conhecimento (BAI08) Gerir a Capacidade e Disponibilidade (BAI04) Gerir Recursos (BAI09) Gerir a Mudança Organizacional (BAI05) **Gerir Configurações (BAI10)**
❖ **Entregar, Servir e Suportar (DSS)** Gerir Operações (DSS01) Gerir Controlos de Processos de Negócios (DSS06) Gerir Pedidos de Serviços e Incidentes (DSS02) Gerir Problemas (DSS03) **Gerir a Continuidade (DSS04)** **Gerir Serviços de Segurança(DSS05)** ❖ **Monitorizar, Analisar e Avaliar (MEA)** Monitorizar, Avaliar e Analisar a Performance e Conformidade(MEA01) Monitorizar, Avaliar e Analisar o Sistema de Controlo Interno(MEA02) Monitorizar, Avaliar e Analisar a Conformidade com os Requisitos Legais (MEA03)

Fonte: Gomes, 2015

Tabela V- Comité de Segurança- Mandato, Princípios Operacionais e Níveis de Autoridade

Área	Descrição
Mandato	O Comité de segurança certifica-se que as boas práticas de segurança são aplicadas de forma eficiente em toda a SPMS, definindo o nível de aceitação do risco de segurança da informação
Princípios Operacionais	Realizar reuniões frequentes durante o desenvolvimento de novas iniciativas ou para situações urgentes Garante a comunicação a um número limitado de pessoas facilitando as tomadas de decisão Em cada reunião produzem-se atas As reuniões do Comité de Segurança podem ser presididas por um Membro do Conselho de Administração
Poder/Autoridade	O Comité de Segurança da Informação é responsável por tomar decisões associadas a segurança da informação
Direitos de Delegação	Não pode delegar papéis noutras áreas uma vez que é o responsável pela estratégia da Segurança da Informação
Escalada	Um Membro do Conselho de Administração pode tomar decisões em assuntos em que não haja consenso no Comité

Fonte: Gomes, 2015

Tabela VI- Coordenador de Segurança- Mandato, Princípios Operacionais e Níveis de Autoridade

Área	Descrição
Mandato	Responsável pelas operações de segurança da Informação da SPMS
Princípios Operacionais	Alinha o programa da segurança com a gestão executiva e deve interagir com os stakeholders com objetivo de suprir as suas necessidades de proteção dos dados • Deve ter uma visão estratégica e completa do negócio; • Ser um bom comunicador; • Deve ter um bom relacionamento com os vários dirigentes da organização; • Deve ser capaz de traduzir as necessidades do negócio em objetivos de segurança da informação.
Nível de Poder/Autoridade	Tem a responsabilidade de: • Executar a estratégia de segurança da informação; • Implementar o programa de segurança da informação; • Definir um plano de gestão de risco e segurança de informação; • Aprovação das políticas de segurança da informação; • Fazer a gestão da equipa de gestão de segurança da informação; • Otimização dos recursos de segurança da informação.

Direitos de Delegação	O Coordenador da Segurança da Informação deve distribuir tarefas para outros gestores de segurança da informação de acordo com a sua área de atuação
Escalada	Toda a informação importante relacionada ao risco e segurança deve ser escalada para o Comité de Segurança da Informação

Fonte: Gomes, 2015

Tabela VII - Boas Práticas para Cultura e Ética Comportamental

Modelo de Referência para Cultura, Ética e Comportamental na SPMS
Comportamentos Desejados ❖ **Foco na Criação de Valor** Satisfação das Necessidades **Otimização de Riscos** Otimização de Recursos ❖ **Compromisso com os Princípios e Normas de eSIS** ❖ **Partilha de Boas Práticas de Gestão e Operação** **Boas Práticas para fomentar/reforçar os comportamentos de desejados no eSIS** ❖ Comunicação e ética dos comportamentos desejáveis do eSIS ❖ Prover incentivos e penalidades relacionadas aos descumprimentos destas práticas ❖ Consciencialização para a promoção de ética e comportamentos desejáveis no eSIS ❖ Normas e regras do eSIS

Fonte: Gomes, 2015

Tabela VIII- Artefactos da Informação no contexto da Segurança e Risco

Riscos	***Segurança***
Perfil de Risco do eSIS	Estratégia de Segurança do eSIS
Plano de Comunicação de Riscos do eSIS	Orçamento de Segurança do eSIS
Relatório de Risco do eSIS	Programa de Segurança do eSIS
Programa de Consciencialização de Riscos	Políticas, normas e procedimentos de Segurança do SIS
Mapa de Riscos	Requisitos de Segurança do eSIS (ex.: Configurações, Desenvolvimentos, contratos)
Indicadores Chaves de Riscos do eSIS	Material de Consciencialização
Taxonomia de Riscos	Relatórios de Segurança (ex. Auditoria, Incidentes, riscos, ameaças, vulnerabilidades).
Relatório de *Business Impact Analisys*	
Matriz de Risco e Controlo de eSIS	
Relatórios de avaliação de risco	

Fonte: Gomes, 2015

Tabela IX- Artefactos de Serviços, Infraestruturas e aplicações no contexto da Segurança e Risco.

Riscos	***Segurança***
Assessoria de risco em programas/projetos	Arquitetura de Segurança
Gestão de Incidentes	*Awareness* de Segurança, Desenvolvimento Seguro
Assessoria de risco em arquitetura empresarial	Avaliações de Segurança
Risk Intelligence	Implementação e configuração de sistemas em conformidade com as normas e boas práticas
Gestão de Riscos	Proteção contra *malware*, ataques externos e tentativas de intrusão ; Resposta a incidentes, testes e revisões de qualidade
Gestão de Crises	Monitorização e alerta de incidentes de segurança

Fonte: Gomes, 2015