Práticas de Segurança da Informação num Centro Hospitalar

Sabina Mota Santos [1], Luís Silva Rodrigues [2], Domingos Silva Pereira[3].

1) ISCAP/IPP, Portugal
sabina.mota.santos@gmail.com

2) ISCAP/IPP, Portugal
lsr@iscap.ipp.pt

3) Portugal
dmspdlf@gmail.com

Resumo

As Tecnologias e Sistemas de Informação (TSI) estão presentes em vários domínios da rede organizacional do mundo inteiro, sendo o desenvolvimento de um bom sistema de gestão da informação crucial para o funcionamento de qualquer organização. É, portanto, necessário garantir que a informação está protegida e que o sistema de informação está em conformidade com o conjunto de normas da área de segurança da informação seguido pela organização. Este artigo pretende elaborar uma avaliação do sistema de gestão em termos de segurança da informação de um centro hospitalar, seguindo os requisitos e recomendações de um *framework* utilizado a nível mundial na área de auditoria de sistemas de informação.

Palavras chave: Segurança da Informação, ISO27001, ITIL, COBIT

1. Introdução

Na era em que nos encontramos, o poder da informação adquiriu um papel muito importante no mundo organizacional. Todas as organizações lidam com informação respeitante ao negócio, aos seus colaboradores, parceiros, utilizadores, etc., e precisam de garantir que a mesma é fidedigna e está protegida para que possam usá-la como base no seu negócio.

Nos últimos anos, tem-se assistido a um desenvolvimento nas normas que visam apoiar as organizações na implementação de um sistema de gestão de segurança da informação. Esta necessidade surge num cenário em que as organizações têm que estar constantemente a melhorar a sua forma de gerir e governar para conseguir dar resposta às novas tendências em tecnologia e às necessidades que vão surgindo nas organizações.

Para apoiar no processo de gestão da segurança da informação existem várias normas, sendo que os três mais utilizados a nível mundial são a ISO27001 (Norma internacional que apresenta

os requisitos para um sistema de gestão da segurança da informação), a ITIL (*Information Technology Infrastructure Library*) e o COBIT (*Control Objectives for Information and related Technology*). O facto de apresentarem requisitos ou recomendações que visam ajudar na gestão da segurança da informação, permite às organizações implementar métodos, princípios, políticas, entre outros, que já se encontram descritos e compreendidos, e surgem tendo por base um estudo do universo organizacional ao longo dos últimos anos.

Quando uma dessas organizações se trata de um hospital público, os dados adquiridos diariamente estão diretamente ligados à saúde e bem-estar dos seus utentes. Este tipo de informação apresenta um teor confidencial e uma importância vital, que torna necessário gerir e proteger essa informação, de modo a garantir que o tratamento prestado ao utente não é posto em causa devido a um mau funcionamento dos sistemas de informação em vigor na organização.

2. Segurança da Informação

Segurança trata-se de garantir a proteção contra adversidades, quer estas aconteçam de forma intencional ou não. Segurança da informação estabelece que o foco dessa proteção se encontra na informação e nos seus elementos mais críticos, tais como os seus sistemas e *hardware* que usam, armazenam e processam essa mesma informação [Whitman and Mattord 2008].

O ISACA (*Information Systems Audit and Control Association*) define segurança da informação como algo que "*garante, dentro da organização, que a informação é protegida da divulgação a utilizadores não autorizados (confidencialidade), das modificações inapropriadas (integridade) e da ausência de acesso quando requerido (disponibilidade)*" [ISACA 2012].

Essa proteção e prevenção dos SI têm em vista garantir os elementos básicos da informação [NIST 2002]: Confidencialidade – só as partes autorizadas é que têm acesso à informação, e esse acesso está sujeito à definição da forma como acedem e à definição do período de tempo em que o mesmo é válido. É importante proteger a informação privada tanto do pessoal como da entidade; Integridade – evitar a modificação ou a destruição imprópria da informação, garantindo que estes atos só são efetuados pelas pessoas autorizadas, por forma a garantir a autenticidade da informação; e Disponibilidade – O acesso e o uso da informação deve ser atempado e de confiança.

Um dos fatores mais importantes na proteção da informação e seus elementos básicos, reside na determinação e constituição de boas bases para uma gestão eficaz da segurança da informação [ISACA 2010]. Essa gestão está concentrada na prática de reunir, monitorizar e analisar dados relacionados com a segurança da informação, enfatizando estratégias de monitorização contínua

ou de avaliações independentes de controlos de segurança, com o intuito de medir a eficácia que os controlos implementados e mantidos pelas organizações têm [Gantz 2014, Rouse 2009].

Um Sistema de Gestão de Segurança da Informação (SGSI) irá ajudar na especificação de quais os instrumentos e quais os métodos que a gestão deve utilizar no seu exercício, conseguindo dessa forma planear, adotar, implementar, supervisionar e melhorar as tarefas e atividades que visam alcançar a segurança da informação [BSI 2008]. A projeção e implementação do SGSI segue uma abordagem de processo e deve ter em atenção as necessidades e objetivos da organização, o seu tamanho e estrutura, os seus requisitos de segurança e os processos que se encontram em funcionamento na mesma [Kouns and Kouns 2011]. Com o apoio do SGSI, todas as pessoas envolvidas no uso e gestão da informação da organização poderão compreender a um nível aceitável as políticas, normas, procedimentos ou outros requisitos de segurança da informação que sejam aplicados dentro da organização [Wright 2005]. Consegue-se desta forma garantir a confidencialidade, integridade e disponibilidade da informação [Cannon 2008].

3. Normas para a Segurança da Informação nas TSI

Quando se trata de realizar a gestão da segurança da informação, as organizações começaram a perceber que era preferível implementar um conjunto de normas ou procedimentos que fossem reconhecidos internacionalmente, do que desenvolverem por si só normas ou procedimentos que se aplicassem exclusivamente à sua própria organização [Solms 2005].

No âmbito de segurança da informação, existem diversas opções tais como: normas da série ISO27000 - família de normas que ajuda as organizações a manter os ativos de informação seguros; lei SOX (*Sarbanes-Oxley*); COBIT; COSO (*Committee of Sponsoring Organizations of the Treadway Commission*); ITIL; etc [Arora 2010]. Estas definem os principais conceitos, princípios e componentes de gestão de segurança da informação, e oferecem importantes referências às organizações para a aplicação apropriada dessa mesma gestão [Kajava et al. 2006]. Constata-se que as normas mais evidenciadas para uma boa implementação da gestão da segurança da informação numa organização são a ISO27001, a ITIL e o COBIT [Susanto et al. 2011, Turner et al. 2008]

3.1 ISO27001

A ISO27001 foi publicada inicialmente em Outubro de 2005 pela ISO (*International Organization for Standardization*) e pela IEC (*International Electrotechnical Commission*) sendo uma das normas da série ISO27000, a qual junta um conjunto de normas focado na gestão dos SGSI [FFIEC 2006; Pelnekar 2011]. A sua versão mais recente data a 2013 e visa

providenciar requisitos para estabelecer, implementar, manter e melhorar de forma continuada um SGSI [ISO 2013]. No entanto, os requisitos apresentados descrevem qual o comportamento esperado para um SGSI, depois de este estar completamente operacional, não se tratando de uma norma que enumera passo a passo a definição e construção de um SGSI [BSIgroup 2014]. Segundo esta norma, um SGSI está planeado para preservar a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão de risco, e para garantir a confiança às partes interessadas da organização de que os riscos estão a ser devidamente geridos [ISO 2013].

A ISO27001 prevê que os objetivos de controlo e os controlos sejam diretamente derivados da ISO27002 (Norma internacional que apresenta o código de boas práticas para os controlos de segurança da informação), na qual se encontram 114 controlos de segurança [BSIgroup 2014]. É também referido que, ao contrário da versão anterior, o modelo Plan-Do-Check-Act (PDCA) não é o modelo base e que outras metodologias poderão ser utilizadas pelas organizações para a estruturação dos processos do SGSI, uma vez que um dos requisitos é a melhoria contínua e o modelo PDCA é só uma das diferentes abordagens que permitem atingir esse fim [BSIgroup 2014]

A ISO faz ainda alusão à necessidade de cumprir os requisitos especificados nas secções da ISO27001, para que seja verdade que a organização se encontra em conformidade com esta norma internacional [ISO 2013]. Esta certificação potencia a forma como é visto o compromisso das empresas em cumprir com as obrigações perante clientes e parceiros. O crescente interesse na certificação ISO27001 deve-se à proliferação de ameaças à informação e ao aumento das exigências regulatórias e legais que se relacionam com a proteção da informação. O facto de esta ter sido construída com a garantia de compatibilidade com outras normas de gestão, tais como a ISO9001 (norma internacional que apresenta critérios para um sistema de gestão da qualidade adequado), a ISO14001 (norma internacional que apresenta critérios para um sistema de gestão ambiental adequado) e a série ISO20000 (família de normas internacionais que tratam sistemas de gestão de serviços), ajuda bastante no aumento do interesse em obter esta certificação por parte das empresas [Calder 2013].

Ao implementar a ISO27001, as organizações podem usar esta norma como um referencial quando se trata da comparação com os seus concorrentes, para além de permitir providenciar informação relevante sobre a segurança de TSI a fornecedores e a clientes. Esta norma pode contribuir para aumentar a consciência de segurança entre a comunidade da organização e incentivará o alinhamento entre o negócio e as tecnologias de informação. Fornece uma estrutura processual para a implementação de segurança de TSI, o que permite determinar o

estado da segurança da informação e o grau de cumprimento das políticas, diretrizes e normas de segurança, ajudando na promoção de uma gestão de custos de segurança eficiente e na conformidade com leis e regulamentos [Pelnekar 2011].

Resumidamente, a ISO27001, como norma internacional de segurança da informação, que requer o cumprimento de requisitos para a obtenção da certificação, apresenta cláusulas e controlos de segurança específicos que dever-se-ão pôr em prática na organização aquando a definição, implementação, manutenção e melhoria contínua de um SGSI.

3.2 ITIL

Publicado entre 1989 e 1995 pela CCTA (*Central Computer and Telecommunications Agency*) [ITGI 2005], fornece orientações aos prestadores de serviços de TSI, garantindo que o valor do negócio seja protegido [Meijer et al. 2011]. A sua última versão de 2007 sofreu pequenas melhorias no ano de 2011, e concentra-se em cinco secções fundamentais do ciclo de vida de um serviço (figura 1). Este ciclo de vida parte da definição e análise dos requisitos do negócio nas fases de estratégia e de conceção de serviço (*Service Strategy e Service Design*), dando atenção também ao ambiente da organização na fase da transição do serviço (*Service Transition*), e visando o funcionamento e a melhoria nas fases de operação do serviço e melhoria continuada do serviço (*Service Operation e Continual Service Improvement*) [Cartlidge et al. 2007].

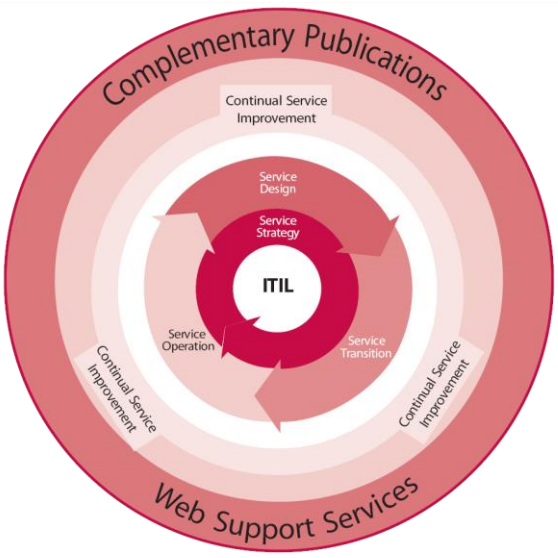

Figura 1 – Ciclo de Vida de um Serviço - ITIL versão 3 [TSO 2007]

Mais detalhadamente, nessas cinco etapas, o *framework* explicita como: determinar requisitos e quais os serviços TSI que devem ser providenciados - Estratégia do Serviço; projetar, criar ou alterar os serviços e os processos de gestão dos serviços por forma a atingir os requisitos do negócio - Conceção do Serviço; validar a utilidade e o fundamento dos serviços e tratar da transição dos mesmos para a vida real - Transição do Serviço; providenciar os serviços e garantir um apoio eficaz e eficiente - Operação do Serviço; e garantir que os serviços tratam de forma continuada as necessidades futuras - Melhoria Contínua do Serviço. Dentro de cada etapa existem processos que suportam as diferentes fases enumeradas. Juntamente aos processos, estão definidas funções, responsabilidades e atividades que se traduzem em recursos, que por sua vez serão utilizados para fornecer uma estrutura às diferentes etapas do ciclo de vida do serviço [Meijer et al. 2011].

Os tópicos relacionados com a gestão da segurança da informação vão sendo discutidos ao longo do ciclo de vida do serviço, nas cinco diferentes publicações da ITIL, tendo uma maior referência na publicação da Conceção do Serviço (Service Design), na sua secção 4.6 [Clinch 2009]. A ITIL prevê um processo de gestão da segurança da informação (ISM – *information security management*) que, por definição, garante a confidencialidade, integridade e disponibilidade dos ativos, dados e informação de uma organização. Foca-se em aumentar a consciencialização dos riscos e problemas de segurança e a forma como estes são tidos em conta, por forma a garantir o sucesso em cada passo dado na gestão dos serviços de TSI [Clinch 2009]. O processo de gestão de segurança é usado para a implementação da segurança da informação dentro de uma organização e tem como objetivo alinhar a segurança de TSI com a segurança do negócio no geral, e garantir que a segurança da informação está a ser gerida de forma eficaz em todos os serviços e em todas as atividades de gestão de serviços de TSI [Sheikhpour and Modiri 2012].

Ao referir-se ao SGSI, o *framework* refere a necessidade do envolvimento dos 4P's - Pessoas, Processos, Produtos e Parceiros - para que o programa de segurança da informação suporte os objetivos da organização. O SGSI apresentado, baseia-se na ISO27001, e está estruturado em 5 elementos base: Controlo, Planeamento, Implementação, Avaliação e Manutenção. Cada um destes elementos do SGSI tem objetivos a atingir. Com o elemento controlo pretende-se estabelecer uma estrutura de gestão para definir e gerir a segurança da informação da organização, e uma estrutura de organização que permita preparar, aprovar e implementar a política de segurança da informação. Pretende-se também alocar responsabilidades e estabelecer e documentar os diferentes controlos. Através do planeamento, a organização conseguirá desenvolver e recomendar medidas de segurança adequadas, tendo por base os diferentes requisitos da organização. Em termos de implementação, assegura-se que os procedimentos,

ferramentas e controlos apropriados estão disponíveis e sustentam a política de segurança da informação. Relativamente à avaliação, prevê-se que seja efetuada uma supervisão e verificação do cumprimento da política de segurança, e que sejam realizadas auditorias regulares à segurança dos sistemas de TSI. Por fim, referente ao elemento manutenção, a ITIL apresenta como objetivos a melhoria dos acordos de segurança especificados, e da implementação de medidas e controlos de segurança [ITGI 2005].

Apurou-se, então, que a ITIL apresenta um processo focado na estruturação de um SGSI adequado, que tem como elementos base o controlo, o planeamento, a implementação, a avaliação e a manutenção da segurança da informação, e que envolve pessoas, processos, produtos e parceiros, assegurando que a gestão da segurança da informação está a ser executada em todos os serviços e em todas as atividades de gestão de serviços.

3.3 COBIT

O ISACA, juntamente com o ITGI (IT Governance Institute), publicou em 1996, a primeira versão do COBIT [Susanto et al. 2011]. Atualmente, o COBIT tem como principal objetivo ser um *framework* de controlo que apoia as organizações a garantirem o alinhamento do uso de TSI com os objetivos de negócio, tendo os seus processos orientados para responder às necessidades do negócio [Ridley et al. 2004].

O COBIT apresenta 5 princípios básicos: atender às necessidades das partes interessadas; cobrir a empresa de ponta a ponta; aplicar um único *framework* integrado; possibilitar uma abordagem holística; e diferenciar governança e gestão. A orientação e especificação dos princípios são feitas de forma detalhada através de facilitadores de governança e gestão da parte TSI da organização. Esses facilitadores estão divididos por 7 categorias: políticas, princípios e *frameworks*; processos; estrutura organizacional; cultura, ética e comportamentos; informação; serviços, infraestruturas e aplicações; e pessoas, e suas habilidades e competências. Estes foram definidos com o intuito de apoiar a implementação dos sistemas de governança e gestão de TSI, tendo em vista o alcance dos objetivos da organização.

Para além dos 5 princípios e dos 7 facilitadores, o COBIT apresenta um conjunto de 37 processos (figura 2). Cinco desses processos estão associados ao domínio avaliar, dirigir e monitorizar (EDM - *Evaluate, Direct and Monitor*) da área de governança. Os restantes estão adjacentes à área de gestão e dividem-se pelos domínios alinhar, planear e organizar (APO - *Align, Plan and Organize*), construir, adquirir e implementar (BAI - *Build, Acquire and*

Implement), entrega, serviço e suporte (DSS - *Deliver, Service and Support*) e monitorizar, avaliar e aferir (MEA - *Monitor, Evaluate and Assess*) [ISACA 2012].

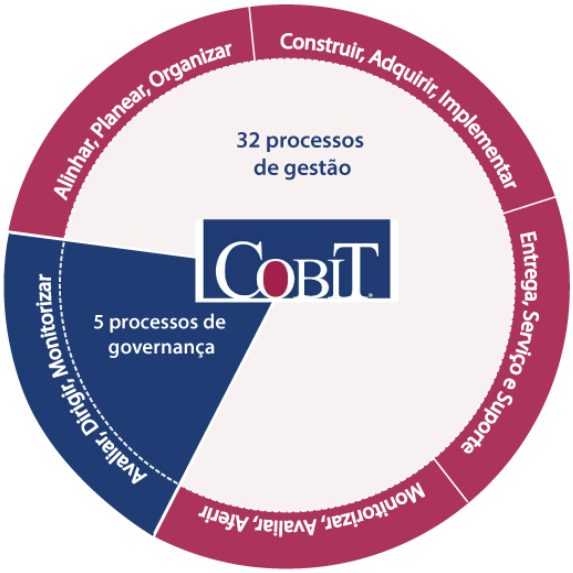

Figura 2 – Domínios e processos do COBIT entre as áreas de governança e gestão [ISACA 2012]

Trata-se de uma boa solução em circunstâncias onde os gestores procuram uma estrutura que apresente uma solução integrada por si só, sem que haja necessidade de implementar juntamente outros *frameworks* de governança de TSI [Arora 2010], pois, perante a existência de várias normas e boas práticas relacionadas com TSI, o COBIT apresenta na sua documentação um alinhamento com outras normas e estruturas, sendo, então, possível ser utilizado como um *framework* de referência para a governança e gestão de TSI [ISACA 2012].

Numa perspetiva de segurança da informação, o COBIT apresenta uma publicação mais focada nesta área, o COBIT 5 para a Segurança da Informação (COBIT5SI) no qual apresenta de forma mais detalhada a aplicação dos diferentes facilitadores na área de segurança. Esta publicação segue os mesmos princípios do COBIT já referidos anteriormente, e descreve como os facilitadores podem ser postos em prática de forma a implementar uma governança e gestão de segurança da informação eficaz e eficiente.

Para tal, apresenta no facilitador Políticas, Princípios e F*rameworks* de segurança da informação sugestões de mecanismos de comunicação utilizados para transmitir as instruções da direção e dos órgãos sociais à restante organização no que respeita a segurança da informação. Os princípios de segurança comunicam as regras a seguir dentro da empresa que servem de apoio ao alcance dos objetivos de governança definidos pelo conselho de administração e pela gestão

executiva. Esses princípios estão divididos em três módulos: suporte ao negócio; defesa do negócio; e promoção de um comportamento de responsabilidade de segurança da informação. As políticas, por sua vez, fornecem orientações mais detalhadas relativamente à forma como se deve pôr em prática os princípios seguidos pela organização. O COBIT5SI sugere a existência de políticas no âmbito das funções de segurança da informação e das restantes funções existentes na organização.

No que se refere ao facilitador Processos, o COBIT5SI descreve um conjunto de práticas e atividades para atingir os objetivos da organização. Esse conjunto é constituído pelos 37 processos já referidos anteriormente, sendo que dois deles, no âmbito geral do COBIT, estão associados à segurança da informação: APO13 Gestão da Segurança (no domínio alinhar, planear e organizar, APO - *Align, Plan and Organize*), e DSS05 Gestão de Serviços de Segurança (no domínio entrega, serviço e suporte, DSS - *Deliver, Service and Support*). No âmbito da publicação COBIT5SI, é apresentada informação específica de segurança relacionada com os todos os processos, tanto os de governança e como os de gestão apresentados no COBIT.

No que toca ao facilitador Estrutura Organizacional, é de referir que as estruturas organizacionais são consideradas as entidades chave para a tomada de decisão dentro da organização. Este facilitador apresenta um conjunto de funções diretamente relacionadas com segurança da informação e pretende que seja executado um conjunto de práticas associadas a cada uma delas, que ofereçam como resultado à organização a tomada de boas decisões.

Na área de Cultura, Ética e Comportamento, o ISACA [ISACA 2012] prende a sua atenção no ciclo de vida cultural, na liderança, assim como no ambiente desejado. Este facilitador visa que os comportamentos devem ser medidos ao longo do tempo para se conseguir, desta forma, aferir a cultura de segurança na organização. Pode-se também encontrar uma lista de comportamentos sugeridos que influenciam positivamente a cultura de segurança da informação.

No COBIT5SI, são analisados também os diferentes tipos de informação considerados relevantes para que a segurança seja garantida, e é aconselhada a realização de uma avaliação da relação entre os diferentes tipos de informação e os *stakeholders*, por forma a perceber quais os colaboradores dentro da organização que originam, aprovam, são informados ou utilizam determinada informação. Para além disso, o COBIT5SI identifica uma lista de serviços relacionados com a segurança que têm um grande potencial de aparecer num catálogo de serviços de segurança e apresenta sugestões de competências que devem ser cobertas pelos colaborados da organização. Desta forma, aborda os restantes facilitadores do COBIT: Informação; Serviços, Infraestruturas e Aplicações; e Pessoas, *Skills* e Competências.

Conclui-se que, juntamente com a sua publicação COBIT5SI, o COBIT apresenta os processos, estrutura organizacional, políticas e informação de TSI, entre outros, que irão permitir uma adequada gestão e governança da segurança da informação, que estejam alinhadas com os objetivos de negócio da organização.

4. Objetivo e Abordagem de Investigação

O principal objetivo passou por analisar uma organização cuja atividade se relacionasse com a área de saúde, relativamente à sua área de segurança da informação, apostando numa avaliação ao sistema de gestão e não tanto numa avaliação mais técnica. Pretendeu-se perceber se numa organização, onde a informação existente está muitas vezes relacionada com assuntos confidenciais dos seus utentes, existem preocupações e processos que garantam que essa mesma informação se encontra protegida e gerida da melhor forma possível. Assim, e após a escolha de uma norma para utilizar como base na estruturação da análise referida, preparou-se a realização de uma comparação entre as orientações providenciadas por essa norma e aquilo que se punha em prática na organização em análise, sendo que esta última informação seria adquirida através do contacto com um colaborador, pertencente à organização em estudo, que fosse de interesse para a área.

Para tal, começou-se por desenvolver-se uma pesquisa que nos indicasse quais as normas que as organizações mais implementavam em termos de segurança da informação. Após identificar-se três normas e desenvolver-se uma análise comparativa entre as três, optou-se pela utilização do COBIT.

Esta opção baseia-se na revisão da literatura efetuada. Tendo por base uma perspetiva de utilização das normas e boas práticas referias dentro de uma organização, Arora [Arora 2010] ao realizar uma comparação entre o COBIT e a ISO27001, afirma que o COBIT apresenta uma solução de gestão de segurança de informação completa ao contrário do que acontece com a norma ISO27001, pois o COBIT apresenta uma boa solução para combinar não só a área de gestão de SGSI mas também a de governança de TSI. Por sua vez, Stroud [Stroud 2010] compara os *frameworks* ITIL e COBIT, e afirma que o COBIT é um *framework* de governança de TSI que nos apresenta o que deve ser feito para garantir uma governança adequada dos processos de TSI, incluindo os de gestão de serviços, e que a ITIL complementa o COBIT apresentando a forma como devem ser planeados, projetados e implementados recursos de gestão de serviços de TSI eficazes. Greenfield [Greenfield 2007] resume a aplicação desta norma e destes *frameworks* referindo que o COBIT diz-nos o que monitorizar e controlar, sendo que a ITIL descreve como proceder para implementar os processos que permitem atingir essa

monitorização e controlo. A ISO27001, por sua vez, estabelece processos que asseguram esses objetivos e que garantem o alinhamento com requisitos legais.

Optou-se, portanto, pelo *framework* COBIT, por este apresentar uma visão mais ampla da gestão e governança da organização, realizando um conexão com as diferentes áreas e a segurança da informação, e mantendo um alinhamento não só com os objetivos do negócio da organização, mas também com as outras duas normas analisadas. No entanto, devido à extensão que o COBIT apresenta, reduziu-se o campo de análise a quatro dos facilitadores enunciados na secção 3.3: Processos; Princípios, Políticas e Frameworks; Estrutura Organizacional; e Informação.

O facilitador Processos foi um dos que se considerou na comparação realizada entre a norma e organização, e a base desta análise prende-se na necessidade de obter uma perceção relativa à implementação dos processos, pois estes permitem a obtenção dos objetivos traçados pela organização. Porém, na revisão literária apurou-se que o COBIT, numa perspetiva geral, apresenta dois processos adjacentes à segurança da informação, sendo que a relação dos restantes processos com esta mesma área, está especificada na publicação COBIT5SI através da apresentação de objetivos, métricas e práticas a aplicar em cada um deles. Assim, ao avaliar todos estes objetivos, métricas e práticas, o foco da análise estaria na parte técnica dos processos. Optou-se, então, por avaliar, de uma forma mais generalizada, a implementação de todos os processos recomendados no COBIT, obtendo assim uma visão mais ampla da gestão e governança da organização, permitindo analisar quais os processos que a organização implementa tendo em vista o alcance dos seus objetivos.

No que se refere à opção de incluir o facilitador Princípios, Políticas e Frameworks na análise a desenvolver, com grande ênfase nos princípios e políticas recomendados, a mesma centra-se no facto de estes serem os principais mecanismos que permitem aos órgãos administrativos comunicar as regras a aplicar que irão servir de apoio à obtenção dos objetivos e as orientações mais detalhadas acerca de como se deve pôr em prática essas mesmas regras. Por isso mesmo, focou-se uma parte da análise na perceção de que tipo de regras e orientações se encontram documentadas na organização.

Relativamente ao facilitador Estruturas Organizacionais, considerou-se um ponto-chave de análise pois as diferentes funções e práticas adjacentes executadas permitem à organização obter um bom resultado no que toca à tomada de boas decisões. Assim, pretendeu-se perceber qual a estrutura organizacional do centro hospitalar por forma a avaliar, tendo por base as recomendações do COBIT5SI, se a mesma se encontra otimizada.

Por último, e sendo a informação um recurso valioso para todas as organizações, optou-se pelo facilitador Informação, com o intuito de verificar qual a informação de segurança da informação que a organização detém neste momento, e quais os *stakeholders* que estão direta ou indiretamente relacionados com a mesma.

Assim, após a escolha do foco admitido na nossa análise, iniciou-se o contacto com o centro hospitalar para posteriormente se recolher a informação para implementar-se a avaliação planeada. Para a recolha da informação, o objetivo passou por perceber a perspetiva de um dos colaboradores com forte presença na área da gestão da informação da organização. Com isto em mente, escolheu-se a entrevista como método que permitiria obter essa informação para futuro tratamento de dados. Na preparação da entrevista, para além de se desenvolver uma listagem das diferentes recomendações adjacentes aos quatro facilitadores, juntou-se também a descrição dos diferentes princípios, políticas, processos, funções, práticas e tipos de informação que se pretendia avaliar durante a realização da mesma. Preparou-se então estas secções com o objetivo de obter uma espécie de *checklist* que mostrasse quais as recomendações do COBIT na área da segurança da informação que estariam a ser aplicadas na organização.

No centro hospitalar, iniciou-se o contacto com o departamento de sistemas de informação, por este ser o departamento que habitualmente trata da gestão da segurança da informação. Assim, direcionou-se o contacto para o diretor do departamento em causa, pois para além de este apresentar uma visão geral do departamento de sistemas de informação e de todos os processos, práticas, etc., que são implementados na área de sistemas de informação, e consequentemente, na área de segurança da informação, apresenta também um conhecimento global da organização. Conseguiu-se, então, a colaboração do diretor do departamento de sistemas de informação, que aceitou participar na realização do nosso caso de estudo participando, para tal, numa entrevista de apuramento de dados que permitissem realizar o objetivo enunciado anteriormente.

5. Resultados Obtidos

Foi, então, desenvolvido um caso de estudo junto de um centro hospitalar da zona norte, sendo o mesmo considerado como uma empresa pública empresarial cuja classificação de atividades económicas é a 86100, a qual está associada às atividades dos estabelecimentos de saúde com internamento. Como já referido, o COBIT apresenta uma maior abrangência em termos de gestão e governança, e como tal foi a norma base utilizada na realização deste caso de estudo. As questões realizadas permitiram-nos analisar quais as recomendações que estavam a ser implementadas na organização em análise, permitindo dessa forma perceber em que nível de conformidade a mesma estaria com o *framework* COBIT, nos pontos analisados.

Verificou-se então que a grande maioria (11 dos 12) dos princípios independentes sugeridos pelo COBIT5SI, que visam ajudar os profissionais de segurança da informação a adicionar valor às suas organizações, se tratam de preocupações da organização e se encontram incluídos na sua documentação, cobrindo os três módulos apresentados no COBIT5SI de suporte ao negócio, de defesa do negócio e de promoção de um comportamento responsável de segurança da informação. No entanto, estão dispersos por vários documentos e este cruzamento de dados em diferentes documentos, embora faça sentido para os órgãos diretivos e de gestão, pode ser um impeditivo à rápida perceção, por parte dos colaboradores da organização, de quais os princípios de segurança a serem seguidos pela organização, sendo considerado este um ponto de melhoria. O mesmo se verifica relativamente às políticas sugeridas pelo COBIT5SI. Estas tratam-se de preocupações presentes no dia-a-dia da organização, focando-se nos controlos de acesso, nas respostas a incidentes, no pessoal de segurança da informação e no meio físico e ambiental de segurança da informação. Contudo, mais uma vez, em termos de documentação não se verifica, em todos os casos, a existência de documentos concretos acerca de cada política. Segundo o COBIT5SI, os diferentes princípios, políticas e *frameworks* devem estar definidos e devidamente documentados, estando portanto muito bem definido onde cada um deles poderá ser encontrado. Verifica-se o mesmo ponto de melhoria relativamente a princípios e políticas, sendo que essa melhoria poderá trazer o benefício à organização de conseguir evitar problemas de segurança causados por alguma falha na informação adquirida pelos seus colaboradores. Numa segunda instância, e ainda acerca de políticas recomendadas, verifica-se que o entrevistado tem conhecimento de outras políticas, não tanto associadas à função de segurança da informação, mas que ajudam numa boa implementação da segurança da informação, havendo, portanto, indícios de uma boa comunicação interna na organização.

Relativamente a processos, para além de verificar-se se os mesmos existiam e eram implementados na organização, avaliou-se também em que etapa de implementação os mesmos se encontrariam (figura 3). Para isso, utilizou-se por base a escala utilizada no modelo de CMMI (*Capability Maturity Model Integration*), uma vez que este se aplica à melhoria de processos de desenvolvimento e manutenção de produtos e serviços. Neste modelo, apresentam-se 5 níveis de maturidade: inicial, no qual os processos são projetados consoantes os problemas que surgem; intuitivo, onde existe uma política por base para a implementação do projeto; definido, com processos bem caracterizados, descritos e compreendidos; gerido quantitativamente, quando a organização tem definido objetivos quantitativos a serem alcançados e os usam como critérios na gestão dos processos; e em otimização, fase na qual a organização se concentra na melhoria contínua do processo [CMMIInstitute 2006].

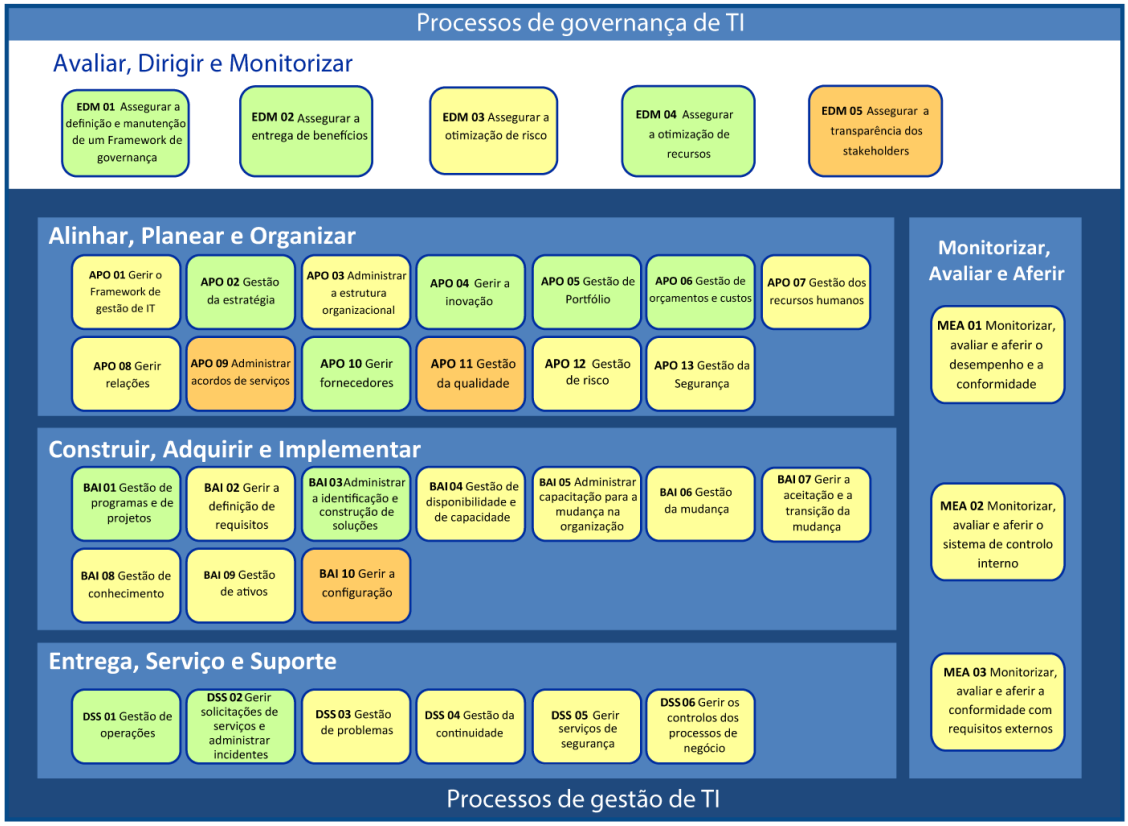

Figura 3 – Fases de implementação dos processos recomendados pelo COBIT [ISACA 2012]

Numa avaliação geral, nenhum dos processos se encontra em fase otimizada, havendo somente doze deles considerados como geridos e mensurados, quatro em fase de intuição e os restantes vinte e um numa fase onde já se encontram definidos. Em termos de média, os processos encontram-se numa fase definida, ficando unicamente quatro processos abaixo da média. Não houve nenhum processo que não tenha sido reconhecido pelo responsável do departamento de SI como uma preocupação ou prática seguida pela organização. Sendo que a nossa análise não se focou nas métricas associadas aos diferentes processos, o facto de existir dentro do departamento de SI um conhecimento acerca dos processos que o COBIT5SI recomenda é de extrema importância, uma vez que estes visam pôr em prática os princípios e objetivos adjacentes à área da segurança da informação. Esta análise poderá também ser utilizada pela organização para identificar quais os processos que necessitam ser melhorados ou que já se encontram numa etapa de desenvolvimento adequada.

No que respeita às estruturas organizacionais recomendadas, verificou-se que grande parte das práticas de segurança, adjacentes às diferentes estruturas organizacionais ou funções, acaba por passar pelas mãos do CISO, mesmo existindo na estrutura da organização uma função preparada para a execução dessas práticas em análise (figura 4).

Em termos das práticas recomendadas para a função do CISO, somente uma das 17 é que não se trata de uma responsabilidade do CISO no centro hospitalar em análise. Para além disso, uma vez que a função do gestor de segurança da informação (ISM – *Information Security Manager*) é operacionalizada na organização pela mesma pessoa que responde à função de CISO, acresce mais 6 práticas, das 9 recomendadas para esta função, às responsabilidades do colaborador a ocupar o cargo de CISO. Apurou-se ainda que a organização em análise ainda não tem nomeado uma comissão de segurança da informação (ISSC – *Information Security Steering Committee*), sendo que 50% das práticas recomendadas pelo COBIT5SI para esta função (ou seja, 5 das 10) caem novamente no cargo do CISO. O mesmo verifica-se relativamente às práticas adjacentes à comissão de risco (ERMC – *Enterprise Risk Management Committee*), nas quais o CISO está responsável na organização por metade (2 de 4). Em termos das práticas associadas aos responsáveis pela informação ou proprietários da empresa, o COBIT5SI apresenta-nos uma listagem de 3 práticas das quais uma não se aplica na organização, outra está associada à função que recomenda, e uma terceira recai sob a alçada do CISO, mais uma vez.

É verdade que a função do CISO tem associada uma grande responsabilidade na área da segurança da informação. No entanto, para uma maior garantia de que as práticas de segurança estão, de facto, a serem cumpridas, deveria existir uma maior segregação das funções. Deste modo, a mesma pessoa não ficaria responsável por demasiadas práticas de segurança evitando que esteja sobrecarregada e não consiga prestar o mesmo nível de atenção às diferentes áreas da segurança e evitando, também, que uma só pessoa tenha um determinado poder relativamente à segurança da informação da organização. A organização poderá organizar uma listagem das diferentes práticas a realizar em termos de segurança da informação, e associar às funções existentes na estrutura da organização. Poderá utilizar como base a listagem do COBIT5SI, pois verificou-se a existência de todas as práticas na organização, mas a listagem deverá, acima de tudo, ser adequada à realidade da organização e baseada numa visão macro com o objetivo de garantir que todas as áreas e práticas de segurança são cobertas e distribuídas pelas funções existentes.

FUNÇÕES		Função na Organização	Comparação com o COBIT5SI
CISO	(Chief Information Security Officer)		
	Práticas recomendadas ao CISO	Sim	94% - CISO
ISSC	Information Security Steering Committee		
	Práticas recomendadas ao ISSC	Não	50% - CISO 50% - Chefes dos Projetos
ISM	Information Security Manager		
	Práticas recomendadas ao ISM	Associada ao CISO	67% - CISO 33% - Chefes dos Projeto
ERMC	Enterprise Risk Management Committee		
	Práticas recomendadas ao ERMC	Sim	50% - ERMC 50% do CISO
RI / PE	Responsáveis pela Informação / Proprietários da Empresa		
	Práticas recomendadas aos RI/PE	Aplicável quando necessário	33% - RI / PE 33% - CISO 33% - não aplicável na organização

Figura 4 – Resumo dos resultados obtidos da avaliação realizada ao centro hospitalar

Por fim, em termos do facilitador Informação, verificou-se que, embora os diferentes tipos de informação, tais como estratégia de segurança da informação, material de consciencialização, orçamento de segurança, entre outros, não se encontrem documentados individualmente, existe uma melhor definição de onde poderão ser encontradas os diferentes tipos de informação de segurança da informação, e que essa informação já se encontra intrínseca no dia-a-dia das atividades realizadas, ao contrário do que acontece com os princípios e as políticas. Embora não seja da mesma forma que o COBIT5SI recomenda, a forma como a organização opera em termos de tratamento dos diferentes tipos de informação relevante à área de segurança da informação não evidencia carecer de tratamento.

Realizou-se também uma matriz que permite o relacionamento dos diferentes tipos de informação com os *stakeholders* existentes na organização (figura 5). Não existindo uma solução para esta matriz, a mesma é importante para permitir ter conhecimento de onde atuam os *stakeholders* da organização podendo perceber-se se a alocação dos mesmos está a ser bem efetuada ou não. Em análise, voltou a verificar-se que a função do CISO é a que está mais sobrecarregada no que toca a originar e aprovar informação de segurança, tendo uma presença ativa em todo o tipo de informação de segurança. Esta informação pode ser uma mais-valia para a organização utilizar na distribuição de tarefas pela sua estrutura organizacional.

Stakeholder		Tipo de Informação									
		Estratégia de Segurança da Informação	Orçamento de Segurança da Informação	Plano de Segurança da Informação	Políticas	Requisitos de Segurança da Informação	Material de Consciencialização	Relatórios de Revisão de Segurança da Informação	Catálogo de Serviços de Segurança da Informação	Perfil de Risco da Informação	Painel de Instrumentos de Segurança da Informação
Interno: Organização	(Presidente e Diretor Executivo) CEO	A	A	I	A	O	A	I			
	(Diretor Executivo de Finanças) CFO	A	A	I	I	O	I	I			
	(Diretor de Operações) COO	A	I	I	I	O	I	I			
	(Diretor de Risco) CRO	O		I	I	O	I	I	I	O	I
	(Diretor de Segurança da Informação) CISO	O	O	O	O	O	O	O	A	A	O
	Direção da Estrutura				I	O	I			O	
	Chefe de Recursos Humanos				I	O	I			O	
	Auditoria	O		I	I	O	I	I	I	O	I
Interno: TSI	(Diretor Executivo de Informação) CIO	O	O	O	A	O	A	A	A	A	A
	Chefe das Operações de TSI	O	I	O	I	O	I	I	I	I	O
	Administração de Sistemas	O	I	O	O	O	I	I	O	O	O
	Chefe de Projeto	O	I	O	O	O	I	I	O	O	O
Externo	Autoridades (aplicação da lei)	O				O					
	Reguladores	O		O		O					
	Vendedores/Fornecedores	O		O		O					
	Parceiros (outros hospitais					O					

O - Origina | A - Aprova | I - Informado | U - Utiliza

Figura 6 – Matriz Stakeholders vs. Tipos de Informação de Segurança da Informação da organização em análise baseada nas recomendações do COBIT5SI [ISACA 2012]

6. Conclusão

A informação adquiriu um papel essencial na nossa sociedade, e com o passar do tempo, a importância deste recurso acresce cada vez mais. Numa perspetiva de organizações que se envolvam diretamente com dados relacionados com um assunto tão confidencial como o é a saúde de cada um de nós, é ainda mais necessário garantir a proteção da informação para que se garanta que a mesma é fidedigna, protegendo assim a reputação da organização aos olhos dos seus clientes e parceiros.

Foi possível apurar que, no centro hospitalar da zona norte em análise, existem preocupações que pretendem garantir o máximo de segurança da informação que possuem. Não só este centro hospitalar já se encontrava a implementar controlos previstos na norma ISO27001, como se verifica que em termos de COBIT, um *framework* mais amplo em termos de gestão e governança e que permite a ponte entre a segurança da informação e os objetivos de negócio

com a sua publicação COBIT5SI, este centro hospitalar reconhece a aplicação de grande parte das recomendações avaliadas. Demonstra, de facto, que a segurança da informação é uma temática de elevada importância para a organização em análise, e que a mesma se encontra a implementar controlos, práticas, processos, entre outros, que permitem que a segurança da sua informação esteja garantida.

Verifica-se, tanto em termos de análise do caso de estudo como em termos de avaliação da revisão bibliográfica realizada, que a utilização de diferentes normas numa organização é uma mais-valia, pelo menos quando a temática se trata de segurança da informação, visto que, como cada norma apresenta o seu âmbito e objetivos específicos, a utilização de outro, de forma alinhada, permite às organizações cobrirem uma maior área de atuação na organização, obtendo assim melhores resultados na gestão da segurança da informação.

7. Referências

Arora, V. (2010) "Comparing different information security standards: COBIT vs. ISO 27001"

BSI (2008). BSI-Standard 100-1 Information Security Management Systems (ISMS), Federal Office for Information Security (BSI)

BSIgroup (2014). Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 - The new international standard for information security management systems. B. S. I. Group.

Calder, A. (2013). Information Security & ISO 27001 - An Introduction. IT Governance Green Paper.

Cannon, D. L. (2008). Certified Information Systems Auditor - Study Guide, Wiley Publishing.

Cartlidge, A., A. Hanna, C. Rudd, I. Macfarlane, J. Windebank and S. Rance (2007). An Introductory Overview of ITIL, The IT Service Management Forum.

Clinch, J. (2009). ITIL V3 and Information Security - White Paper, Best Management Practice.

CMMIInstitute (2006). CMMI for Development. v1.2.

FFIEC (2006). IT Examination Handbook. Information Security Booklet. F. F. I. E. Council.

Gantz, S. (2014). The Basis of IT Audits - Purposes, Processes, and Practical Information.

Greenfield, D. (2007) "Standards For IT Governance - ITIL, COBIT, and ISO 17799 provide a blueprint for managing IT services.".

ISACA (2012). CoBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.

ISACA (2012). CoBIT 5 for Information Security.

ISO (2013). ISO/IEC 27001:2013 [Information technology — Security techniques — Information security management systems — Requirements].

ITGI (2005). Aligning COBIT, ITIL and ISO17799 for Business Benefit: Management Summary (with OGC and itSMF).

Kajava, J., J. Anttila, R. Varonen, R. Savola and J. Röning (2006) "Information Security Standards and Global Business."

Kouns, B. L. and J. Kouns (2011). The Chief Information Security Officer - Insights, tools and survival skills, IT Governance Publishing.

Meijer, M., M. Smalley, S. Taylor and C. Dunwoodie (2011). ITIL® V3 and BiSL: Sound guidance for business IT alignment from a business perspective. B. M. Practice.

NIST (2002). Federal Information Security Management Act of 2002 (Title III of E-Gov), National Institute of Standards and Technology 48-63.

Pelnekar, C. (2011). Planning for and Implementing ISO 27001. ISACA Journal.

Ridley, G., J. Young and P. Carroll (2004). COBIT and its Utilization: A framework from the literature. Hawaii International Conference on System Sciences.

Rouse, M. (2009). "Security Information Management (SIM)." Search Security - TechTarget.

Sheikhpour, R. and N. Modiri (2012). "A best practice approach for integration of ITIL and ISO/IEC 27001 services forinformation security management." Indian Journal of Science and Technology 5.

Solms, B. v. (2005). "Information Security governance: COBIT or ISO 17799 or both?" Computers & Security 24: 99-104.

Stroud, R. (2010) "Like Peanut Butter & Jelly: Pairing COBIT® and ITIL® for Better Service Management and Governance ".

Susanto, H., M. N. Almunawarand and Y. C. Tuan (2011). "Information Security Management

TSO (2007). The Official Introduction to the ITIL Service Lifecycle. O. o. G. Commerce, The Stationery Office (TSO)

Turner, M. J., J. Oltsik and J. McKnight (2008). ISO, ITIL and COBIT triple play fosters optimal security management execution. SC Magazine for IT Security Professionals.

Whitman, M. and H. Mattord (2008). Principles of Information Security.

Wright, C. S. (2005). Implementing an Information Security Management System (ISMS) - Training process.