Práticas de Segurança da Informação: um estudo de caso num centro hospitalar

Sabina Aneide Amaral da Mota Santos

Dissertação de Mestrado

Mestrado em Auditoria

Porto – 2014

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO

INSTITUTO POLITÉCNICO DO PORTO

Práticas de Segurança da Informação: um estudo de caso num centro hospitalar

Sabina Aneide Amaral da Mota Santos

Dissertação de Mestrado

apresentada ao Instituto de Contabilidade e Administração do Porto

para a obtenção de grau de Mestre em Auditoria,

sob a orientação de Luís Silva Rodrigues

Porto – 2014

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO

INSTITUTO POLITÉCNICO DO PORTO

Resumo:

Nos dias de hoje e cada vez mais as tecnologias e sistemas da informação (TSI) são utilizadas em diferentes domínios. Como tal, o desenvolvimento de um bom sistema de gestão da informação é crucial para o funcionamento das organizações, independentemente do sector em que exercem a sua atividade.

Uma das preocupações que afeta todos as organizações é a segurança da informação, visto que a informação é a base de qualquer negócio. Deve, então, ser garantido que esta está protegida dos diferentes tipos de ataques e que o sistema de informação está em conformidade com o conjunto de normas seguido.

Este trabalho pretende apresentar os três normativos mais utilizados na implementação e desenvolvimento de um sistema de gestão de segurança da informação, e fazer uma comparação entre os mesmos, identificando assim as suas principais diferenças. Numa fase seguinte, é posto em prática os requisitos e/ou recomendações de um deles, avaliando-se a área de segurança da informação de uma organização, tendo por base esses mesmos requisitos e/ou recomendações, permitindo analisar na realidade a teoria estudada.

Palavras chave: Sistemas de Informação, Auditoria de Sistemas de Informação, Segurança da Informação, COBIT

Abstract:

Nowadays, information systems and technology is inserted in different kinds of main areas. Therefore, the development of a good information system is crucial to the functioning of organizations, regardless of the sector in which they conduct their activity.

One of the concerns that affects all organizations is information security, because the information is the foundation of any business. Therefore, it must be ensured that information is protected from many types of attacks and that information system complies with a set of standards.

This work wants to present the three standards and guidelines most used into the implementation and development of a information security management system, compare them and identify the differences between them. Then, it was used one of them as a basis to analyze an organization, using its requirements and/or recommendations into the evaluation of the information security area of the organization in study, allowing us to analyse in the real world the theory that has been studied.

Key words: Information Systems, Audit Information Systems, Information Security, COBIT

Dedicatória

A ti, Ricardo.

Começou contigo e só faz sentido com a tua presença.

Agradecimentos

Não podia acabar esta pequena etapa da minha vida sem agradecer a todas as pessoas que dedicaram um pouco do seu tempo para me ajudar e motivar na realização deste mestrado e desta minha dissertação.

Um especial agradecimento ao meu Professor e orientador da dissertação, Doutor Luís Rodrigues. Agradeço-lhe por ter aceite acompanhar-me nesta aprendizagem e por estar sempre pronto a tirar dúvidas, ajudar com interpretações e sugestões, dar coragem e força para as atividades que nunca tinham feito parte do meu dia-a-dia. Sem dúvida, a minha grande base para esta dissertação.

Um grande obrigado ao entrevistado, responsável pelo departamento de sistemas de informação do centro hospitalar em estudo, pela disponibilidade para a entrevista, pelos conselhos dados, pela informação disponibilizada, e pela compreensão durante todo o processo de análise.

Não posso também deixar de agradecer à Doutora Alcina Dias por se ter mostrado sempre pronta a ajudar-me com dúvidas de legislação, metodologias, e todos esses assuntos menos divertidos da elaboração de um grande trabalho como este. Fez com que todos os grandes passos parecem-se fáceis de dar.

Queria também agradecer ao Doutor Bruno Horta Soares, que sendo o grande representante do COBIT em Portugal, foi um acréscimo extremamente positivo ao meu conhecimento sobre o assunto e presenteou-me sempre com a sua prontidão em ajudar-me na minha dissertação.

Aos meus colegas de mestrado, especialmente à Denise Costa, por nunca ter faltado apoio e motivação, mesmo nos momentos em que todos achávamos que as coisas podiam estar a correr melhor.

À minha mãe, por nunca me ter pressionado e acreditar sempre que eu iria conseguir. Aliás, como em todos os momentos da minha vida académica, profissional e pessoal.

À minha irmã Rute, por se manter sempre presente no processo, lembrando sempre que estava quase-quase, mesmo quando o que faltava era bem maior do que o que estava feito. A sua eterna confiança em mim, far-me-á sempre andar para a frente.

À minha prima Rita, por ser a minha pequenina, que me lembrava que não se podia estar sempre a estudar. Ver o brilho nos seus olhos ao dizer-me que sou exemplo de vida para ela, põe qualquer hipótese de falhar completamente de parte.

Aos meus avós, pela educação que me deram, pela forma como me mostram o quanto orgulhosos estão de mim, e por me lembrarem que sem trabalho não se chega a lado nenhum.

À Sofia, por ter ouvido os diferentes passos do processo da minha tese, e me ter ajudado com os seus dotes de designer gráfica – até parece fácil!

À Né, por acreditar sempre com muita força que eu irei conseguir tudo a que me proponho alcançar.

E por fim, não podia deixar de agradecer aos meus amigos, por todo o apoio que me deram num dos grandes desafios com que me cruzei e por estarem prontos a celebrar comigo agora que o finalizei.

Lista de Abrevitaturas

AI - Acquire, Implement

APO - Align, Plan, Organize

BAI - Build, Acquire, Implement

CA - Conselho de Administração

CCTA - Central Communications and Telecommunications Agency

CEO - Chief Executive Officer

CFO - Chief Financial Officer

CIA - Confidentiality, Integrity, Availability

CIO - Chief Information Officer

CISO - Chief Information Security Officer

CMMI - Capability Maturity Model Integration

COBIT - Control Objectives for Information and Related Technology

COBIT5SI - COBIT 5 para a Segurança da Informação

COO - Chief Operating Officer

COSO - Committee of Sponsoring Organizations of the Treadway Commission

CRO - Chief Risk Officer

DDoS - Distribute Denial of Service

DoS - Denial of Service

DS - Deliver and Support

DSS - Deliver, Service, Support

EDM - Evaluate, Direct, Monitor

EPE - Empresa Pública Empresarial

ERM - Enterprise Risk Management

ERMC - Enterprise Risk Management Committee

ESG - Enterprise Strategy Group

IDS - Intrusion Detection System

IEC - International Electrotechnical Commission

ISACA - Information Systems Audit and Control Association

ISC - International Information System Security Certification Consortium

ISF - Information Security Forum

ISM - Information Security Management

ISMC - Information Security Management Committee

ISO - International Organization for Standardization

ISSC - Information Security Steering Committee

ISSM - Information Systems Security Manager

ITIL - Information Technology Infrastructure Library

ITGI - IT Governance Institute

itSMF - IT Service Management Forum

ME - Monitor, Evaluate

MEA - Monitor, Evaluate, Assess

OGC - Office of Government Commerce

PDCA - Plan-Do-Check-Act

PIN - Personal Identification Number

PMO - Project Management Office

PO - Plan, Organize

RACI - Responsible, Accountable, Consulted, Informed

SGSI - Sistemas de Gestão de Segurança da Informação

SNS - Serviço Nacional de Saúde

SOX - Sarbanes-Oxley Act

SI - Sistemas de Informação

TSI - Tecnologias de Sistemas de Informação

UPS - Uninterruptible Power Supply

VMO - Value Management Office

VPN - Virtual Private Networks

Índice

Índice de Tabelas

Índice de Figuras

1. Introdução

Na era em que nos encontramos, o poder da informação tomou proporções gigantescas. Todas as organizações lidam com informação do negócio, dos seus colaboradores, dos seus parceiros, dos seus utilizadores, etc., e precisam de garantir que a mesma é fidedigna e está protegida para que possam usá-la como base no seu negócio. Por isso mesmo, a importância da segurança da informação tem vindo a aumentar nos últimos anos, principalmente porque os ataques à informação têm sofrido um acréscimo, quer aconteçam por puro prazer ou para causar estragos às organizações.

Nos últimos anos, tem-se assistido a um desenvolvimento nos normativos que visam apoiar as organizações na implementação de um sistema de gestão de segurança da informação, visto que estas 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. Três desses normativos de referência na área da segurança da informação, muitas vezes utilizados em conjunto e que podem ser aplicados às diferentes estratégias e focos são a ISO27001[1], a ITIL[2] e o COBIT[3]. 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 já descritos e compreendidos, tendo por base um estudo do universo organizacional ao longo dos últimos anos. Desta forma, as organizações poderão focar-se no desenvolvimento da sua atividade em vez de perder tempo a criar o que já se encontra criado e disponível.

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.

[1] ISO27001 - Norma internacional que apresenta os requisitos para um sistema de gestão da segurança da informação
[2] ITIL - Information Technology Infrastructure Library [http://www.itil-officialsite.com/]
[3] COBIT - Control Objectives for Information and Related Technology [http://www.isaca.org/cobit/pages/default.aspx]

1.1 Objetivos do Estudo

Tendo como base o contexto referido anteriormente, foram definidos dois objetivos. O primeiro objetivo pretende avaliar quais as opções que uma organização tem, em termos normativos, para usar como base na definição de um sistema de segurança da informação. O segundo objetivo passou por desenvolver um caso de estudo junto de um hospital público português, utilizando por base uma das normas ou *frameworks* estudados, para perceber como é feita a gestão de segurança da informação nessa organização.

Através da revisão bibliográfica, recolheu-se e comparou-se informação de uma norma internacional e de dois *frameworks* de boas práticas, os quais apresentam requisitos ou orientações a aplicar aquando a implementação de um sistema de gestão de segurança da informação: a norma internacional ISO27001, e a libraria ITIL e o *framework* de gestão COBIT.

Uma vez que o *framework* COBIT apresentou um alinhamento com a restante gestão da organização, foi desenvolvido um estudo de caso tendo por base as suas orientações para que a segurança da informação seja assegurada. Efetuou-se então uma análise a um hospital público português, sendo que a mesma não teve uma perspetiva técnica mas sim uma perspetiva de gestão da informação.

Estudar a forma como um hospital desenvolve a gestão da sua informação, e acima de tudo da segurança da mesma, foi bastante aliciante pois a área da saúde é importante para todos os cidadãos, por ser crítica para a realização de todos os outros planos que existem na vida de cada um. Iniciou-se esta dissertação antevendo-se que no fim iria-se poder fornecer mais informação que possa ser utilizada na melhoria da gestão da informação, tanto na organização em estudo como em todas as outras que tenham o mesmo fim.

1.2 Organização do Documento

A presente dissertação está organizada em 7 capítulos.

O primeiro capítulo introduz o projeto de dissertação em causa, identificando os objetivos e motivações para a sua realização.

No Capítulo 2 é abordada a temática de auditoria de sistemas de informação, nomeadamente alguns conceitos associados aos sistemas de informação, desenvolvendo um pouco o processo de auditoria realizado para validar os sistemas de informação aplicados nas organizações.

No capítulo 3, introduz-se o tema principal desta dissertação: a segurança da informação. Apresenta-se conceitos a ter em conta ao longo desta dissertação e alguns agentes, ameaças e invasores existentes nesta área de atuação. Pode-se, ainda, consultar os principais tipos de segurança da informação existentes, acompanhados por alguns exemplos do que representam na vida real.

Poderá ser encontrada no capítulo 4, uma apresentação da importância das normas em tecnologia da informação, passando depois à especificação dos normativos identificados que contêm uma forte componente de segurança da informação: a ISO27001, a ITIL e o COBIT. Uma vez que a análise realizada no caso de estudo desta dissertação se baseou no conjunto de boas práticas de segurança da informação do ISACA[4], apresenta-se uma estruturação mais detalhada do COBIT 5 para a Segurança da Informação (COBIT5SI). Conclui-se este capítulo com uma comparação efetuada aos três normativos estudados.

No Capítulo 5, é apresentada a abordagem metodológica utilizada, e explicados, com mais detalhe, os objetivos planeados para esta dissertação.

Tendo por base a execução do estudo de caso, apresenta-se os seus resultados no capítulo 6, primeiramente descrevendo a organização em estudo, e seguindo-se da estruturação dos dados recolhidos e adjacente análise.

O último capítulo apresenta as conclusões do trabalho realizado e outras possíveis soluções a serem desenvolvidas e implementadas pela organização.

[4] ISACA - Information Systems Audit and Control Association [https://www.isaca.org/Pages/default.aspx}

2. Auditoria de Sistemas de Informação

Neste capítulo é feito o enquadramento da temática. Inicia-se com uma breve explicação do que se entende do termo sistemas de informação. De seguida, especifica-se, em termos de objetivos e causalidade, a auditoria de sistemas de informação, finalizando este capítulo com uma pequena explicação do processo da mesma.

2.1 Sistemas de Informação

O termo Sistemas de Informação (SI) é, hoje em dia, conhecido e falado mundialmente. A sua utilidade e o seu impacto em diversas áreas, têm despoletado um crescente interesse, a nível mundial, na exploração de formas inovadoras de aplicação de tecnologia, uma vez que esta se encontra em constante e rápida evolução [Ray and Acharya 2004]. É verdade que este rápido crescimento da tecnologia implica um aumento de ameaças às organizações, mas a sua capacidade de revolucionar as mesmas permite criar novas oportunidades de negócio e oferecer a possibilidade de reduzir custos [Cascarino 2007].

Este contexto de mudança continuada impõe que as empresas se informem devidamente por forma a transformar os SI num aliado no que toca à obtenção de sucesso nos objetivos estipulados. É necessário que as empresas se adaptem rapidamente às novas condições, no sentido de poderem progredir, competir e até sobreviver [Carneiro 2009].

Para que isso seja possível, deve-se começar por compreender os conceitos que envolvem o tema.

Informação é o conjunto de dados que foram interpretados e compreendidos pelo destinatário da mensagem [Lucey 2005]. Trata-se de factos ou conclusões que adquirem significado num determinado contexto. Os dados são manipulados e apresentados, e esse tratamento conduz a uma melhor compreensão da situação [Oz 2009]. É vital que exista um cuidado com a simbologia utilizada e o contexto da mensagem, por forma a reduzir a incerteza e a aumentar a probabilidade da entrega da informação ao destinatário [Lucey 2005].

Um Sistema é um conjunto de componentes inter-relacionados que trabalham em parceria para um objetivo comum. A função de um sistema é receber *inputs* e transformá-los, através de processos, em *outputs*, pesando os *feedbacks* recebidos relativamente à sua *performance*, e conseguindo assim aplicar os melhores mecanismos de controlo [Bocij et al. 2008].

Seria de esperar que fosse fácil obter uma definição universal dos SI [Amaral 1994], todavia, quando se trata de definir SI evidencia-se que o mesmo termo é usado para designar diferentes coisas [Falkenberg et al. 1998, Carvalho 2000].

Ainda assim, Carneiro [Carneiro 2009] define SI como um conjunto de sistemas ou regras e procedimentos que as organizações utilizam para acumular, organizar e fornecer dados. Outras definições têm como foco a utilização de sistemas computorizados ou informáticos, não dando tanto ênfase aos documentos ou elementos humanos, em que muitas vezes os SI se baseiam [Oliveira 2006]. No entanto, e de uma forma geral, considera-se que um SI é um sistema que recolhe, processa, armazena e distribui informação numa organização, com o objetivo de que a mesma esteja acessível a quem dela necessite [Carvalho 1996].

Como todos os outros sistemas, os SI devem ser compreendidos por todos os colaboradores da organização. A sua compreensão é necessária para que consigam utilizá-los como suporte do seu trabalho e na interação com as outras pessoas da organização [Oz 2009]. No entanto, e apesar dos avanços tecnológicos, ainda se encontra nas empresas problemas de falta de aplicação de normas, metodologias, formação e cultura generalizada [Carneiro 2009].

2.2 Auditoria de Sistemas de Informação

Inicialmente, o processo de análise aos SI encontrava-se inserido na auditoria financeira como um complemento técnico pertencente à análise efetuada. No entanto, a necessidade de adaptação criada pelo crescimento da importância da informação e pelo impacto criado pelas TSI nas organizações, implicou que esta área fosse tratada e executada como uma auditoria independente [Piattini 2000].

Na verdade, as organizações atingem os seus objetivos e cumprem as suas missões com o apoio da informação que contêm e da tecnologia que dispõem no tratamento da mesma. Como tal, as organizações são as principais interessadas em assegurar que o uso de TSI esteja a ser efetuado de forma adequada, que o seu funcionamento esteja de acordo com o esperado e que os ativos e outros recursos de TSI estejam devidamente alocados e protegidos [Gantz 2014]. Para além destes aspetos, Senft e Gallegos [Senft and Gallegos 2009] referem ainda que o risco associado às novas tecnologias serviu também de impulso à necessidade sentida nas organizações de existir uma auditoria que garanta que os controlos aplicados são adequados.

Acontece que a gestão eficaz da informação e tecnologias relacionadas adquiriu uma importância crítica, sendo considerada fulcral na sobrevivência e sucesso a longo prazo de qualquer organização [Cascarino 2007], e como consequência do peso que os SI adquiriram na realização dos objetivos da empresa e do seu sistema de gestão, foi desenvolvida a Auditoria dos Sistemas de Informação [Carneiro 2009].

Gantz [Gantz 2014] define auditoria como um exame sistemático e objetivo de vários aspetos numa organização, que tem como objetivo comparar o que esta faz com um conjunto definido de critérios ou requisitos. Assim, Auditoria dos SI examina processos, ativos de TSI e controlos em vários níveis da organização, com o intuito de determinar o quanto a organização adere às normas e/ou requisitos aplicáveis.

Auditoria dos SI é, portanto, a revisão dos SI que surge da necessidade de se verificar se as funções, e operações para as quais foram criadas, se estão a realizar, e de se comprovar que os dados nelas contidos estão de acordo com os princípios de fiabilidade, integridade, precisão e disponibilidade [Oliveira 2006]. É a avaliação das TSI, das práticas e das operações para assegurar a integridade da informação da organização [Senft and Gallegos 2009].

Como se trata de uma auditoria com um caráter transversal, sendo que, hoje em dia, todas as áreas de negócio utilizam SI, manuais ou computorizados, a auditoria dos SI pode ser utilizada no desenvolvimento de outro tipo de auditorias, como por exemplo, nas auditorias interna e externa [Cascarino 2007].

Segundo Oliveira [Oliveira 2006], a Auditoria dos SI tem como objetivos:

- Verificar a existência de medidas de controlo interno aplicáveis, com caráter generalizado, a qualquer SI da organização objeto de auditoria;
- Avaliar a adequação do SI às diretrizes básicas de uma boa gestão informática;
- Oferecer uma descrição do SI com base nas suas especificações funcionais e nos resultados que proporciona;
- Verificar se o SI cumpre os normativos legais aplicáveis;
- Verificar se a informação proporcionada pelo SI é fiável, íntegra e precisa;
- Determinar se o SI atinge os objetivos para os quais foi desenhado, de forma eficaz e eficiente;
- Propor as recomendações oportunas para que o SI se adapte às diretrizes consideradas como essenciais para o seu bom funcionamento;

Piattini [Piattini 2000], para além dos referidos, acrescenta como objetivos:

- Validação dos controlos de acesso às diferentes instalações da organização;
- Automação das atividades de auditoria interna;
- Colaboração com auditores externos;
- Formação interna, tanto dos utilizadores dos SI como dos colaboradores pertencentes ao departamento de SI;

2.3 Processo de Auditoria dos SI

O ISACA define o processo de auditoria dos SI como uma etapa que incorpora toda a prática de auditoria dos SI, incluindo procedimentos, e uma metodologia abrangente, permitindo a um auditor dos SI realizar a auditoria de forma profissional [ISACA 2010].

Gantz [Gantz 2014] estrutura este processo apresentando o início na fase de planeamento da auditoria e de preparação para a recolha de evidências. Segue-se a execução da própria auditoria que irá resultar na publicação das descobertas efetuadas num relatório final, e, por último, a realização de acompanhamento à resposta aos resultados de auditoria.

Esta evolução de acontecimentos pode ser também verificada no documento *'IT Standards, Guidelines, and Tools and Techniches for Audit and Assurance and Control Professionals*', onde o ISACA apresenta normas diretamente relacionadas ao processo de auditoria, as quais se encontram listadas na tabela 2.1 [ISACA 2010].

Normas de Auditoria e Consultoria de SI
S1 Carta de Auditoria
S2 Independência
S3 Normas e Éticas Profissionais
S4 Competência
S5 Planeamento
S6 Execução do Trabalho de Auditoria
S7 Reporte
S8 Atividades de Follow-Up
S9 Atos Irregulares e Ilegais
S10 Governança de TSI
S11 Uso da Avaliação de Risco no Plano de Auditoria
S12 Materialidade da Auditoria
S13 Usar o Trabalho de Outros Técnicos
S14 Evidência de Auditoria
S15 Controlos de TSI
S16 Comércio Eletrónico

Tabela 2.1 Normas para proceder à realização de auditorias e consultorias de SI (adaptada de [ISACA 2010])

A norma S5 foca-se exatamente na primeira etapa sugerida por Gantz [Gantz 2014], especificando alguns detalhes a ter em consideração na fase de planeamento. Estes passam por evidenciar que o auditor dos SI deverá: planear quais as áreas a cobrir com a auditoria dos SI, por forma a atingir os objetivos de auditoria e cumprir as leis e normas profissionais aplicáveis à mesma; desenvolver uma abordagem baseada em risco e tê-la documentada; desenvolver e documentar um plano de auditoria que liste todos os detalhes da mesma, desde a natureza, aos objetivos, passando pela época em que se concretizou e qual a sua extensão, e evidenciando também quais os recursos necessários; e definir e detalhar quais os procedimentos de auditoria necessários para concluir a própria auditoria. A fase de

planeamento permite dar uma atenção apropriada às áreas importantes da auditoria, identificar potenciais problemas e resolvê-los de forma atempada assim como organizar e gerir devidamente o trabalho de auditoria com o intuito de realizar o mesmo de forma eficaz e eficiente [Costa 2010].

Para que o planeamento seja bem executado, é necessário que o auditor dos SI retenha alguns conhecimentos fulcrais da organização que o irão ajudar a definir quais os procedimentos a aplicar na mesma. Para isso, é importante que o auditor obtenha conhecimento sobre o negócio da organização, saiba quais os objetivos estratégicos e financeiros, assim como os objetivos operacionais para o controlo interno [Cannon 2008].

No entanto, esse conhecimento poderá não ser suficiente para ajudar a definir quais as áreas prioritárias a tratar na auditoria e a inserir no plano em elaboração.

Sayana [Sayana 2002] corrobora a norma S5, no seu ponto 4, constatando que o auditor é muitas vezes confrontado com questões relativamente ao que auditar, quando e com que frequência, e que a resposta a estas perguntas é conseguida adotando uma abordagem baseada no risco. O ISACA fortifica esta necessidade de existência de uma avaliação de riscos indicando, na sua norma S11, no seu ponto 3, que o auditor deverá usar uma avaliação de riscos apropriada para o desenvolvimento geral do planeamento da auditoria e para a determinação de prioridades, conseguindo desta forma alocar de forma eficaz os recursos disponibilizados [ISACA 2010]. Cascarino [Cascarino 2007] afirma que é mesmo uma das responsabilidades do auditor cooperar no processo facilitando a identificação e avaliação de riscos e auxiliando na monitorização para que a gestão consiga perceber o quão bem os riscos estão a ser geridos pela organização.

Após o auditor realizar a avaliação de riscos, e ter o planeamento efetuado tendo em conta as áreas mais prioritárias para a execução da auditoria, segue-se essa mesma execução.

Na norma S6, execução do trabalho de auditoria, o ISACA salienta três conceitos: supervisão, evidências e documentação. Relativamente à supervisão, regista a importância da equipa de auditoria ser supervisionada de forma a providenciar segurança razoável de que os objetivos de auditoria são realizados e de que as normas profissionais aplicáveis são cumpridas. Quanto às evidências, verifica a necessidade do auditor dos SI obter evidência suficiente, confiável e relevante para alcançar os objetivos da auditoria, e que apoie, através de uma análise e interpretação adequada, os resultados e conclusões da auditoria. No que toca à documentação, nota que todo o processo de auditoria deve ser documentado, descrevendo detalhadamente o trabalho de auditoria realizado e as evidências de auditoria que suportam os resultados e conclusões do auditor [ISACA 2010]. Esta é a fase onde se irão realizar os procedimentos pensados na fase de planeamento com o objetivo de perceber se existe conformidade nas áreas auditadas com aquilo que está previsto acontecer dentro da organização. Existem dois tipos de testes que poderão ser utilizados: os que irão verificar a

presença ou ausência de algo, conhecidos como testes de conformidade; e os que procuram verificar o conteúdo e a integridade da evidência, denominados por testes substantivos [Cannon 2008].

Após a realização de testes, da recolha de evidências, de ter os resultados documentados e de perceber quais as conclusões a apresentar relativamente à auditoria efetuada, chega o momento de passar esse conhecimento à gestão da organização, através do relatório de auditoria [Senft and Gallegos 2009]. A norma S7, foca-se em indicar ao auditor o que este relatório deverá conter [ISACA 2010]. O auditor deverá, no final da auditoria, fornecer à organização um relatório, indicando qual a organização auditada, quais os destinatários dos relatórios e quais as restrições à auditoria caso existam, indicando também o âmbito, os objetivos, o período, a extensão e a natureza da auditoria. Para além disso, deverá apresentar as suas descobertas no âmbito da auditoria e posteriores conclusões, assim como, recomendações que o auditor ache necessárias e adequadas. Neste relatório, todas os resultados apresentados deverão estar bem fundamentados com as evidências recolhidas ao longo da auditoria [ISACA 2010].

Como referimos anteriormente, tendo em conta as fases apresentadas por Gantz [Gantz 2014], após fornecer à organização os resultados da auditoria, resta acompanhar a resposta que a organização dá aos mesmos. Seguindo essa linha de pensamento, o ISACA apresenta a norma S8, referente às atividades de *follow-up*, onde constata que após a entrega do relatório, o auditor deve solicitar e avaliar informação relevante para que possa concluir se estão a ser postas em prática as ações planeadas, e se estas estão a ser realizadas de forma apropriada e atempada [ISACA 2010].

3. Segurança da Informação

Neste capítulo introduz-se segurança da informação e a sua gestão dentro de uma organização. Segue-se uma breve apresentação dos agentes de segurança da informação, assim como das habituais ameaças e invasores nesta área de atuação. Por fim, é realizada uma descrição de dois tipos de segurança (física e lógica) com o intuito de apresentar alguns exemplos concretos do que se trata a segurança da informação na prática.

3.1 Conceito

A informação adquiriu um papel essencial na nossa sociedade, e com o passar do tempo, a importância deste recurso acresce cada vez mais, sendo a sociedade atual considerada como a sociedade da informação [Piattini 2000]. É 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 [FFIEC 2006]. Uma vez que a informação serve de base à continuidade do negócio, aplicam-se controlos para garantir essa proteção. A seleção e aplicação de controlos que sejam apropriados, permite à entidade utilizar a segurança como uma forma de atingir os seus objetivos [Senft and Gallegos 2009].

Segurança trata-se de garantir a proteção contra adversidades, quer estas aconteçam de forma intencional ou não, e 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].

Dimitriadis [Dimitriadis 2011] refere num artigo publicado no ISACA que primeiramente a segurança da informação era vista como um problema técnico, sendo que esta visão fez com que inicialmente a arquitetura de segurança passa-se principalmente por controlos preventivos. No entanto, essa abordagem mostrou ser insuficiente, uma vez que os incidentes de segurança continuavam a aumentar. Dimitriadis [Dimitriadis 2011] afirma que os problemas associados à definição de segurança da informação dificultaram a explicação do valor da mesma às organizações.

Hoje em dia, no entanto, as organizações já têm uma noção mais enquadrada com a realidade no que toca à importância da segurança da informação, uma vez que a informação serve de base à continuidade do próprio negócio [Senft and Gallegos 2009].

O ISACA 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.
- **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 [Rouse 2009], 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]. Por forma a automatizar esta gestão, as organizações podem basear-se num Sistema de Gestão de Segurança da Informação (SGSI) [Rouse 2009].

Um sistema de gestão abarca todas as políticas que se considerem pertinentes à supervisão e à gestão dentro da organização, com a finalidade de atingir os objetivos da mesma. Assim, um 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], e consegue-se desta forma garantir a confidencialidade, integridade e disponibilidade da informação [Cannon 2008].

3.2 Agentes

Para que seja garantida a segurança da informação através da implementação do SGSI integrado na organização, é necessário que haja estrutura organizacional base que suporte os objetivos de gestão na área da segurança [Cannon 2008].

O ISACA [ISACA 2010] aponta como algumas das posições associadas à gestão da segurança da informação as dos gestores executivos, que são responsáveis pela proteção dos ativos de informação e por manterem uma política de segurança presente e ativa na organização; as dos utilizadores, que seguem os procedimentos em vigor na política de segurança da organização e aderem aos regulamentos de segurança aplicáveis; e as dos auditores dos SI, que irão fornecer uma avaliação independente relativa à adequação dos objetivos de segurança da organização com os controlos implementados relacionados com estes objetivos, revendo também a sua eficácia.

No entanto, as três posições com mais ênfase nesta área passam pelo diretor da segurança da informação, o CISO (*Chief Information Security Officer*), cuja responsabilidade se centra em articular e definir as políticas ativas na organização para proteger os seus ativos de informação, garantindo que as mesmas estão a ser cumpridas; pelo diretor de privacidade que é o responsável por articular e fazer cumprir as políticas que irão proteger a informação confidencial dos clientes e dos colaboradores; e pelo gestor de segurança dos SI, ISSM (*Information Systems Security Manager*), que irá assegurar no dia-a-dia o cumprimento das regras de segurança do sistema, seguindo as diretrizes definidas pelo diretor de segurança e de privacidade. Este último, deverá supervisionar e ter o apoio de uma equipa de analistas de segurança de SI que irão trabalhar projeto a projeto, lidando com os diferentes problemas de segurança em vigor. [Cannon 2008], [ISACA 2010].

3.3 Ameaças e Invasores

As organizações têm que lidar com ameaças ao seu negócio. Esta é uma realidade que acompanha o mundo dos negócios desde sempre. E existem vários exemplos de como estas ameaças se podem fazer sentir numa organização, desde o roubo de informação, a fraude, sabotagem, espionagem industrial, etc. Ter conhecimento de que tipos de ameaças podem pôr em causa a segurança das nossas organizações é uma mais-valia no processo de gestão da segurança da informação das mesmas [Cannon 2008].

No que diz respeito à classificação das diferentes ameaças que podem afetar a informação ou os SI de uma organização, de acordo com Piattini [Piattini 2000], poderemos diferenciá-las numa perspetiva de origem e, nesse caso, poderemos nomeá-las como acidentais, que derivam de erros humanos, de falha de equipamentos, falta de energia, etc.; naturais, que advêm de causas naturais; ou intencionais, isto é, feitas com a intenção de danificar os SI da entidade e a informação contida neles. Se, no entanto, nos quisermos focar no modo

operacional com que ocorrem, passamos a uma fase em que a ameaça já passou a ataque, pois já se concretizou, e poderemos designá-los como passivos, que são caracterizados pela observação, com o objetivo de adquirir informação; ou ativos, onde se verifica um ato malicioso com o intuito de interferir com os sistemas da empresa [Piattini 2000].

No que toca a esta última abordagem, existem alguns exemplos no âmbito de cada tipo de ataque. Por exemplo, pode ser realizada uma análise da rede com o objetivo de conhecer a infraestrutura da mesma por completo. Temos ainda o *eavesdropping*, o tradicional método de espiar com a intenção de obter informação. Estes são exemplos de ataques passivos.

Relativamente a ataques ativos podemos apontar o *phishing*, que se trata de copiar as páginas da internet de uma determinada entidade e utilizar essa informação para elaborar um *email* ou uma página da internet falsa, enganando assim os utilizadores. Temos também o *spamming*, cuja ação está associada ao envio de uma mensagem de forma continuada para um grande número de utilizadores. Podemos referir também os típicos vírus, que se tratam de programas que interrompem o processamento normal das tecnologias de informação e se replicam e distribuem para múltiplos computadores, sem ajuda externa, fazendo essa transição absolutamente sozinhos; e ainda a técnica *salami* que perpetua alterações tão insignificantes que quando vistas isoladamente não são detetadas, mas que no todo podem representar perdas de valor elevado para a organização. Outro tipo de ataque ativo utilizado é o DoS (*Denial of Service*) que tem como objetivo sobrecarregar o sistema, remotamente, conseguindo que o utilizador habitual não possa processar nada no computador; e temos também a sua evolução, o DDoS (*Distribute Denial of Service*), onde é possível utilizar um computador da organização tendo em vista o lançamento de ataques contra outros computadores da mesma organização, sobrecarregando-os. Estes são alguns exemplos de ataques que podem trazer danos para a organização, tanto numa perspetiva financeira ou política como numa perspetiva reputacional. É importante manter em mente a possibilidade de acontecerem, e usar a informação relativamente a estas ameaças na definição do plano de segurança da informação da organização, porque embora não saibamos quando irão acontecer, a organização deve estar pronta a lidar com as mesmas [Cannon 2008].

Este fator de imprevisibilidade é, sem dúvida, uma mais-valia para os invasores, e nunca se sabe quais são os motivos que os irão mover para a ação, pois estes podem ser políticos, económicos, com teor vingativo ou simplesmente por pura paixão e divertimento. Mas, seja qual for o motivo, acaba sempre por interferir e causar danos à organização, embora uns sejam mais graves do que outros. Existem muitos invasores com tempo, acesso e habilidades necessárias para perpetuar os diferentes ataques [Cannon 2008].

Por exemplo, os *hackers* são programadores com a capacidade e o conhecimento para explorar os detalhes de um programa e redesenhá-lo, com o objetivo de conseguir um acesso que à partida lhes estaria restrito. Por sua vez, os *crackers* tentam ganhar acesso a um sistema

alheio sem permissão, quebrando, assim, as medidas de segurança aplicadas. Já os *script kiddies* utilizam programas já desenvolvidos por outrem para procederem à invasão planeada.

Estes ataques podem também ser perpetuados pelos empregados que já têm garantido o acesso aos sistemas da organização, o que facilita a execução de qualquer atividade ilícita contra a entidade, e podendo, assim, utilizar a informação disponibilizada internamente para ações que ponham em causa o alcance dos objetivos da entidade. No entanto, alguns ataques podem surgir devido à ignorância, sendo ataques acidentais, em que alguém, por falta de conhecimento, acaba cometendo uma infração que ponha em risco a organização [ISACA 2010].

3.4 Tipos de Segurança

É necessária a existência de um programa de segurança que vise assegurar que os diferentes tipos de informação que suportam as atividades de negócio, tais como sistemas, dados, imagens, textos ou registos de vozes, estão a ser protegidos [Musaji 2001]. Para que esta garantia seja conseguida irão ser utilizados vários instrumentos em diversas áreas de ação [Silva et al. 2003].

Cascarino [Cascarino 2007] enumera as seguintes áreas como estando dentro do âmbito da segurança dos SI: segurança física, segurança com o pessoal, segurança de dados, segurança das aplicações informáticas, segurança dos sistemas informáticos, segurança das telecomunicações, segurança das operações computacionais, retenção de registos vitais, seguros, serviços contratados fora da organização, planos de recuperação após desastre e fraude e/ou crimes informáticos.

O ISACA [ISACA 2010], por sua vez, evidencia duas áreas de segurança: segurança física e segurança lógica. Esta são as duas áreas de segurança que iremos desenvolver de seguida.

3.4.1 Segurança Física

Musaji [Musaji 2001] defende que a primeira linha de defesa para a maioria dos SI é a segurança física. De facto, no que toca a salvaguarda da informação, o ambiente físico no qual a organização opera é um dos mais importantes elementos [Silva et al. 2003]. Oliveira [Oliveira 2001] afirma que, embora importantes, as técnicas de proteção de dados não serão uma vantagem no plano de segurança da organização se a segurança física não estiver garantida. No entanto, em muitas organizações a segurança física encontra-se abaixo dos padrões aceitáveis [Oliveira 2001, Champlain 2003, Cascarino 2007, Carneiro 2009].

A segurança física abrange todos os controlos que visam proteger o lado físico do sistema contra a danificação ou até mesmo de roubo [Musaji 2001]. Tem como principal objetivo assegurar a proteção dos SI respetivamente às suas dimensões físicas e aos seus

componentes, nomeadamente *hardware*, *software*, documentação e meios magnéticos [Carneiro 2009]. Esta proteção não está somente focada naqueles que se encontram dentro da organização, tendo também atenção aos indivíduos que não estejam dentro das instalações [Musaji 2001].

Basicamente, a segurança física consiste em implementar barreiras físicas e procedimentos de controlo, que sejam utilizados como medidas de prevenção e contramedidas perante as possíveis ameaças aos recursos existentes na organização e à informação confidencial da mesma [Carneiro 2009]. Para tal, pode-se utilizar uma variedade de componentes.

Uma das formas de defesa na segurança física concentra-se na utilização de diversos tipos de fechaduras. As chaves convencionais são um dos meios mais utilizados no controlo do acesso a salas restritas. Aqui deverá existir um responsável tanto pela contratação dos fornecedores que instalam as fechaduras novas, como pela emissão de todas as chaves, e também pela entrega aos indivíduos que deverão ter acesso à chave emitida, garantindo de igual modo que qualquer chave sobresselente esteja devidamente protegida [Champlain 2003]. Embora se trate de um método barato e fácil de instalar não permite ter a informação de quem abriu a fechadura em determinada altura, pois toda a gente tem uma chave, a qual não identifica a pessoa que a utilizou.

Em casos onde gostaríamos de saber quem utilizou determinado acesso poderíamos usar uma fechadura eletrónica. Nestes casos cada utilizador receberá um cartão de acesso eletrónico de identificação única que lhe irá permitir o acesso [Cannon 2008]. Aqui, temos a vantagem de ter um maior controlo sobre os acessos efetuados, tendo como possibilidade, por exemplo, restringir o acesso de um certo indivíduo a determinada área durante um período de tempo específico [Champlain 2003]. No entanto, este tipo de fechadura não nos permitirá ter uma certeza absoluta sobre a quantidade de pessoas que usufruíram do acesso garantido.

Um tipo de ferramenta que se poderia utilizar neste sentido seriam as câmaras de videovigilância, que permitem acompanhar em tempo real, ou ter acesso posterior, à atividade que está a decorrer no local onde as mesmas se encontram instaladas [Cannon 2008]. Para que seja possível utilizar o registo dessas câmaras no futuro, é necessário que o sistema de vídeo esteja programado para que o dia, a data e a hora apareçam na gravação. As câmaras devem ser posicionadas em locais estratégicos que permitam um visão clara dos diferentes acessos da organização que se destinam a proteger, e os monitores deverão ser instalados nos locais onde os guardas efetuam o seu trabalho. Esta é uma outra mais-valia no que toca a segurança física: a existência de guardas de segurança [Champlain 2003].

A componente humana adjacente aos guardas na organização permite que se observe detalhes que o sistema de segurança informático tenha ignorado ou não tenha identificado como ameaça, sendo possível desta forma lidar com exceções ou eventos especiais. A única

desvantagem foca-se na possibilidade de estes agentes da segurança serem suscetíveis a suborno ou conluio [Cannon 2008].

A juntar a este tipo de controlo, dever-se-á manter um dos mais antigos métodos de detetar uma violação física: o alarme. Os sistemas de alarme tratam-se do mínimo absoluto de uma segurança física, e poderão ser instalados com o fim de sinalizar que uma determinada porta foi aberta, por exemplo, ou que numa determinada área em certo período de tempo foi detetada a ocorrência de movimentos quando isso não era suposto acontecer [Cannon 2008].

Para além deste tipo de controlos, a localização dos centros de dados é um outro aspeto a considerar aquando o planeamento da segurança física [Silva et al. 2003]. Os equipamentos de processamento de dados requerem uma atenção especial uma vez que são um recurso valioso da organização que precisa de ser protegido. Idealmente, o centro de processamento de dados não deverá chamar qualquer tipo de atenção para os seus verdadeiros conteúdos, evitando suscitar algum interesse malicioso nas pessoas que estejam mais propícias a cometer roubo ou vandalismo [Cannon 2008]. Existem algumas orientações a ter em conta: o centro de processamento de dados não deverá ser construído num piso térreo, numa cave ou no último piso do edifício, uma vez que deve estar localizado na zona mais resguardada possível para a qual não existam quaisquer tipos de acessos diretos do exterior; os acessos existentes devem ser facilmente monitorizados; não deverão existir condutas de água ou de esgotos nas imediações do centro de dados; as condutas necessárias à alimentação de energia e ao processamento da atmosfera devem estar construídas dentro de chão ou teto falsos; os sistemas de alimentação elétrica deverão ser redundantes; e os sistemas de deteção e supressão de incêndios deverão ser apropriados à instalação [Silva et al. 2003].

Estes tipos de sistemas de deteção e supressão de incêndios poderão ser acionados por fumaça, fogo ou até mesmo calor, e a sua instalação deverá ser efetuada em locais estratégicos e monitorizados eletronicamente [Champlain 2003]. Existem três tipos base de detetores de incêndios: deteção de fumaça, através de detetores óticos ou radioativos; deteção de calor, através de um termostato de temperatura fixa que ativa acima dos 200 graus ou detetando um rápida ascensão da temperatura em questão de minutos; e deteção de chama, acionado através da radiação violeta ou da pulsação de uma chama. Normalmente, o sistema de deteção de incêndios, ativa um alarme para iniciar a resposta humana ou aciona o sistema de supressão de fogo, que pode ou não envolver descarga de água ou produtos químicos.

Todavia, a deteção de incêndios não deverá ser a única preocupação no que toca a controlos ambientais no interior da instalação de processamento [Cannon 2008]. Este tipo de instalações requer um ambiente fresco, seco e livre de poeira [Champlain 2003]. Dever-se-á implementar sistemas de deteção de temperatura, para esta não estar demasiado alta mas também para esta não arrefecer em demasia, afetando os sistemas assim como as pessoas que trabalham diretamente com os mesmos. A ventilação será uma boa aposta para manter os equipamentos

informáticos arrefecidos, e o ar condicionado garante que a humidade esteja controlada evitando dessa forma a eletricidade estática [Cannon 2008].

Outra preocupação em termos físicos está associada à existência de água neste tipo de imediações. A água pode destruir computadores e causar curto-circuitos, o que poderá interferir com a fonte de alimentação de energia. Como tal, deverão existir detetores de água montados em todos os andares, nas áreas informatizadas e nas adjacentes, e devem ser montados no chão falso e no teto também. Idealmente deveria existir dois sensores de água com diferentes alturas. O primeiro soaria o alarme, o segundo desligaria a alimentação de energia do equipamento informático, mitigando danos e prevenindo também a perda de vidas [Musaji 2001].

No geral, a falta de fonte de alimentação elétrica é uma das situações mais graves a evitar pois poderá interferir com as operações a serem levadas a cabo na organização. Uma vez que a energia elétrica é a força vital dos equipamentos computorizados, a fonte de alimentação deverá ser ininterrupta [Cannon 2008]. Um sistema de alimentação de emergência e um sistema de alimentação ininterrupta, também conhecido como UPS (*uninterruptible power supply*), devem estar planeados em todas as instalações de processamento de informação.

O sistema de alimentação de emergência é constituído por um gerador e pelo *hardware* necessário para fornecer energia elétrica às zonas críticas operacionais para que continuem em funcionamento. Em caso de falha de energia, o seu acionamento deve ser automático. Um sistema UPS trata-se de um conjunto de baterias e componentes de suporte de *hardware* que irão fornecer potência suave e contínua aos equipamentos de informática até que o sistema de alimentação de emergência possa ser ativado completamente, evitando assim que a falha de energia interfira com as operações em andamento ou que cause algum tipo de perda de dados [Champlain 2003].

Tendo em consideração estas possibilidades de segurança física, podemos então planear a nossa segurança lógica [Oliveira 2001].

3.4.2 Segurança Lógica

Depois de termos garantida a segurança física dos diferentes ativos e recursos da organização, é indispensável garantir que a segurança lógica esteja de igual modo assegurada, pois a maior parte da informação em suporte digital encontra-se exposta a ataques [Silva et al. 2003]. A segurança lógica consiste em estabelecer barreiras e procedimentos que controlem o acesso aos dados e à informação, estando estes baseados em autorizações determinadas anteriormente [Carneiro 2009]. Estes controlos lógicos de segurança serão concebidos para o sistema de acordo com os diferentes graus de risco associados ao sistema. Logicamente, um sistema de alto risco obterá uma maior dedicação em termos de tempo e recursos do que um

sistema de baixo risco, uma vez que é fulcral criar controlos lógicos mais robustos [Champlain 2003].

Existe uma variedade de controlos lógicos elevada e, devido à constante evolução, as gerações tecnológicas e o seu aumento de complexidade tornam a segurança lógica numa das áreas mais ricas, complexas e difíceis de gerir. No entanto, podemos considerar que os controlos lógicos se dividem por três grandes áreas: prevenção, proteção e reação [Silva et al. 2003].

Uma das maiores preocupações de qualquer organização centra-se no acesso aos dados, mais especificamente, em quem tem autorização para aceder aos mesmos. A segurança lógica permite determinar quem é autorizado a aceder determinada área ou informação. Como tal, a identificação e autenticação dos utilizadores é um pré-requisito para todas as medidas de segurança [Cascarino 2007].

A identificação e autenticação trata-se de um processo que permite provar a identidade de determinado indivíduo. Esta informação é bastante útil no que toca à responsabilização dos indivíduos, pois interliga os mesmos às atividades registadas no sistema. Este processo é considerado a primeira linha de defesa na segurança lógica pois evita que pessoas não autorizadas acedam ao sistema ou à informação que o mesmo contém [ISACA 2010]. Estes dois conceitos descrevem momentos diferentes, sendo que a identificação se realiza quando o utilizador se dá a conhecer aos SI e a autenticação foca-se na análise e verificação que o SI irá realizar à informação fornecida pelo utilizador [Carneiro 2009]. Geralmente, a autenticação irá analisar algo que o utilizador saiba, algo que o utilizador possua ou alguma característica pessoal que o utilizador tenha, podendo utilizar estas técnicas isoladamente ou combinadas [ISACA 2010].

Carneiro [Carneiro 2009] aponta quatro dessas técnicas que permitem autenticar a identidade de um utilizador: exigir ao utilizador um elemento que somente ele saberá, por exemplo uma palavra-chave, uma chave criptográfica ou um PIN[5]; exigir a utilização de um objeto que o utilizador possua, como por exemplo um cartão magnético; apresentar características específicas do utilizador, desde impressões digitais a análise da iris, como exemplo; ou ainda requerer ao utilizador que efetue a leitura de um determinado elemento, sendo exemplo os padrões de escrita.

Este tipo de ideia de se descodificar determinados dados, que se verifica na última técnica referida, está também na base de um outro mecanismo muito utilizado na segurança lógica: a criptografia.

A criptografia está associada à ação de transformar uma certa mensagem numa outra ilegível, escondendo desta forma a mensagem inicial. Esta ação é conseguida através do uso de um

[5] PIN - Personal identification number

algoritmo com funções matemáticas e um código secreto especial. Este método irá permitir proteger a informação armazenada ou em trânsito, identificar pessoas que consigam o acesso à mensagem, pois são as que à partida têm acesso ao código secreto, e deter alterações de dados. No entanto, nada garante que um intruso apague todos os dados, mesmo que criptografados ou ainda que esse mesmo intruso modifique o programa por forma a conseguir alterar a chave secreta, o que não permitirá ao recetor descodificar a mensagem recebida [Oliveira 2001].

Existem duas possibilidades de utilização desta solução: a chave secreta (criptografia simétrica ou de chave única) e a chave pública/chave privada (criptografia assimétrica ou de duas chaves). Na primeira possibilidade, o mesmo código é utilizado para cifrar e decifrar os dados, sendo que na segunda possibilidade dá-se a existência de um par de chaves, uma chave pública e outra privada, estando as duas relacionadas entre si pois a primeira é utilizada para cifrar os dados e a segunda para os decifrar. No entanto, neste caso, a chave pública, como o próprio nome indica, é distribuída livremente e a chave privada será do exclusivo conhecimento do seu detentor [Silva et al. 2003]. Aquando a escolha das chaves dever-se-á ter em atenção de que por mais poderosa que seja a criptografia, a realidade é que os seus códigos podem ser decifrados [Oliveira 2001].

Problemas de controlo de acesso são bastante frequentes nas redes de computadores. Trata-se de um verdadeiro desafio, no qual de um lado temos os utilizadores que exigem facilidade de uso do sistema, e do outro os responsáveis pelo sistema que esperam que existam controlos mais rígidos para garantir a segurança. Para tal, têm sido desenvolvidos vários métodos para alcançar este objetivo.

O sistema *single sign-on* (ligação única) tem como finalidade melhorar os controlos de acesso à rede, implementando um sistema de segurança elevada que seja, no entanto, de fácil para o utilizador [Cannon 2008]. Mais especificamente a ideia centra-se no objetivo de consolidar todas as funções de administração, autenticação e autorização que se realizem na organização numa única função de administração centralizada. Com isto, a entidade evita que os utilizadores sejam obrigados a fornecer um conjunto diferenciado de credenciais para obter acesso ao sistema operacional ou a várias aplicações, situação tal que muitas vezes leva a momentos de esquecimento de senhas ou até mesmo a anotações das mesmas, aumentando assim os riscos de ocorrência de uma falha de segurança na organização [ISACA 2010].

Um dos exemplos mais comuns é *Kerberos*, um sistema de *single sign-on* desenvolvido pelo Instituto de Tecnologia de Massachusetts com o objetivo de melhorar a segurança e também a satisfação do utilizador [Cannon 2008]. *Kerberos* é um sistema de autenticação de rede, programado com criptografia forte, que oferece segurança nas transações entre clientes e servidores que se realizem em redes não seguras [Silva et al. 2003]. A operação de autenticação baseia-se no utilizador efetuar o login uma vez no *Kerberos,* sendo que

posteriormente o sistema autentica o utilizador e permite a este aceder a todos os recursos [ISACA 2010].

Uma outra forma de proteger as redes de computadores de ameaças internas e externas centra-se na utilização de *firewalls* [Cannon 2008]. Sempre que uma organização se conecta à internet enfrenta um perigo potencial, pois este tipo de conexão a tornará vulnerável a ataques. Assim sendo, as organizações deverão implementar um *firewall* nas suas redes como um meio de segurança de perímetro. No entanto, numa perspetiva de eficácia, os *firewalls* devem permitir que os indivíduos pertencentes à rede corporativa tenham acesso à internet e, ao mesmo tempo, impedir que hackers ou outros perpetuadores tenham acesso à rede e causem danos [ISACA 2010] Aliás, a principal vantagem do uso de *firewalls* regista-se no facto de estes reduzirem o acesso externo à rede [Cannon 2008]. Pela mesma lógica, devem-se aplicar *firewalls* aos sistemas mais sensíveis ou críticos da organização que precisam de ser protegidos de determinados utilizadores dentro da rede corporativa (hackers internos). Os *firewalls* tratam-se de dispositivos instalados em pontos estratégicos onde as conexões de rede têm associadas regras que permitem controlar o tipo de tráfego que entra e sai [ISACA 2010]. Este conceito, porém, gera uma falsa sensação de segurança, pois os *firewalls* só conseguem controlar o tráfego que passa diretamente por eles, não protegendo outros pontos de acesso.

Ainda no mundo inseguro da internet, as organizações provêm de um outro elemento que permite conectar vários utilizadores remotos através de uma rede pública. As redes privadas virtuais (VPN - *Virtual Private Network*) permitem estabelecer uma ligação virtual temporária, de forma rentável e altamente flexível. Visualmente, podemos imaginar um túnel criptografado que permite passar com segurança dados entre duas máquinas, de uma máquina para uma rede, ou entre duas redes [Cannon 2008]. Um dos requisitos destas redes virtuais privadas é o de esta deve estar definida ao pormenor, e somente o administrador da rede segura poderá adicionar ou remover participantes. É ainda função do administrador criar e manter regras que sejam suficientemente seguras no que toca a controlos de acesso à informação, baseando-se nas políticas de segurança da VPN existentes, que deverão ser claras o suficiente em termos de diferenciação de acordo com as necessidades de cada utilizador. O administrador deverá definir essas regras utilizando os diferentes privilégios de acessos registados nas políticas mas num modo em que não se interfira com a produtividade na organização.

Não faz sentido falar-se de ligações efetuadas pelo mundo da internet sem considerar-se a ameaça constante de vírus às redes das organizações. Todas as organizações deverão estabelecer soluções que se dediquem à deteção de vírus. Os antivírus contêm uma base de dados de excertos de códigos binários únicos de vírus, que através de um processo de comparação permitem identificar os vírus em questão. Este é um dos motivos para os quais este tipo de soluções deva ser atualizado constantemente [Silva et al. 2003].

Outro tipo de sistemas que tem uma função semelhante à da deteção de vírus é o sistema de deteção de intrusões (IDS - *Intrusion Detection System*), onde o objetivo foca-se em informar o

administrador de alguma suspeita de invasão ou de ataque que possa estar a ocorrer [Costa 2010]. Este tipo de sistemas existe desde que começamos a usar computadores, sendo exemplo a ação de um administrador a tentar descobrir indícios de comportamentos fora do normal enquanto acompanha a atividade da sua rede. Agora numa era mais moderna, temos sistemas computorizados a fazer esse acompanhamento e a permitir que se saiba o que se passa na infraestrutura informática da organização. Estes sistemas irão fornecer-nos a informação sobre o que se passa do lado de fora do perímetro da rede. Ou seja, em vez de simplesmente bloquearem os ataques, como fazem os *firewalls* ou os antivírus, eles irão saber exatamente o que aconteceu e o número de tentativas de intrusão oriundas do exterior que a rede da organização sofreu [Silva et al. 2003].

Estes são só alguns exemplos de segurança lógica que a organização pode aplicar na sua rede, no entanto este é um tema, como já referido, bastante rico e complexo, e existem muitas outras tecnologias, e cada vez serão mais, que a entidade pode utilizar para garantir a sua proteção.

4. Normas e Boas Práticas em Segurança da Informação

Após uma pequena introdução da importância das normas existentes na área de TSI, descreve-se de forma mais detalhada três dela: ISO27001, ITIL e COBIT. É, ainda, apresentada com um maior ênfase a estruturação do *framework* COBIT relativamente à área de segurança, nomeadamente a sua publicação COBI5SI, pois é a base do caso de estudo desenvolvido nesta dissertação.

4.1 Normas e Boas Práticas em 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].

Num contexto mais abrangente de TSI , o ITGI[6], o OGC[7] e o itSMF[8] [ITGI 2005] afirmam que seguir boas práticas em TSI é importante por vários motivos: a sua gestão é fulcral para o sucesso da estratégia do negócio; ajudam a garantir uma governança eficaz das atividades de TSI; a definição de um *framework* dentro da organização permite que toda a gente saiba o que fazer; e trazem para a organização diferentes benefícios, tais como menos erros, maior proveito, confiança dos parceiros de negócios e respeito por parte das entidades reguladoras. Estas mesmas organizações, com o objetivo de facilitar a aplicação de normas num contexto de negócio, alinharam as três normas mais adotadas na área de TSI: COBIT, ITIL e a ISO/IEC17799[9].

No âmbito de segurança da informação, existem diversas opções tais como: normas da série ISO27000[10]; lei SOX[11]; COBIT; COSO[12]; ITIL; etc [Arora 2010]. Estas definem os principais conceitos, princípios e componentes de gestão de segurança da informação, e oferecem

[6] ITGI - IT Governance Institute [http://www.itgi.org/]
[7] OGC - Office of Government Commerce
[8] itSMF - IT Service Management Forum [http://www.itsmfi.org/]
[9] ISO/IEC17799 - Norma que estabelecia diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação numa organização
[10] série ISO27000 - Família de normas ISO 27000 ajuda as organizações a manter os ativos de informação seguros.
[11] SOX - Sarbanes–Oxley Act [http://www.soxlaw.com/]
[12] COSO - Committee of Sponsoring Organizations of the Treadway Commission [http://www.coso.org/]

importantes referências às organizações para a aplicação apropriada dessa mesma gestão [Kajava et al. 2006].

No entanto, nem todas as normas especificam como é que as medidas de segurança podem ser aplicadas e encaixadas com a gestão e os processos dos SI, e, por essa razão, um gestor não deverá se concentrar exclusivamente na aplicação de uma só opção. Deverá sim avaliar os diferentes conjuntos de normas e diretrizes oferecidos, e analisar quais os que se adaptam e cobrem as necessidades da organização [Arora 2010]. Deverá ainda ter em consideração que as normas não se tratam somente de guias técnicos, e que para garantir uma aplicação o mais adequada possível, dever-se-á ter em consideração o contexto do negócio em que vão ser inseridas, e quais as áreas dentro da organização às quais a introdução das mesmas trará mais proveito [ITGI 2005]. Para isso, a escolha e aplicação das normas a seguir na organização não deverá ser feita sem o conhecimento da envolvente e práticas de negócio, e dos procedimentos de segurança da informação [Kajava et al. 2006].

Numa perspetiva de segurança da informação Turner et al. [Turner et al. 2008], baseando-se num inquérito realizado pela ESG[13], afirma que as normas e *frameworks* mais seguidos mundialmente nesta área são a ISO/IEC17799, o ITIL e o COBIT. Mais recentemente, e após algumas alterações na legislação existente na área de segurança da informação na ISO[14] que iremos explicar de seguida, 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].

4.1.1 ISO27001

A ISO27001 foi publicada inicialmente em Outubro de 2005 pela ISO e pela IEC[15] [FFIEC 2006], sendo uma das normas da série ISO27000, a qual junta um conjunto de normas focado na gestão dos SGSI [Pelnekar 2011]. Em 2013, foi publicada a segunda versão da ISO27001, sendo esta uma revisão da versão publicada em 2005 [BSIgroup 2014].

Inicialmente, esta norma era conhecida como BS7799[16]. No entanto, quando a ISO decidiu incluir um conjunto de normas que se concentrassem na gestão dos SI, e por forma a incluir, no novo conjunto de normas, uma que tratasse da gestão da segurança da informação, esta norma foi incluída na série ISO27000 com a denominação de ISO27001 [Arora 2010]. Em Julho de 2007, o mesmo aconteceu com a originalmente chamada ISO/IEC17799, que sofreu uma

[13] ESG - Enterprise Strategy Group [http://www.esg-global.com/]
[14] ISO - International Organization for Standardization [http://www.iso.org/iso/home.htm]
[15] IEC - International Electrotechnical Commission [http://www.iec.ch/}
[16] BS7799 - Norma publicada pelo BSIgroup que apresenta orientações para a gestão de riscos de segurança da informação

renumeração para ISO27002[17] [Turner et al. 2008], na qual se pode encontrar o código de conduta e as práticas recomendadas que podem ser usadas tendo em vista o cumprimento das especificações da ISO27001 [Calder 2013]. Estas duas normas fazem parte da família da série ISO27000, como se pode constatar na figura 4.1.

Figura 4.1 **Normas incluídas na ISO27000 series [ISO 2013]**

A ISO27001 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]. É preciso, também, ter em consideração a influência que os objetivos e necessidades da organização, os requisitos de segurança, os processos usados e o tamanho e estrutura da organização têm na definição e implementação desse SGSI. Este, 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].

Antes da revisão, a ISO27001 e a ISO27002 detalhavam 133 medidas de segurança, as quais estavam organizadas por 11 seções [Pelnekar 2011]. Nas publicações de 2013, verifica-se uma reestruturação. Na ISO27001:2013, está referido que os objetivos de controlo e os controlos são diretamente derivados da ISO27002:2013, na qual iremos agora encontrar 114 controlos e 14 secções [BSIgroup 2014].

[17] ISO27002 - Norma internacional que apresenta o código de boas práticas para os controlos de segurança da informação

Para além disso, é de referir que na sua versão de 2005, a ISO27001 apresentava o modelo PDCA[18] para que as organizações o aplicassem com o objetivo de estruturar todos os processos do SGSI [ISO 2005], e na publicação de 2013 refere que outras metodologias poderão ser usadas pelas organizações para essa estruturação. Isto deve-se ao facto de que esta nova versão apresenta como um dos requisitos a melhoria contínua, e o modelo PDCA é só uma abordagem para atingir esse mesmo requisito [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 está em conformidade com esta norma internacional [ISO 2013].

A certificação assegura 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[19], a ISO14001[20] e a série ISO20000[21], 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].

4.1.2 ITIL

Publicada entre 1989 e 1995 pela CCTA[22], que se encontra agora integrada no OGC [ITGI 2005], e com a sua utilização inicialmente confinada ao Reino Unido e Holanda [Cartlidge et al. 2007], a ITIL fornece orientações aos prestadores de serviços de TSI, garantindo que o valor

[18] PDCA - O modelo Plan-Do-Check-Act apresenta um ciclo de quatro fases (planear, implementar, verificar, agir) para a realização de mudanças e para a melhoria contínua.
[19] ISO9001 - Norma internacional que apresenta critérios para um sistema de gestão da qualidade adequado
[20] ISO14001 - Norma internacional que apresenta critérios para um sistema de gestão ambiental adequado
[21] série ISO20000 - Família de normas internacionais que tratam sistemas de gestão de serviços
[22] CCTA - Central Communications and Telecommunications Agency

do negócio seja protegido [Meijer et al. 2011], apresentando métodos eficazes e eficientes de prestação de serviços de TSI [ITProcessMaps 2013].

Esta versão inicial consistia num conjunto de 31 livros que previam cobrir todos os aspetos da prestação de serviços de TSI. Após a sua revisão, foi então publicada uma segunda versão, sendo esta última, um produto mais direcionado, com menos livros, e com uma forte orientação para os processos requeridos para uma entrega eficaz dos serviços aos clientes [TSO 2007]. Em 2007 foi publicada uma versão melhorada da libratia ITIL que se concentra em cinco seções fundamentais do ciclo de vida de um serviço, representados na figura 4.2. Este ciclo de vida parte da definição e análise dos requisitos do negócio nas fases de estratégia e de *design* 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]. Em 2011, foi publicado um *update* da ITIL, baseado no feedback dos utilizadores, que se focou principalmente na correção de erros e inconsistências encontrados [ITProcessMaps 2013].

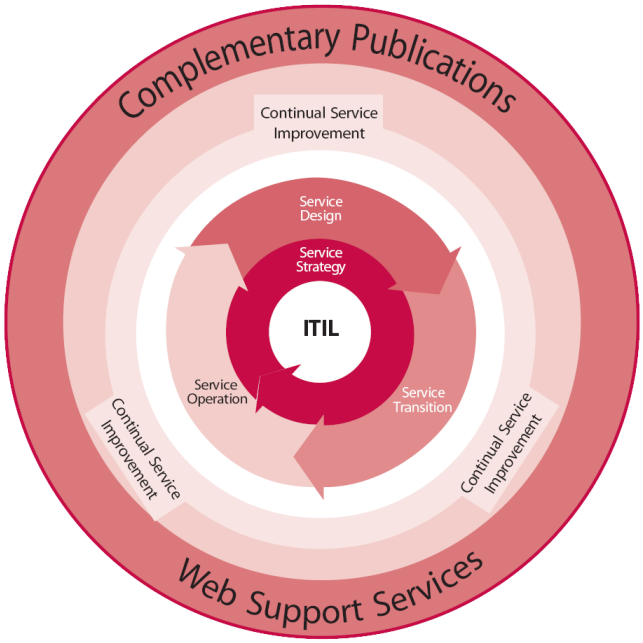


Figura 4.2 Ciclo de Vida de um Serviço - ITIL versão 3 [TSO 2007]

Cartlidge et al.[Cartlidge et al. 2007] apontam as seguintes vantagens na utilização desta libraria:

- Aumento da satisfação do utilizador e consumidor dos serviços dos SI;
- Melhoria na disponibilidade do serviço que consequentemente leva a um aumento dos lucros e receitas da organização;

- Redução de perdas de tempo e de repetição de operações e melhoria no uso e gestão de recursos que conduz a uma poupança a nível financeiro;
- Melhor perceção relativamente à altura indicada para o lançamento de novos produtos e serviços;
- Melhoria na tomada de decisão e na otimização do controlo dos riscos;

A ITIL está estruturada num ciclo, com cinco etapas, que gere os serviços de TSI e apoia os resultados do negócio. Nessas cinco etapas, a libraria 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].

Ao contrário do que se encontrava na versão 2, atualmente a ITIL não publica em separado um documento sobre gestão da segurança. 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, uma vez que, dentro da filosofia defendida pela ITIL, a consciência e consideração dos riscos de segurança são obrigações em todos os passos da gestão de serviços de TSI. Ainda assim, a maior referência a este tema é dada na publicação da Conceção do Serviço (Service Design), na seção 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. A ITIL 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, a libraria 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].

4.1.3 COBIT

O ISACA, juntamente com o ITGI, 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].

Após a primeira publicação em 1996, seguiu-se uma segunda edição em 1998, e uma terceira em 2000. Em dezembro de 2005, é lançada a quarta edição, que após uma revisão, é atualizada em 2007 para a versão 4.1 do COBIT [Seeram 2012]. Esta versão contém um conjunto de 34 processos de controlo de alto nível, para os quais estão definidos objetivos de controlo detalhados, e que se encontram agrupados em 4 domínios, sendo estes Planear e Organizar (PO - *Plan and Organize*), Adquirir e Implementar (AI - *Acquire and Implement*), Entregar e Suportar (DS - *Deliver and Support*) e Monitorizar e Avaliar (ME - *Monitor and Evaluate*) [Santos 2009].

A versão 5.0 foi lançada em Abril de 2012 [Seeram 2012], aumentando o seu foco nas diferentes partes interessadas e na interseção entre negócio e TSI, para além de deixar de ter objetivos de controlo e passar sim a apresentar processos de gestão. 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, 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; capacidades do serviço; 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, ilustrados na figura 4.3. 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].

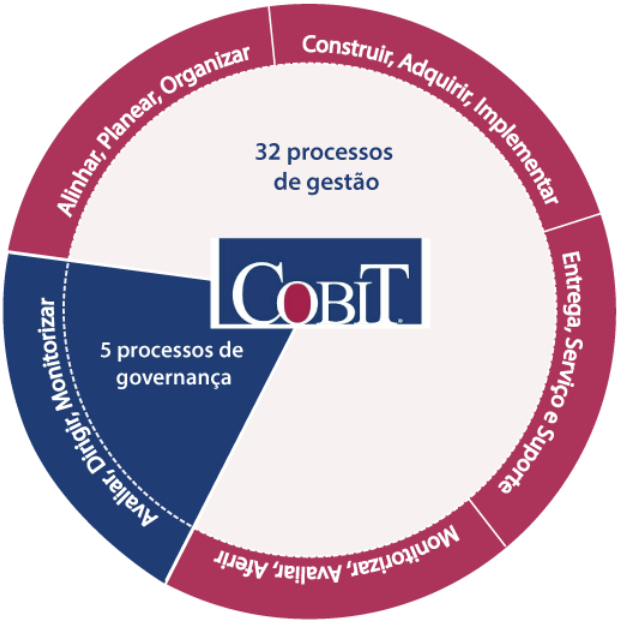


Figura 4.3 Domínios e processos do COBIT entre as áreas de governança e gestão [ISACA 2012]

O COBIT fornece um conjunto de boas práticas, mais focadas nos controlos a aplicar e não tanto na sua execução, que ajudam a otimizar os investimentos na área das tecnologias da informação, a assegurar a entrega dos serviços e a estabelecer métricas que permitam avaliar o que correu mal quando as coisas não correm como esperado [ITGI 2007].

Nele está reunida toda a informação que as organizações necessitam de adotar no caso de pretenderem implementar uma estrutura de governança e de controlo de TSI, sendo que esta se encontra estruturada através de domínios e processos e segue uma lógica e gestão que visam ajudar a otimizar os investimento de TSI [ITGI 2007]. 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].

O COBIT contribui para as necessidades da empresa ao interligar os requisitos do negócio e os objetivos de TSI, identificando os principais recursos de TSI, fornecendo ferramentas para a gestão, fornecendo métricas que permitem adquirir o nível de desempenho de TSI e clarificando responsabilidades e papéis a ter em conta no desenrolar dos processos de TSI [ITGI 2007]. Visa, também, que deve existir uma preocupação com a organização na totalidade, não estando exclusivamente focado na função de tecnologias de informação mas abrangendo todas as funções e processos dentro da empresa [ISACA 2012].

Na sua última versão, o COBIT, pode-se encontrar uma publicação mais focada na segurança da informação: o COBIT5SI [ISACA 2012]. Uma vez que o caso de estudo desenvolvido nesta dissertação se baseia neste documento, este será apresentado de forma mais detalhada na secção 4.1.3.1.

4.1.3.1 COBIT 5 para a Segurança da Informação

O ISACA publicou o COBIT5SI, sendo esta a publicação que providencia com mais detalhe as melhores práticas para os profissionais da área de segurança da informação e outras partes interessadas dentro da organização. Para o ISACA, a segurança da informação garante que dentro da organização a informação está protegida contra a divulgação a utilizadores não autorizados (confidencialidade), contra a alteração inapropriada (integridade) e contra a falta de acesso quando este é necessário (disponibilidade). Cobrindo o conceito CIA (*Confidentiality, Integrity and Availability*), a segurança da informação transforma-se numa vantagem competitiva para qualquer organização, seja por garantir a confiança das partes interessadas, por abordar o risco de negócio ou pela criação de valor para a organização [ISACA 2012].

Os principais motivos para o desenvolvimento do COBIT5SI passam pela necessidade de: existir uma descrição de segurança da informação que, num contexto empresarial, tenha em conta as responsabilidades de segurança, não só na área de TSI como também em todas as outras funções dentro da organização, cobrindo todas as áreas da mesma; estabeleça uma relação com os objetivos da organização; e vise atingir uma governança e gestão eficazes de segurança da informação [ISACA 2012]. O ISACA refere também a necessidade de: manter as informações dentro de um nível de risco aceitável; assegurar a disponibilidade dos serviços e sistemas de forma continuada para os *stakeholders*, internos ou externos, garantindo a satisfação do utilizador de serviços de TSI; cumprir com o crescente número de leis e regulamentos e providenciar transparência relativamente a esse mesmo cumprimento; e conseguir que o custo de serviços de TSI e de proteção de tecnologia seja contido.

Devido à existência de várias normas associadas a esta área, o COBIT5SI surge para alinhar e conectar as diferentes normas de alto nível que existem no mercado, ajudando a compreender

como os vários *frameworks*, boas práticas e normas estão posicionadas em relação às outras e como podem ser utilizadas juntamente e de forma complementar com o COBIT5SI [ISACA 2012].

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. No facilitador Políticas, Princípios e *Frameworks* de segurança da informação encontramos 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. Para uma melhor compreensão, é necessário que os mesmos existam num número limitado e tenham uma linguagem clara.

Em 2010, o ISACA, o ISF[23] e o ISC[24] uniram-se para desenvolver 12 princípios independentes que visam ajudar os profissionais de segurança da informação a adicionar valor às suas organizações [ISACA 2012]. Esses princípios estão divididos em três módulos, especificadas na tabela 4.1**.** No módulo de suporte ao negócio define-se como princípios: foco no negócio; fornecer qualidade e valor aos *stakeholders*; cumprir com os requisitos legais e regulamentares relevantes; fornecer informações oportunas e precisas sobre o desempenho da segurança da informação; avaliar atuais e futuras ameaças à informação; e promover a melhoria contínua da segurança da informação. No que toca à defesa do negócio, dever-se-á: adotar uma abordagem baseada no risco; proteger a informação confidencial; concentrar-se nas aplicações de negócio mais críticas; e desenvolver sistemas de forma segura. Relativamente à promoção de um comportamento de responsabilidade de segurança da informação, estão definidos como princípios: agir de forma ética e profissional; e fomentar uma cultura positiva de segurança da informação. A descrição dos diferentes princípios pode ser encontrada no anexo II.

[23] ISF - Information Security Forum [https://www.securityforum.org/]
[24] ISC^2 - International Information System Security Certification Consortium [https://www.isc2.org/]

PRINCÍPIOS
Suporte ao Negócio
Foco no Negócio
Fornecer qualidade e valor aos stakeholders
Cumprir com os requisitos legais e regulamentares relevantes
Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação
Avaliar atuais e futuras ameaças à informação
Promover a melhoria contínua da segurança da informação
Defender o Negócio
Adotar uma abordagem baseada no risco
Proteger informação confidencial
Concentrar-se nas aplicações de negócio críticas
Desenvolver sistemas de forma segura
Promover um comportamento responsável de segurança da informação
Agir de forma ética e profissional
Fomentar uma cultura positiva de segurança da informação

Tabela 4.1 Princípios recomendados no COBIT5SI (adaptada de [ISACA 2012])

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, como constatado na tabela 4.2**.** Em termos de políticas no âmbito das funções diretamente relacionadas com a segurança da informação, sugere-se a definição de: controlo de acesso; pessoal de segurança da informação; meio físico e ambiental de segurança da informação; e resposta a incidentes. Relativamente a outras funções dentro da organização, sugere-se como políticas a definir na organização: continuidade do negócio e recuperação de desastres; gestão de ativos: regras de comportamento (uso aceitável); aquisição, desenvolvimento e manutenção de *software*; gestão de fornecedores; gestão das operações e da comunicação; conformidade; e gestão de risco. A descrição das diferentes políticas pode ser encontrada no anexo II.

POLÍTICAS
Impulsionadas pela função de segurança da informação
Controlo de acesso
Pessoal de segurança de informação
Meio físico e ambiental de segurança de informação
Resposta a incidentes
Impulsionadas por outras funções dentro da organização
Continuidade do negócio e recuperação de desastres
Gestão de ativos
Regras de comportamento (uso aceitável)
Adquirir sistemas de informação, desenvolvimento e manutenção de software
Gestão de fornecedores
Gestão das operações e da comunicação
Conformidade
Gestão de Risco

Tabela 4.2 Políticas recomendadas no COBIT5SI (adaptada de [ISACA 2012])

Respetivamente ao facilitador Processos, este descreve um conjunto de práticas e atividades para atingir os objetivos da organização. Esse conjunto, como pode ser verificado na figura 4.4, é constituído por 37 processos que se encontram divididos inicialmente por duas áreas de atuação, governança e gestão, sendo depois divididos pelos 5 domínios já referidos anteriormente: EDM, APO, BAI, DSS e MEA.

Destes 37 processos, dois deles, no âmbito geral do COBIT, estão associados à segurança da informação: APO13 Gestão da Segurança, e DSS05 Gestão de Serviços de Segurança. No âmbito da publicação COBIT5SI, é apresentada informação específica de segurança relacionada com os diferentes processos de governança e gestão apresentados no COBIT. Cada processo está estruturado, no Anexo B desta publicação, providenciando a seguinte informação: identificação do processo - número, nome, área e domínio; descrição do processo - o que o processo faz; propósito do processo - o que o processo visa alcançar; objetivos e métricas do processo - quais os objetivos do processo e quais as métricas adjacentes a cada um desses objetivos; descrição detalhada das práticas do processo - apresentação dos *inputs* e outputs das práticas relacionadas com segurança da informação, informando origem e destino respetivamente, assim como das atividades específicas de segurança da informação desse mesmo processo. As descrições dos diferentes processos podem ser encontradas no anexo III da presente dissertação.

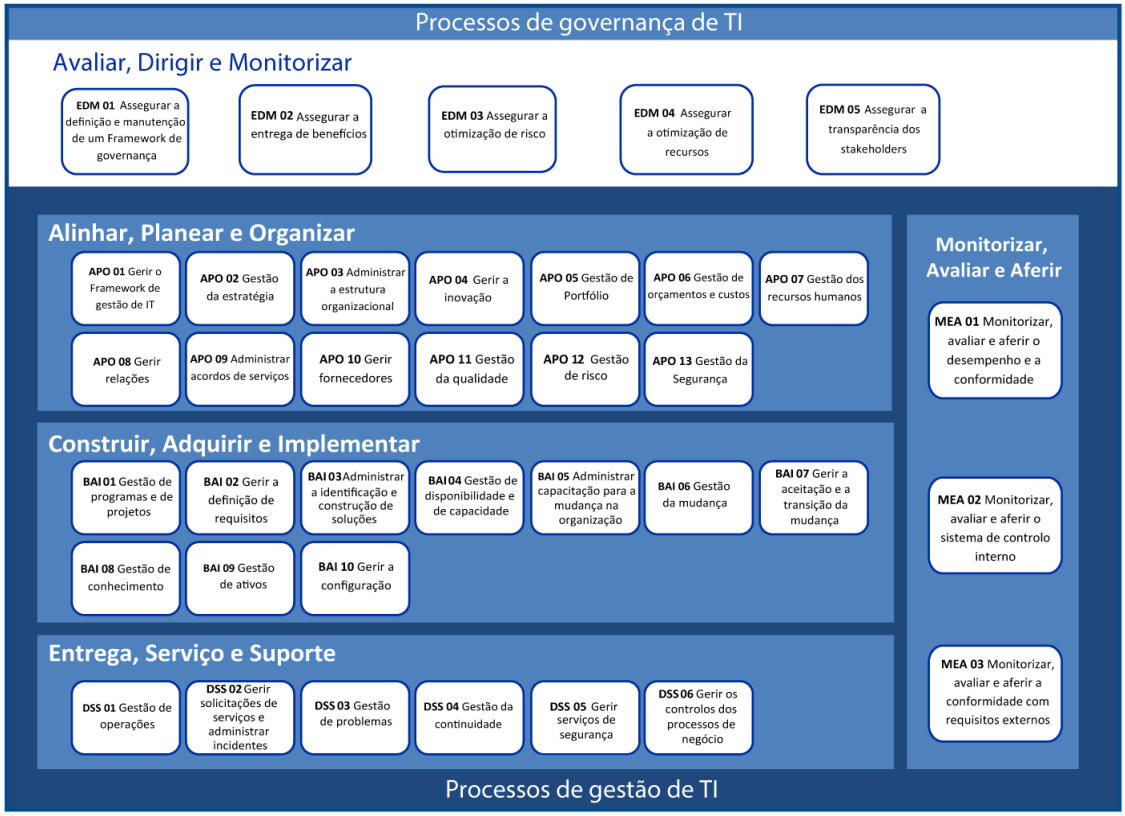


Figura 4.4 Representação dos 37 processos do COBIT e adjacentes domínios (adaptada de [ISACA 2012])

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 pretende que seja executado um conjunto de práticas associadas às diferentes funções, que ofereçam como resultado à organização a tomada de boas decisões. O COBIT5SI, sugere a existência de certas funções ou estruturas dentro da organização que estejam diretamente relacionadas com a segurança da informação, especificadas na tabela 4.3**.** Podemos encontrar no Anexo C do COBIT5SI, informação referentes à composição, mandato, principais operações, esfera de controlo e nível de autoridade, assim como os *inputs* e *outputs* que se esperam das seguintes funções ou estruturas de segurança da informação: diretor de segurança da informação (CISO - *Chief Information Security Officer*); comité de direção de segurança da informação (ISSC - *Information Security Steering Committee*); gestor de segurança da informação (ISM - *Information Security Manager*); comité de gestão de risco da organização (ERMC - *Enterprise Risk Management Committee*); responsáveis pela informação. Para além destas informações, no anexo C, encontra-se um conjunto de práticas pelas quais as diferentes funções ou estruturas organizacionais deveriam estar encarregadas ou serem responsabilizadas seguindo

a lógica do mapa RACI[25] (responsável, responsabilizado, consultado ou informado). Este mapa permite identificar qual o envolvimento que as diferentes funções têm com os projetos em causa [ISACA 2012]. As descrições das diferentes funções podem ser encontradas no anexo IV da presente dissertação**.**

FUNÇÕES / ESTRUTURAS ORGANIZACIONAIS
Diretor de Segurança da Informação (CISO)
Comité de Direção de Segurança da Informação (ISSC)
Gestor de Segurança de Informação (ISM)
Comité de Gestão do Risco do Negócio (ERM - Enterprise Risk Management)
Responsáveis pela Informação / Proprietários da empresa

Tabela 4.3 Funções e/ou estruturas organizacionais recomendadas pelo COBIT5SI (adaptada de [ISACA 2012])

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. Como se pode ver na tabela 4.4, COBIT5SI sugere que a segurança da informação deve ser praticada diariamente em todas as operações, e que as pessoas devem respeitar as políticas e os princípios, para além de ter presente que toda a gente é responsável pela proteção da informação da organização. As pessoas têm acesso a uma quantidade de orientação suficiente e detalhada e são incentivadas a participar, e inclusive questionar, a situação atual da segurança da informação. Os *stakeholders* devem saber como identificar e responder às ameaças das empresas e deve ser fomentada uma gestão proactiva que visa o suporte a inovações, e uma gestão de negócios que se envolva numa colaboração interfuncional contínua para conceder programas de segurança da informação eficazes e eficientes. Sugere, ainda, que a gestão executiva deve reconhecer o valor que a segurança da informação tem para o negócio.

[25] RACI - Responsible, Accountable, Consulted, Informed

COMPORTAMENTOS DESEJADOS
Segurança da Informação é praticada diariamente nas operações
As pessoas respeitam as políticas e os princípios
É providenciada orientação suficiente e detalhada às pessoas e estas são encorajadas a participar e a desafiar a situação atual
Toda a gente é responsabilizada pela proteção
Os stakeholders identificam e respondem às ameaças da organização
A gestão de topo apoia e antecipa inovações de forma proativa
A gestão do negócio empenha-se na obtenção de uma colaboração interfuncional contínua
A gestão executiva reconhece o valor do negócio

Tabela 4.4 Comportamento considerados no COBIT5SI como desejados numa organização (adaptada de [ISACA 2012])

Como já constatado anteriormente, a informação é um recurso valioso para as organizações, e trata-se de um dos facilitadores apresentados pelo ISACA. No COBIT5SI, são analisados os diferentes tipos de informação de segurança relevantes, que podem ser consultados na tabela 4.6, assim como a relação entre estes e os *stakeholders*. Mais propriamente, quais são os *stakeholders* que aprovam, originam, são informados, ou utilizam os diferentes tipos de informação [ISACA 2012]. A listagem de *stakeholders* sugerida no COBIT 5 para a Segurança da Informação pode ser consultada na tabela 4.5**.**

STAKEHOLDERS
Interno: Organização
Conselho
Presidente e Diretor Executivo (CEO - *Chief Executive Officer*)
Diretor Executivo de Finanças (CFO - *Chief Financial Officer*)
Diretor das Operações (COO - *Chief Operating Officer*)
Diretor de Risco (CRO - *Chief Risk Officer*)
Comité de Direção de Segurança da Informação (ISSC)
Diretor de Segurança da Informação (CISO)
Executivos
Sócios
Comités de Direção de Projetos e Programas
Direção da Estrutura
Comité de Gestão do Risco do Negócio (ERM - *Enterprise Risk Management*)
Chefe de Recursos Humanos
Consultoria
Auditoria
Gabinete de gestão de projetos e programas (PMO - *Project Management Office*)
Gabinete de gestão de valor (VMO - *Value Management Office*)
Interno: TSI
Comité de Estratégia de TSI
Diretor da Informação (CIO - Chief Information Officer)
Chefe de Estrutura
Chefe de Desenvolvimento
Chefe das Operações TSI
Chefe de Administração de TSI
Gestor de Serviços
Gestor da Segurança da Informação (ISM)
Gestor da Continuidade de Negócio
Diretor da Privacidade
Externo
Investidores
Seguradoras
Autoridade Legal
Reguladoras
Parceiros do Negócio
Vendedores/Fornecedores
Auditores Externos

Tabela 4.5 Stakeholders que o COBIT5SI prevê existirem numa organização (adapatada de [ISACA 2012])

O ISACA aponta como tipo de informação relacionada com a segurança a estratégia de segurança da informação, o seu orçamento, plano, requisitos, políticas e materiais de consciencialização, relatórios de avaliação e perfil de segurança da informação assim como seu o painel de incidentes. É ainda referido o ciclo de vida da informação, a partir da perspetiva de segurança, que inicia-se no planeamento e organização da informação, seguindo-se pelo uso da mesma. Posteriormente dá-se a monitorização dessa mesma informação para garantir que a informação ainda é viável, sendo que a fase final do ciclo de vida da informação se dá com o seu arquivo ou exclusão [ISACA 2012]. A descrição dos diferentes documentos de segurança da informação pode ser consultada no anexo V.

TIPOS DE INFORMAÇÃO
Estratégia de Segurança da Informação
Orçamento da Segurança da Informação
Plano de Segurança da Informação
Políticas
Requisitos de Segurança da Informação
Material de Consciencialização
Relatórios de Revisão de Segurança da Informação
Perfil de Risco da Informação
Painel de Segurança da Informação

Tabela 4.6 Tipos de Informação de segurança da informação que o COBIT5SI recomenda (adaptada de [ISACA 2012])

Para que seja possível desenvolver serviços, infraestruturas ou aplicações é necessário identificar quais os recursos que são necessários para garantir a segurança da informação e as funções relacionadas à mesma. O COBIT5SI identifica uma lista de serviços relacionados com a segurança (tabela 4.7) que têm um grande potencial de aparecer num catálogo de serviços de segurança, e para cada um deles apresenta descrições detalhadas, atributos e objetivos. O ISACA estabelece que fornecer uma arquitetura e proporcionar a consciencialização da segurança, fornecer avaliações de segurança e respostas adequadas a incidentes, assim como proteger a organização de forma adequada contra *malware*, ataques externos e tentativas de intrusão, e providenciar serviços de monitorização e de alerta para eventos relacionados com a segurança, seriam serviços de segurança que deveriam constar no catálogo de segurança de uma organização [ISACA 2012].

CATÁLOGO DE SERVIÇOS
Arquitetura de segurança
Consciência de segurança
Desenvolvimento seguro
Avaliações de segurança
Sistemas adequadamente configurados e seguros
Acessos dos utilizadores, consoante os direitos estabelecidos
Proteção adequada contra ataques externos e tentativas de intrusão
Resposta adequada a incidentes
Testes de segurança
Serviços de monitorização e alerta

Tabela 4.7 Serviços de segurança recomendados pelo COBIT5SI (adaptada de [ISACA 2012])

Por último, para que a função de segurança da informação dentro da organização seja operacionalizada de forma eficaz, é necessário que os colaboradores que tenham ações relacionadas com essa função tenham os conhecimentos e experiência adequados. No sétimo facilitador, pessoas, *skills* e competências, o COBIT5SI apresenta sugestões de *skills* e competências que devem ser cobertas pelos colaborados da organização, registadas na tabela

4.8. Os colaboradores a exercer funções na área de segurança da informação, deveriam ter conhecimentos de governança e formulação de estratégia de segurança da informação assim como de gestão de risco da própria informação. Habilidade em desenvolver a arquitetura e as operações de segurança da informação, assim como a realização da avaliação, testes ou observância da informação é também uma mais-valia referida no *framework* de boas práticas. Para ajudar na perceção dos diferentes *skills* e competências, o COBIT5SI apresenta a definição, atributos e metas de cada um deles.

SKILLS / COMPETÊNCIAS
Governança de segurança da informação
Formulação da estratégia de segurança da informação
Gestão de risco da informação
Desenvolvimento da estrutura de segurança da informação
Operações de segurança da informação
Avaliação, testes e observância da informação

Tabela 4.8 Skills e Competências que o COBIT5SI considera importantes serem cobridas pelos colaboradores da organização (adaptada de [ISACA 2012])

4.1.4 ISO27001, ITIL e COBIT e a Segurança da Informação

No decorrer da revisão bibliográfica, foi possível apurar algumas diferenças entre o conjunto de normas apresentado.

Verifica-se que estas surgiram em anos diferentes e foram impulsionadas por diferentes organizações, tendo sofrido ao longo dos anos revisões para que se fossem adaptando à realidade organizacional. A atualização mais recente foi efetuada pela ISO27001, em 2013, sendo que a última versão da ITIL corresponde ao ano de 2011, quando publicaram uma atualização da versão 3, e a última publicação do COBIT data a 2012. Estes últimos *frameworks*, nas suas publicações, referem que se encontram alinhados à norma internacional ISO27001, para que seja possível que as organizações as possam aplicar em conjunto. No entanto, note-se que este alinhamento demonstrado nestes *framework* é adjacente à publicação de 2005 da norma ISO27001, sendo que é possível que seja necessário haver uma atualização dos *frameworks* ITIL e COBIT para que possam continuar alinhados com as mudanças efetuadas.

É também de notar que estes normativos apresentam estruturas diferentes, nas quais incluem a área de segurança. Na figura 4.5. pode-se verificar que a ISO27001 sendo a norma internacional que visa cobrir a gestão da segurança da informação, juntamente com a ISO27003, tem toda a sua estrutura focada nesta área. Por sua vez, a ITIL apresenta um processo de SGSI, que é considerado ao longo das diferentes etapas do ciclo de vida de um serviço apresentadas nos seus 5 livros, mas que recebe um maior cuidado na secção 4.6 do livro *Service Design*. No caso do COBIT, existe uma publicação, COBIT5SI, na qual o ISACA

faz a ponte entre a área de segurança da informação com os sete facilitadores que considera ajudarem à realização de uma governança e gestão adequadas.

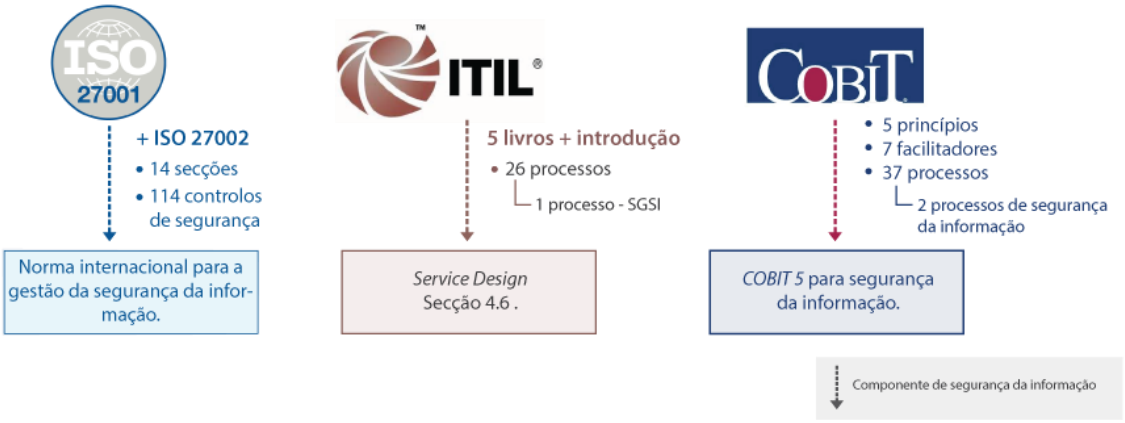


Figura 4.5 Estruturas e adjacentes componentes de segurança da ISO27001, do ITIL e do COBIT

Como já referido, tanto a norma internacional ISO27001 como os *frameworks* de boas práticas ITIL e COBIT apresentam ações que permitem às organizações o desenvolvimento de um SGSI apropriado. No entanto, numa perspetiva geral, o âmbito em que surgem não é o mesmo. Enquanto que a libraria ITIL surge com o intuito de dar orientações na gestão de serviços de TSI, o COBIT tem como foco a gestão e governança de TSI, permitindo um alinhamento com as restantes áreas da organização. Por sua vez, a ISO27001 está muito mais focada na própria gestão da segurança da informação. Estas diferenças podem ser percecionadas também nos objetivos adjacentes a cada um deles, como poderá ser constatado na figura 4.6**.**

Figura 4.6 Âmbitos e objetivos da ISO27001, do ITIL e do COBIT

Numa perspetiva de utilização desta norma e destes *frameworks* de boas práticas dentro das organizações, [Arora 2010] apresenta uma comparação entre o COBIT e a ISO27001, onde conclui que o COBIT apresenta uma solução de gestão de segurança de informação completa ao contrário do que acontece com a norma ISO27001. Por sua vez, Stroud [Stroud 2010] compara os *frameworks* ITIL e COBIT, afirmando 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.

Numa análise global, e mantendo o foco na área de segurança da informação, verifica-se que 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 esteja alinhada com os objetivos de negócio da organização. Por sua vez, 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. Por último, a ISO27001, como norma internacional 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.

5. Abordagem de Investigação

De seguida, encontram-se estruturados e detalhados os objetivos que se pretendeu atingir com o desenvolvimento deste trabalho de dissertação, apresentando as metodologias, métodos e técnicas que foram utilizados para obter esses mesmos objetivos.

5.1 Objetivo do Trabalho de Investigação

O trabalho desenvolvido nesta dissertação divide-se em duas partes, tendo uma delas natureza teórica e a outra natureza prática.

Em termos teóricos, teve-se como objetivo identificar as diferentes normas ou *frameworks* de boas práticas que se poderiam aplicar nas organizações na área de TSI, e, numa fase seguinte, identificar os normativos que seriam os mais utilizados na área da segurança da informação, pois esta é o centro da presente dissertação.

Após efetuada a identificação das normas e *frameworks* de segurança da informação, planeou-se desenvolver uma análise de cada um desses normativos, a qual se utilizaria para apresentar uma visão final, onde se poderia encontrar referências às diferentes origens, progressões, âmbitos, objetivos, estruturas e componentes de segurança. O objetivo passou por conseguir realçar o papel que cada um dos normativos poderia representar, por forma a garantir que as organizações que os apliquem obtenham a implementação de um sistema de gestão de segurança da informação adequado.

Em termos práticos, o principal objetivo passava por analisar uma organização relativamente à sua área de segurança da informação, apostando numa avaliação ao sistema de gestão e não tanto numa avaliação mais técnica. Assim, e após a escolha de um normativo para utilizar por base na estruturação da análise referida, preparou-se a realização de uma comparação entre as orientações providenciadas por esse normativo 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.

5.2 Abordagem Metodológica

Perante os objetivos de natureza teórica, iniciou-se uma pesquisa de literatura sobre as áreas de conhecimento mais relevantes para o desenvolvimento deste projeto. Após efetuar-se a revisão bibliográfica e filtrar-se a informação através de uma forte componente de leitura, deu-se a preparação de uma pesquisa de dados que nos permitisse dar seguimento ao estudo.

Como em qualquer pesquisa, existe uma fase de recolha de dados para posterior análise, e pode-se apontar, neste sentido, dois tipos de investigação: positivista e interpretativa [Bhattacherjee 2012].

Na investigação positivista, o conhecimento consiste em perceber o como e o porquê das pessoas efetuarem ligações entre diferentes factos para obterem teorias que expliquem o comportamento [Livesey 2006]. Assume-se que a realidade é objetiva e que esta pode ser expressa através da mensuração sistemática e estatística de relacionamentos entre variáveis [Moresi 2003].

A investigação interpretativa assenta na ideia de que a interação social está baseada em três princípios: estamos sempre conscientes de nós próprios e do nosso relacionamento com os outros (consciência); fazemos escolhas deliberadas sobre como nos comportar nas diferentes situações (ação); e somos imprevisíveis em certos momentos (imprevisibilidade) [Livesey 2006]. Tendo em conta estes três princípios, esta abordagem tem como objetivo compreender os diferentes fenómenos através da análise das referências fornecidas pela população estudada. Neste caso, é assumido que a realidade é subjetiva e socialmente construída [Moresi 2003].

Na presente dissertação, como já referido, numa vertente prática do trabalho efetuado, teve-se como objetivo comparar as orientações fornecidas por um certo normativo com as práticas desenvolvidas numa determinada organização. Com esse propósito, desenvolveu-se uma investigação interpretativa para se obter o conhecimento dessas práticas através de um dos colaboradores da organização, ou seja, baseando as conclusões retiradas na opinião da pessoa com a qual se estabeleceu contacto.

Segundo Yin [Yin 2009], o estudo de caso é o método de investigação mais adequado quando nos deparamos com questões que focam-se no “como” e no “porquê” das coisas, quando temos pouco controlo nos eventos que estamos a analisar, e quando o nosso objeto de análise se trata de um fenómeno atual analisado num contexto da vida real. Yin [Yin 2009] acrescenta que neste tipo de método de investigação, lida-se com situações nas quais haverá mais variáveis de interesse do que as apontadas pelos dados reunidos. Os estudos de caso podem ser de natureza positivista, sendo utilizados para o teste de hipóteses, ou de natureza interpretativa, participando na construção de uma teoria [Bhattacherjee 2012]. De facto, uma vez que se trata de um método de investigação, o estudo de caso é utilizado em diversas situações, contribuindo para o nosso conhecimento acerca de indivíduos, grupos e organizações, tanto a nível social, político como fenomenal [Yin 2009].

Como, numa fase inicial da parte mais prática do trabalho desenvolvido no âmbito desta dissertação, foi necessário estabelecer contacto com uma organização e apurar a forma como aplicam ou desenvolvem as suas atividades de gestão da informação, com foco principal na segurança da informação, os resultados obtidos foram baseados na implementação de um

estudo de caso, sendo este um dos métodos aplicados para implementar a investigação interpretativa necessária ao alcance dos objetivos.

No desenrolar deste tipo de investigações, tem que se recolher e processar diferentes tipos de dados, o qual se pode fazer através dos métodos quantitativos e/ou qualitativos [Bhattacherjee 2012], sendo que o método qualitativo será mais depressa associado à abordagem interpretativa, enquanto que o método quantitativo é normalmente associado a estudos positivistas [Moresi 2003]. Cada um deles refere-se ao tipo de dados que estão a ser adquiridos (que podem variar entre pontuações numéricas, métricas - quantitativos - e entrevistas, observações - qualitativos) e à forma como estes estão a ser analisados (por exemplo, através de regressão - técnica quantitativa - ou codificação - técnica qualitativa) [Bhattacherjee 2012].

O método quantitativo tem como base instrumentos estatísticos, não só no levantamento de dados como também no tratamento dos mesmos. Deste modo, garante-se a precisão dos resultados, evitando distorções de análise ou de interpretações, o que permite ter uma margem de segurança quanto às inferências feitas [Raupp and Beuren 2004]. Neste tipo de métodos, defende-se que a maneira de chegar à compreensão das diferentes relações, mesmos daquelas mais complexas, é explicando ou compreendendo as relações entre as diferentes variáveis [Günther 2006]

Por outro lado, o método qualitativo é indutivo, ou seja, neste caso o pesquisador irá desenvolver os conceitos, as ideias e entendimentos a partir de padrões que consiga encontrar nos dados [Moresi 2003]. Como tal, este tipo de pesquisa deve ser flexível e adaptável, e requer um maior cuidado na descrição de todos os passos da pesquisa, desde o planeamento, à obtenção dos dados, passando pela transcrição e finalizando na preparação dos mesmos para a análise [Günther 2006]. Os três métodos qualitativos mais comuns são: observação participante, ideal para recolher dados sobre os comportamentos que ocorrem de forma natural nos contextos habituais; entrevista em profundidade, que são apropriadas para reunir dados relacionado com histórias, perspetivas e experiências de um determinado individuo; e grupo focal, que permitem descobrir dados sobre as normas culturais de um determinado grupo e gerar um visão geral de questões que sejam de interesse para os grupos culturais ou subgrupos representados [Mack et al. 2005].

Uma vez que o nosso objetivo passou por perceber a perspetiva de um dos colaboradores com forte presença na área da gestão da informação da organização, o método que nos permitiu obter essa informação para futuro tratamento de dados foi o método qualitativo, entrevista em profundidade.

5.3 Preparação do Estudo de Caso

Depois de perceber-se qual a metodologia a aplicar, assim como as técnicas que melhor se adequavam aos objetivos da presente dissertação, deu-se início ao planeamento das ações que levariam à concretização dos mesmos.

Assim, no início de Junho de 2013 foram contactados, via email, diversos hospitais públicos na zona do Porto, Braga e Santa Maria da Feira. Uma vez que a primeira tentativa não resultou em nenhuma resposta, voltou-se a enviar outro email para as mesmas instituições, ainda no mês de Junho, sendo que desta vez, para além de incluirmos como destinatário a direção do hospital, envolvemos o contacto dos departamentos de sistemas de informação disponibilizados nos diferentes websites. Desta vez, obtemos uma resposta positiva de um centro hospitalar, com o qual marcou-se de imediato uma reunião para se poder apresentar melhor a ideia do estudo. Esta reunião teve lugar no dia 4 de Julho de 2013.

Após apresentar as linhas orientadoras da presente dissertação e qual o papel que o contacto referido desempenharia na mesma, combinou-se a realização da entrevista que teve lugar nas instalações do departamento de sistemas de informação do centro hospitalar, no dia 14 de Agosto de 2013.

Para a elaboração das questões da entrevista, utilizou-se como base a publicação do ISACA, COBIT5SI, estudada na revisão bibliográfica, uma vez que pretendia-se aferir quais as práticas, estruturas organizacionais ou informações de segurança da informação que a organização tinha implementadas, mantendo presente a vertente comparativa com o *framework* COBIT que esta dissertação apresenta. Para tal, foram preparadas definições dos diferentes processos, estruturas, etc. para serem disponibilizados ao longo da entrevista, podendo assim o entrevistado estar alinhado com a realidade apresentada no COBIT e conseguir estabelecer uma melhor relação com as orientações analisadas e aquilo que é efetuado na sua organização. Devido à dimensão que o COBIT apresenta, foram analisados somente 4 facilitadores: políticas e princípios, processos, estruturas organizacionais e informação. A estrutura da entrevista pode ser encontrada no anexo I, sendo que as definições encontram-se nos anexos II, III, IV e V.

6. Apresentação e Análise de Resultados

Neste capítulo encontram-se os resultados recolhidos no desenvolvimento do caso de estudo e respetiva análise.

6.1 Caracterização da Instituição

O centro hospitalar em estudo trata-se de uma empresa pública empresarial (EPE) que em 2011 apresentou 165 milhões de euros faturados, e abarca cerca de 3100 empregados. É uma grande empresa, cuja classificação de atividades económicas é a 86100, que está associada às atividades dos estabelecimentos de saúde com internamento.

A sua missão passa por prestar cuidados de saúde diferenciados, tendo em vista uma articulação com a rede de saúde primária e com os hospitais do Serviço Nacional de Saúde (SNS), apostando na motivação e satisfação dos seus profissionais; participar no ensino pré e pós-graduado, assim como garantir uma formação contínua necessária ao desenvolvimento dos seus profissionais; e apostar na investigação e no desenvolvimento científico em todas as áreas das ciências da saúde.

Tem como visão garantir um continuado desenvolvimento e aperfeiçoamento técnico e científico nas valências que integra, na qualidade da assistência prestada aos utentes e na experiência na gestão clínica, numa lógica de transparência e de responsabilização.

No organograma da organização podemos encontrar o serviço de SI na área dos serviços de apoio à prestação de cuidados, mais especificamente dentro da unidade de organização, planeamento e gestão financeira. Este departamento tem basicamente quatro grandes áreas funcionais, dando-se mais relevância a três delas, como se pode verificar na Figura 6.1. As três principais áreas são a gestão de projetos, a gestão de aplicações e a gestão de produção, sendo que a área acessória é a de consultoria/assessoria ao conselho e aos diretores de serviço, em termos de sistemas da informação.

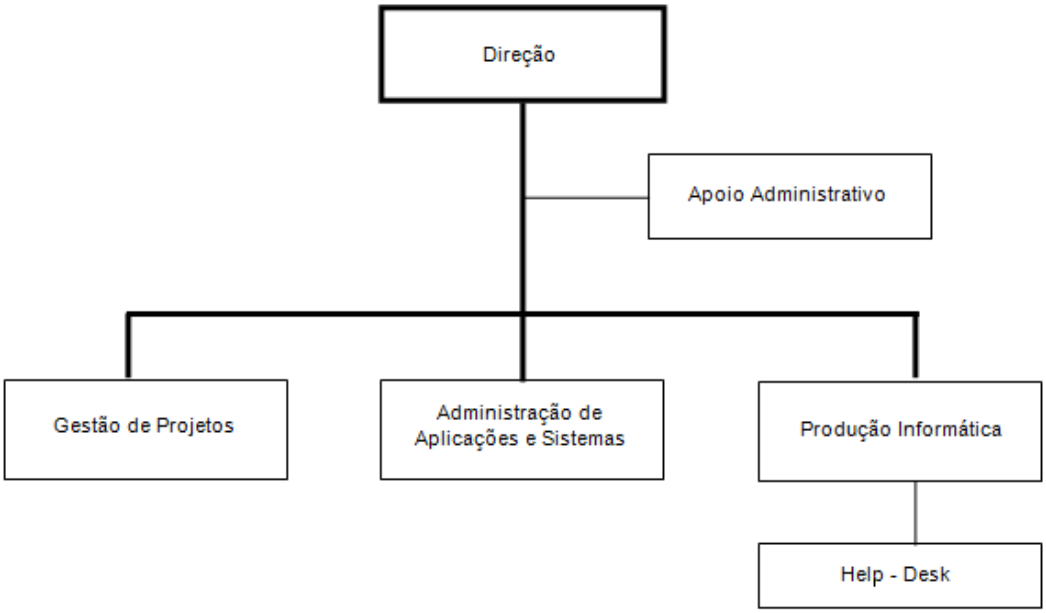


Figura 6.1 **Organigrama do departamento de SI da organização em análise**

O entrevistado é o CISO e o diretor do departamento de SI da organização em análise.

6.2 Resultados obtidos da Entrevista

Como visto no capítulo 2.2, uma auditoria pretende comparar o que uma organização faz com um conjunto definido de critérios ou requisitos. Esta dissertação pretendeu desenvolver um caso de estudo que tivesse presente uma vertente de auditoria, podendo assim pôr em prática a teoria apresentada na revisão bibliográfica. Na elaboração da entrevista, quis-se, portanto, realizar uma recolha de dados que permitisse elaborar uma comparação entre as orientações apresentadas no COBIT5SI e aquilo que estaria a ser implementado na organização.

Como referido no capítulo 3.1, por forma a garantir a confidencialidade, integridade e disponibilidade da informação é necessário que todas as pessoas envolvidas no uso e gestão da informação da organização compreendam as políticas, normas, processos ou outros requisitos de segurança da informação que estão a ser aplicados na organização. Assim, e devido à extensão do *framework* COBIT, decidiu-se que a entrevista se basearia somente na abordagem de segurança da informação de quatro dos facilitadores apresentados no COBIT5SI: princípios e políticas; processos; estruturas organizacionais; e tipos de informação.

Os resultados obtidos estão divididos por vários pontos. Inicia-se com a apresentação dos resultados da entrevista obtidos relativamente aos princípios recomendados pelo COBIT5SI, seguidos da apresentação dos resultados adjacentes às políticas recomendadas pelo mesmo. Na secção 6.2.3, podem-se verificar quais os processos que estão a ser implementados na

organização e em que fase de implementação se encontram. Nas secções seguintes, apresentam-se as estruturas organizacionais, e práticas adjacentes, presentes na organização, finalizando a apresentação dos resultados com os diferentes tipos de informação e *stakeholders* existentes na organização.

6.2.1 Princípios de Segurança da Informação do COBIT5SI

Como referido na secção 4.1.3.1, o COBIT5SI apresenta um conjunto de princípios de segurança da informação que considera importantes para garantir que as regras de segurança da informação estão a ser comunicadas pela direção e pelos órgãos sociais à restante organização. Como estas regras servem de apoio ao alcance dos diferentes objetivos da organização, quer de governança quer de gestão, introduziu-se na análise efetuada uma secção onde se pretendia analisar quais os princípios, sugeridos pelo COBIT5SI, que eram aplicados na organização, e se haveria outros princípios a serem aplicados para além dos sugeridos.

No seguimento da entrevista, o entrevistado afirmou que nem sempre existe um documento específico que esteja destinado a uma destas questões mais concretamente, no entanto os diferentes princípios cruzam-se em diversos documentos que estabelecem a gestão de segurança de informação na organização, sendo que alguns deles servem inclusive de base ao surgimento de certas políticas, como é o caso do princípio cumprir com os requisitos legais e regulamentares relevantes que foi identificado como a base para a política geral de segurança e para a listagem das dez boas práticas de segurança da informação utilizadas na organização.

Do conjunto de princípios que o COBIT5SI sugere para uma boa comunicação das regras de segurança da informação, o único que não se encontra a ser implementado na área de segurança da informação corresponde à preocupação em fornecer qualidade e valor aos *stakeholders*. O entrevistado justifica esta questão afirmando que "*na área de segurança da informação a nossa preocupação existe no sentido de diminuir o risco e evitar problemas de segurança, e não tanto em agregar valor. É diminuir o risco*". Por esta mesma razão, e até à data da entrevista, ainda não tinha sido construída nenhuma solução pensada em ser uma mais-valia para os *stakeholders*. Os resultados podem ser consultados na tabela 6.1, e a explicação do que cada um destes princípios antevê, pode ser consultada no anexo II**.**

PRINCÍPIOS	Centro Hospitalar
Suporte ao Negócio	
Foco no Negócio	√
Fornecer qualidade e valor aos stakeholders	x
Cumprir com os requisitos legais e regulamentares relevantes	√
Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação	√
Avaliar atuais e futuras ameaças à informação	√
Promover a melhoria contínua da segurança da informação	√
Defender o Negócio	
Adotar uma abordagem baseada no risco	√
Proteger informação confidencial	√
Concentrar-se nas aplicações de negócio críticas	√
Desenvolver sistemas de forma segura	√
Promover um comportamento responsável de segurança da informação	
Agir de forma ética e profissional	√
Fomentar uma cultura positiva de segurança da informação	√

√ presente | X não existe

Tabela 6.1 Checklist de Princípios baseada nas recomendações do COBIT5SI

Para além dos princípios sugeridos pelo COBIT5SI, o entrevistado aponta o princípio da vigilância como um dos seguidos pela organização, que se destina a aumentar a sensibilidade dos colaboradores no que toca a identificar comportamentos indevidos e a fornecer informações para iniciar ações que os minimize ou erradique. O entrevistado defende que este deve ser um "*estado policial que cada um dos colaboradores deve ter no seu posto de trabalho*", atuando de uma forma empenhada na proteção dos recursos da empresa, incluindo os sistemas de informação.

Com base na análise comparativa, nota-se, então, que a grande maioria dos princípios sugeridos pelo COBIT5SI se tratam de preocupações da organização e se encontram incluídos na sua documentação. No entanto, 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.

6.2.2 Políticas de Segurança da Informação do COBIT5SI

As políticas visam ser mais detalhadas, fornecendo orientação para que os princípios seguidos pela organização sejam postos em prática. Como referido anteriormente na secção 4.1.3.1, o COBIT5SI apresenta sugestões de políticas, divididas entre a área de segurança da informação e restantes áreas de SI, estas últimas impulsionadas por outras funções dentro da organização. Usou-se essa informação como base, primeiro, para identificar quais as políticas associadas à função de segurança da informação sugeridas no COBIT5SI que poderiam estar

a ser implementadas na organização, e, numa segunda instância, para perceber-se se o entrevistado tinha conhecimento das políticas adjacentes a outras áreas, com o intuito de avaliar a comunicação transversal na organização.

Assim, obteve-se a informação que o departamento de sistemas de informação da organização está de acordo com a importância das políticas sugeridas. Relativamente à política controlo de acesso, o entrevistado explica que existem "*processos no terreno, suportados por ferramentas informáticas"*, que visam informar as pessoas sobre o que têm de fazer quando têm de se credenciar, por exemplo, afirmando que "*existe uma cultura que já passou para ação"*. Quanto à política resposta a incidentes, indica que a mesma pode ser encontrada incorporada na política geral de segurança, onde está definido o conceito de incidente e as medidas a seguir caso o mesmo se registe. Em termos de preocupação relativamente ao meio físico e ambiental dos recursos de apoio às operações, embora não exista um documento base neste tópico, o entrevistado indica que o mesmo faz parte da lógica de projeto, atribuindo-se automaticamente cuidados adicionais de segurança nas áreas consideradas mais sensíveis. No que toca à política sugerida com foco no pessoal de segurança da informação, o entrevistado admitiu que a forma como o mesmo é avaliado é equivalente à forma como a avaliação é feita aos restantes funcionários em funções diferentes, tratando-se de uma preocupação existente no departamento de sistemas de informação mas não havendo, no entanto, práticas que defiram das administradas às restantes funções. A definição de cada uma destas políticas pode ser encontrada no anexo II.

O entrevistado acrescenta que "*o COBIT é um framework de gestão da função de TSI"*, e que, por sua vez, a ISO27001 está mais centrada na segurança de um SI. Como tal, afirma que as políticas e controlos base utilizados na organização resultam diretamente do que está previsto na ISO27001.

Como já dito, tentou-se também perceber em que nível estaria a ocorrer a comunicação ao departamento de SI das políticas existentes na organização mas não diretamente ligadas à função de segurança da informação. O entrevistado evidenciou conhecimento dos outros tipos de políticas consideradas importantes pelo COBIT5SI mas que são impulsionadas por outras funções dentro da organização. De notar, que embora seja o responsável pelo departamento de sistemas de informação, algumas destas políticas não são desenvolvidas pelo seu departamento, como é o caso da política de gestão de risco, no entanto, o entrevistado afirmou que a comunicação está a ser realizada e que tem conhecimento e acesso às políticas em questão.

A verificação de que políticas estão a ser implementadas na organização, tanto na área de segurança da informação como nas restantes áreas da organização, pode ser consultada na tabela 6.2.

POLÍTICAS	Centro Hospitalar
Impulsionadas pela função de segurança da informação	
Controlo de acesso	√
Pessoal de segurança de informação	±
Meio físico e ambiental de segurança de informação	±
Resposta a incidentes	√
Impulsionadas por outras funções dentro da organização	
Continuidade do negócio e recuperação de desastres	√
Gestão de ativos	√
Regras de comportamento (uso aceitável)	√
Adquirir sistemas de informação, desenvolvimento e manutenção de software	√
Gestão de fornecedores	√
Gestão das operações e da comunicação	√
Conformidade	√
Gestão de Risco	√

√ presente | ± preocupação presente

Tabela 6.2 Checklist de Políticas baseada nas recomendações do COBIT5SI

Esta informação permite concluir que grande parte das políticas sugeridas estão a ser postas em prática e tratam-se de preocupações presentes no dia-a-dia da organização. No entanto, 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 que na secção anterior, sendo que com essa melhoria poderá trazer o benefício á organização de conseguir evitar problemas de segurança causados por alguma falha na informação adquirida pelos seus colaboradores.

Numa segunda estância, 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.

6.2.3 Processos do COBIT e Segurança da Informação

Um outro aspeto que se quis analisar seria quais os processos que a organização tem implementados na organização. Como referido nas secções 4.1.1, 4.1.2 e 4.1.3, todos os normativos estudados apresentavam processos relacionados com a segurança da informação que requeriam ou recomendavam estarem implementados nas diferentes organizações que implementem os mesmos. No caso do COBIT, dos 37 processos apresentados só dois é que estão diretamente ligados à área da segurança da informação, no entanto, e como se

apresentou no capitulo 4.1.3.1, todos estes processos tem uma vertente de segurança que é tratada com mais detalhe no COBIT5SI.

Como não se quis entrar numa abordagem técnica, optamos por avaliar se os 37 processos estavam a ser aplicados na organização, e se sim em que etapa de implementação estariam. Para obtermos informação acerca do estado de cada um dos processos, decidimos avaliar os mesmos com base numa escala de avaliação. A escala que usamos por base foi a mesma que é implementada 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 definidos 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].

Interpretando como vermelho a fase inicial, laranja a fase intuitiva, amarelo a fase de definição, verde a fase de gerido e mensurável, e azul a fase em constante otimização, pode-se consultar os resultados na figura 6.2.

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: assegurar a transparência dos stakeholders, administrar acordos de serviços, gestão da qualidade e gerir a configuração. O entrevistado explica que embora habitualmente um "*processo é algo que está escrito"*, na realidade não têm um modelo que explique como é que a equipa faz os diferentes processos. Baseiam-se, sim, num "*conjunto de práticas e de documentos que vão no sentido de responder"* à definição dos diferentes processos. Acrescenta, ainda, que na área de governança, o processo que visa assegurar a definição e manutenção de um framework de governança não está otimizado porque, entre outras razões, nem sempre a visão da função de TSI é partilhada pelo conselho de administração, que poderá ter em mãos outras preocupações e ainda "*não identificou a função TIC como um vetor estratégico"*.

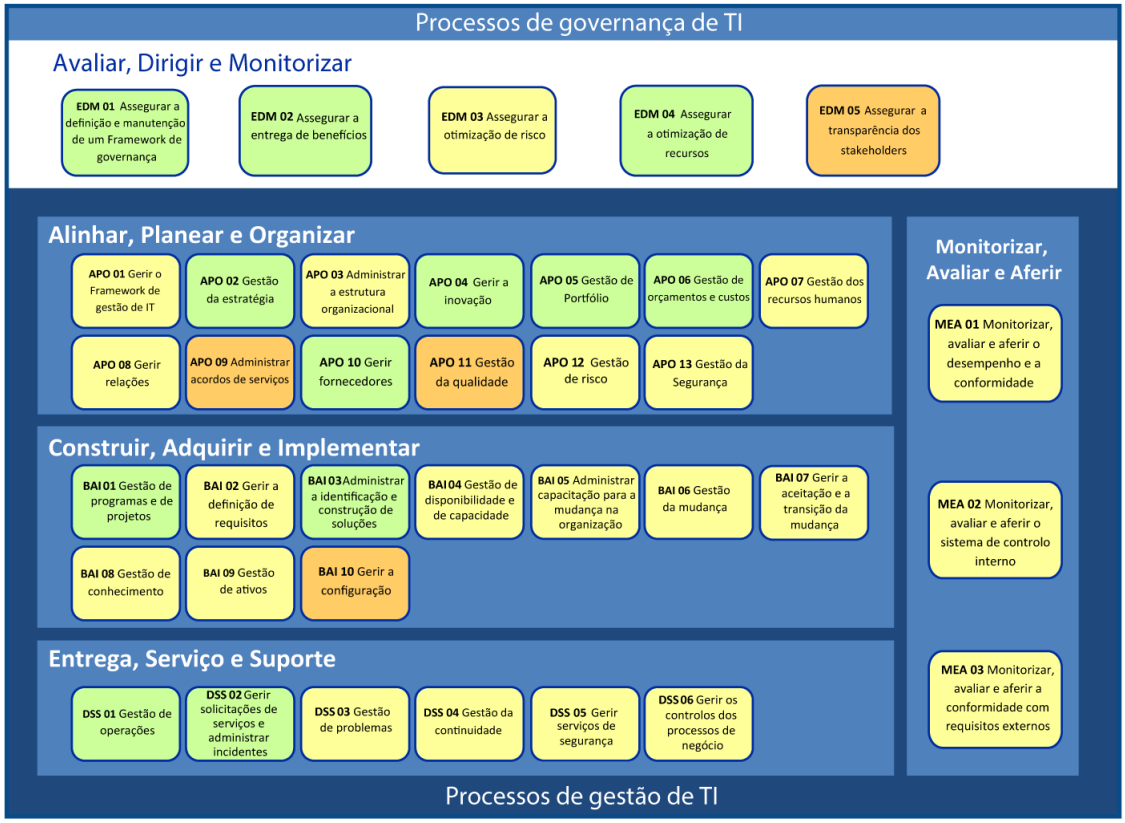


Figura 6.2 Fases de implementação dos processos recomendados pelo COBIT5SI

Ainda assim, 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.

6.2.4 Estruturas Organizacionais de Segurança da Informação do COBIT5SI

Sendo importante a tomada de decisão no dia-a-dia de cada organização, achou-se importante verificar quais seriam as estruturas organizacionais da organização que levam a cabo essas tomadas de decisões. Para isso, para além de verificar-se quais as funções e/ou estruturas recomendas pelo COBIT5SI, que se encontram enquadradas na organização, analisou-se também quais as práticas a ser efetuadas na organização que estão associadas a cada uma dessas funções e/ou estruturas. O âmbito destas funções e/ou estruturas organizacionais pode ser encontrado no anexo IV.

Da entrevista, retirou-se a informação de que a função CISO está inserida na estrutura do departamento de SI, sendo também associada à mesma pessoa a responsabilidade que o COBIT5SI delega ao gestor de segurança da informação (ISM). O entrevistado refere também que o comité está previsto na política, havendo "*referência à Comissão de Segurança da Informação* (ISMC - *Information Security Management Committee*)", e que a mesma "*foi aceite pelo conselho anterior, mas não está nomeada e, não estando nomeada, não existe*", embora já tenha sido pensada. Relativamente aos responsáveis pela informação, explica que não se aplica nenhuma regra onde esteja especificado quem é o dono da informação, no entanto, quando se trata de projetos transversais à organização, o que acontece é que essa posição está definida inicialmente, mas, à medida que o tempo vai passando, vai-se dissipando, pois após o projeto entrar na fase de produção e existir um acompanhamento inicial, deixa de ser necessário este cargo na realização do projeto. Ou seja, neste tipo de projetos transversais, é definido um diretor do projeto do lado do utilizador que fica responsável pelo acompanhamento inicial e cuja ligação se vai dissolvendo ao longo do tempo. Já em projetos que se realizem exclusivamente no departamento de sistemas de informação, este cargo está associado ao dono do serviço. A existência destas funções pode ser consultada na tabela 6.3.

FUNÇÕES / ESTRUTURAS ORGANIZACIONAIS	Centro Hospitalar
Diretor de Segurança da Informação (CISO)	√
Comité de Direção de Segurança da Informação (ISSC)	X
Gestor de Segurança de Informação (ISM)	≈ CISO
Comité de Gestão do Risco do Negócio (ERM - Enterprise Risk Management)	√
Responsáveis pela Informação / Proprietários da empresa	±

√ presente | ± preocupação existente | X não existe | ≈ função associada a

Tabela 6.3 Checklist de Funções e/ou estruturas organizacionais baseada nas recomendações do COBIT5SI

Para além das funções, o COBIT5SI apresenta um conjunto de práticas que associa a cada uma dessas funções e/ou estruturas. definindo os diferentes tipos de envolvimento através do mapa RACI, que, como referido na secção 4.1.3.1, apresenta prevê que certa entidade é responsável (R), responsabilizado (A), consultado (C) ou informado (I) . Nas tabelas 6.4, 6.5, 6.6, 6.7 e 6.8**.**, pode-se analisar as diferenças existentes em cada uma das funções e/ou estruturas organizacionais, entre o envolvimento que o COBIT5SI recomenda e o envolvimento praticado na organização.

Acerca das práticas associadas à função do CISO (tabela 6.4), podemos verificar que a instituição acaba por ter a mesma associação que a prevista no COBIT5SI no que toca ao CISO prestar contas relativamente a um determinado conjunto de práticas, como demonstrado na tabela 6.4. Já quando se trata de este estar encarregado por certas práticas, as coisas funcionam de forma ligeiramente diferente daquela sugerida no COBIT5SI:

- O CISO está responsabilizado por garantir que o acompanhamento da gestão de riscos de TSI seja realizado, no entanto, a equipa toda de TSI está encarregada desse mesmo acompanhamento;
- Da mesma forma, a equipa de TSI é responsável por pesquisar, definir e documentar os requisitos de segurança da informação, limitando-se o CISO a ter que dar a cara pela realização desta prática;
- Após o chefe do projeto no departamento de Ti validar os requisitos de segurança da informação com os stakeholders, patrocinadores do negócio e com o pessoal de execução técnica, o CISO só terá que ser informado relativamente a esta atividade;
- O chefe do projeto é o responsável por garantir que é feita a avaliação ao potencial impacto das mudanças efetuadas, enquanto que o CISO só terá que garantir que esta prática seja efetuada, sem que seja o mesmo a implementá-la;
- Na prática que se foca em recolher e analisar os dados de desempenho e conformidade relacionados com a segurança da informação e com a gestão de riscos da informação, o CISO terá que garantir que a mesma acontece, sendo que o chefe do projeto que colabora, em cada caso, com o núcleo de gestão de riscos, é que fica encarregado desta ação;

Relativamente ao comité de gestão de risco (tabela 6.5), na organização em análise, este não participa na definição da estratégia de segurança da informação nem na revisão dos perfis de risco e da avaliação de risco da informação, estando estas práticas ao cargo do CISO, que define a estratégia sempre que esta for necessária e tem como preocupação constante o risco da informação. Ainda assim, verifica-se que em termos de definir e implementar a avaliação de risco e as estratégias de resposta, este comité é considerado responsabilizado por estas tarefas, como é sugerido pelo COBIT5SI.

CISO	COBIT	C.Hospitalar
Práticas		
Identificar e comunicar as ameaças de segurança da informação, assim como os comportamentos desejados e as mudanças necessárias para enfrentar as mesmas.	R	R
Garantir que a gestão do ambiente e das instalações se adequa aos requisitos de segurança da informação.	R	R
Proteger contra malware.	R	R
Gerir a segurança na conectividade e de rede.	R	R
Gerir a segurança de terminais.	R	R
Gerir a identidade dos utilizadores e o acesso lógico.	R	R
Gerir o acesso físico a ativos de IT.	R	R
Monitorizar a infraestrutura para eventos relacionados com a segurança.	R	R
Proporcionar meios para melhorar a eficiência e eficácia da função de segurança da informação (por exemplo, através da formação do pessoal de segurança da informação; documentação de processos, tecnologias e aplicações; e padronização e automatização do processo).	R	R
Acompanhar a gestão de riscos de IT.	A	R
Definir e comunicar uma estratégia de segurança da informação que esteja alinhada com a estratégia da organização.	A	A
Pesquisar, definir e documentar os requisitos de segurança da informação.	A	R
Validar os requisitos de segurança da informação com os stakeholders, patrocinadores do negócio e pessoal de execução técnica.	A	I
Desenvolver políticas e procedimentos de segurança da informação.	A	R/A
Definir e implementar a avaliação de risco e as estratégias de resposta e cooperar com o departamento de risco na gestão do risco da informação.	A	A
Garantir que o impacto potencial das mudanças é avaliado.	A	R
Recolher e analisar dados de desempenho e conformidade relacionados à segurança da informação e à gestão de riscos da informação.	A	R

R – Responsável | A – Responsabilizado | I - Informado

Tabela 6.4 Diferenças entre o envolvimento da função CISO realizado na organização e aquele recomendado pelo COBIT5SI

ERMC	COBIT	C. Hospitalar
Práticas		
Aconselhamento sobre a estratégia de segurança da informação definida pelo ISSC.	A	› CISO
Estabelecer os níveis de tolerância ao risco da organização.	R	A
Definir e implementar a avaliação de risco e as estratégias de resposta.	R	R
Rever a avaliação de risco da informação e os perfis de risco.	A	› CISO

R – Responsável | A – Responsabilizado | › - Prática associada ao

Tabela 6.5 Diferenças entre o envolvimento da estrutura organizacional ERMC realizado na organização e aquele recomendado pelo COBIT5SI

Seguem-se as práticas associadas aos responsáveis pela informação (tabela 6.6), onde se verifica que o nível de envolvimento em termos de comunicar, aconselhar e coordenar os esforços da gestão de risco de informações com os chefes hierárquicos é muito reduzido, não se aplicando. Porém, o entrevistado indica que se esta prática for realizada por alguém, o encarregado e responsabilizado pela mesma será o administrador da aplicação ou projeto, da parte da informática. Em termos de reporte de mudanças nos processos e/ou nas estratégias de negócio verifica-se que a função é dividida entre o departamento de TSI e o responsável pela informação, sendo que algumas vezes este último comunica as mudanças ao

departamento de TSI e noutras o departamento acaba por se aperceber das mesmas sem necessitar de qualquer tipo de reporte. Já no que toca a aumentar a visibilidade da função de segurança da informação e das políticas e procedimentos de segurança da informação dentro da empresa, o responsável pela informação não tem qualquer tipo de envolvimento, estando esta prática à responsabilidade do CISO.

Responsáveis pela Informação	COBIT	C. Hospitalar
Responsáveis pela Informação / Proprietários da empresa		
Comunicar, aconselhar e coordenar os esforços da gestão de risco de informações com os chefes hierárquicos.	R	*
Reportar as mudanças nos processos e/ou nas estratégias de negócio (isto é, novos produtos ou serviços) ao ISSC.	R	R
Aumentar a visibilidade da função de segurança da informação e das políticas e procedimentos de segurança da informação dentro da empresa.	R	› CISO

R – Responsável | › - Prática associada ao | * - Não Aplicável

Tabela 6.6 Diferenças entre o envolvimento dos responsáveis pela informação realizado na organização e aquele recomendado pelo COBIT5SI

Para além das funções analisadas anteriormente, tentou-se perceber qual seriam as funções e/ou estruturas organizacionais que teriam o nível de envolvimento que o COBIT5SI aconselha no caso daquelas que não se verificaram na instituição.

Como se pode verificar nas tabelas 6.7 e 6.8, grande parte destas práticas são garantidas pela função do CISO. Esta tendência não se verifica somente nestas práticas associadas pelo COBIT5SI a funções que não se encontram previstas na estrutura da organização. Nota-se que no geral, grande parte das práticas de segurança acaba por passar pelas mãos do CISO mesmo que exista na estrutura da organização uma função que seja igualmente capaz de garantir a sua execução.

ISSC	COBIT	C. Hospitalar
Práticas		
Definir e comunicar uma estratégia de segurança da informação que esteja alinhada com a estratégia da organização.	R	› CISO
Pesquisar, definir e documentar os requisitos de segurança da informação.	R	› CISO
Validar os requisitos de segurança da informação com os stakeholders, patrocinadores do negócio e pessoal de execução técnica.	R	› Chefe de Projeto
Desenvolver políticas e procedimentos de segurança da informação.	R	› CISO
Desenvolver um plano de segurança da informação que identifica o ambiente de segurança da informação e os controlos a serem implementados pela equipa do projeto para proteger os ativos da organização.	R	› Chefe de Projeto
Garantir que o impacto potencial das mudanças é avaliado.	R	› Chefe de Projeto
Recolher e analisar dados de desempenho e conformidade relacionados à segurança da informação e à gestão de riscos da informação.	R	› Chefe de Projeto
Estabelecer, acordar e comunicar o papel do CISO e do ISM.	A	› Conselho de Administração (CA)
Aumentar a visibilidade da função de segurança da informação dentro da empresa e, potencialmente, fora da mesma.	A	› CISO + Núcleo de Gestão de Risco
Contribuir, em toda a organização, nos esforços de gestão da continuidade do negócio.	A	› CISO + Núcleo de Gestão de Risco

R – Responsável | A – Responsabilizado | › - Prática associada ao

Tabela 6.7 Representação de quais as funções que respondem ao envolvimento recomendado pelo COBIT5SI relativamente à estrutura organizacional ISSC

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.

Uma forma de melhorar todo este processo, seria organizar uma listagem das diferentes práticas a realizar em termos de segurança da informação, e associar às funções existentes na estrutura da organização. Não terá que ser necessariamente a mesma lista de práticas que o COBIT5SI recomenda, que, aliás, foi toda ela reconhecida como práticas efetuadas na organização. Deverá, sim, ser uma lista 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. No entanto, essa visão de cima de todo o processo deveria também analisar se não haverá necessidade de criar novas funções para que seja evitada a sobrecarga.

ISM	COBIT	C. Hospitalar
Práticas		
Desenvolver e comunicar uma visão comum para a equipa de segurança da informação que esteja alinhada com a visão da organização.	R	› CISO
Gerir a alocação do pessoal de segurança da informação de acordo com os requisitos do negócio.	R	› CISO
Realizar avaliações de risco da informação e definir o perfil de risco da mesma.	R	› Chefe de Projeto
Gerir funções, responsabilidades, direitos de acesso e níveis de autoridade.	R	› Chefe de Projeto
Desenvolver um plano de segurança da informação que identifica o ambiente de segurança da informação e os controlos a serem implementados pela equipa do projeto para proteger os ativos da organização. Monitorizar esses controlos internos e ajustar/melhorar quando necessário.	R	› Chefe de Projeto
Identificar e comunicar os pontos fracos de segurança da informação, assim como os comportamentos desejáveis e as mudanças necessárias para enfrentar os mesmos.	R	› CISO
Proporcionar meios para melhorar a eficiência e eficácia da função de segurança da informação (por exemplo, através da formação do pessoal de segurança da informação; documentação de processos, tecnologias e aplicações; e padronização e automatização do processo).	R	› CISO + Chefe de Projeto (+ CA em caso de investimento)
Recolher e analisar dados de desempenho e conformidade relacionados à segurança da informação e à gestão de riscos da informação.	R	› CISO
Garantir que a gestão do ambiente e das instalações se adequa aos requisitos de segurança da informação.	R	› CISO

R – Responsável | › - Prática associada ao

Tabela 6.8 Representação de quais as funções que respondem ao envolvimento recomendado pelo COBIT5SI relativamente à função ISM

Através desta estruturação, as diferentes funções e pessoas adjacentes saberiam quais as práticas pelas quais se encontram encarregadas; quais aquelas pelas quais têm que prestar contas; de quais é que necessitam de receber informação; e também quais são as práticas nas quais adquirem um papel de consultoria.

6.2.5 Tipos de Informação de Segurança da Informação do COBIT5SI

O COBIT5SI apresenta vários tipos de informação relacionados com segurança da informação, disponibilizando também uma matriz que relaciona as diferentes informações com os diferentes *stakeholders*, com o objetivo de se conseguir percecionar quem é que origina, aprova, é informado de, ou utiliza os diferentes tipos de informação. Na seção da entrevista destinada ao facilitador Informação apresentado no COBIT5SI, começou-se por tentar perceber em que ponto estariam os diferentes tipos de informação, mais propriamente, se os mesmos tinham documentos direcionados para cada um deles ou se não se encontravam registados na organização. A descrição de cada uma destes documentos relevantes para a segurança da informação pode ser encontrada no anexo V desta dissertação.

O entrevistado afirmou que não existem relatórios de avaliação de segurança da informação mas que todos os restantes, de uma forma ou de outra, se encontram documentados. O mesmo encontra-se demonstrado na tabela 6.9. No entanto, somente o material de consciencialização é que se encontra especificado num documento com esse único fim, sendo que todos os outros estão estipulados mas fazem parte de documentos que envolvem toda a

organização. Obteve-se a informação de que "*existe um documento que estabelece bem como a segurança da informação deve ser gerida, mas isso não é propriamente uma estratégia*". Sendo a área de segurança da informação uma área de desenvolvimento interno, a sua estratégia está integrada em vários processos e projetos, não existindo, porém, um documento isolado. No entanto, refere ainda, que se for necessário mostrar o que já foi feito, encontra-se tudo documentado. Em termos de orçamento de segurança da informação, este encontra-se integrado no documento que estipula o orçamento geral, e o plano de segurança da informação faz parte do plano anual dos sistemas de informação. Informa ainda que existem listas de requisitos documentados, adjacentes aos diferentes projetos, onde se encontram não só os requisitos de origem funcional mas também os de segurança, desempenho e gestão. Por fim, confirma a existência da definição do que é um incidente grave, e se surgir um incidente cuja fonte seja segurança, esse momento dá origem a um relatório específico, por isso, a organização não tem um painel de incidentes ou de segurança, tem sim uma lista de incidentes com os quais já lidou no passado, na qual os de segurança fazem parte.

De notar, que embora as políticas e o perfil de risco da informação sejam considerados tipos de informação pelo COBIT5SI, como visto na secção 4.1.3.1, os mesmos não foram introduzidos nesta *checklist*. A razão para tal acontecer pode ser baseada no anexo E do COBIT5SI. Neste anexo, relativamente às políticas é referido que um dos facilitadores se foca exatamente nesse objeto e portanto reencaminha para lá. Por sua vez, não existe qualquer indicação e descrição do perfil de risco da informação no anexo E, e, como tal, o mesmo não foi considerado.

TIPOS DE INFORMAÇÃO	C. Hospitalar
Estratégia de Segurança da Informação	±
Orçamento da Segurança da Informação	±
Plano de Segurança da Informação	±
Políticas	±
Requisitos de Segurança da Informação	±
Material de Consciencialização	±
Relatórios de Revisão de Segurança da Informação	√
Perfil de Risco da Informação	X
Painel de Segurança da Informação	±

√ presente | ± preocupação existente | X não existe

Tabela 6.9 Checklist de tipos de informação de segurança da informação baseada nas recomendações do COBIT5SI

O entrevistado acrescenta que para além dos documentos referidos anteriormente estarem inseridos nas suas políticas ou planos de SI, nos mesmos podem ser encontrados também um conjunto de definições dos diferentes conceitos utilizados na área e das diferentes funções existentes.

Através da informação dada pelo entrevistado, e embora os tipos de informação não se encontrem documentados individualmente, verifica-se que, ao contrário do que acontece com os princípios e as políticas, 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. Embora não seja da mesma forma que o COBIT5SI recomenda, nesta seção a forma como a organização opera não evidencia carecer de tratamento, para além do facto de não terem nenhum relatório de revisão de segurança da informação.

De seguida, e antes de passarmos à análise da matriz já referida, tentamos perceber quais os *stakeholders* que a organização contava na sua estrutura organizacional. Juntamente com o entrevistado procedemos a um ajustamento, retirando aqueles que não se encaixavam na realidade da organização. Na tabela 6.10, poder-se-á consultar aqueles que existem na organização e os que não serão considerados pois não se verificam na organização em análise. Mais ainda, recolhemos a informação do entrevistado daquelas funções que na organização estão associadas à mesma pessoa. Em termos de nomenclatura, a única alteração que o entrevistado indicou refere-se ao facto de o chefe de administração de TSI ser a área de administração de sistemas, sendo este o conceito que se utilizou na matriz.

O passo seguinte passou por cruzar os diferentes tipos de informação existentes na organização com os diferentes tipos de *stakeholders*, visando perceber quais destes últimos origina (O), aprova (A), é informado (I), ou utiliza (U) os diferentes tipos de informação. Os resultados encontram-se demonstrados na figura 6.11.

STAKEHOLDERS	C. Hospitalar
Interno: Organização	
Conselho	x
Presidente e Diretor Executivo (CEO - *Chief Executive Officer*)	√
Diretor Executivo de Finanças (CFO - *Chief Financial Officer*)	√
Diretor das Operações (COO - *Chief Operating Officer*)	√
Diretor de Risco (CRO - *Chief Risk Officer*)	√
Comité de Direção de Segurança da Informação (ISSC)	x
Diretor de Segurança da Informação (CISO)	√
Executivos	x
Sócios	x
Comités de Direção de Projetos e Programas	x
Direção da Estrutura	√
Comité de Gestão do Risco do Negócio (ERM - *Enterprise Risk Management*)	≈ CRO
Chefe de Recursos Humanos	√
Consultoria	x
Auditoria	√
Gabinete de gestão de projetos e programas (PMO - *Project Management Office*)	x
Gabinete de gestão de valor (VMO - *Value Management Office*)	x
Interno: TI	
Comité de Estratégia de TI	x
Diretor da Informação (CIO - Chief Information Officer)	√
Chefe de Estrutura	≈ CIO
Chefe de Desenvolvimento	≈ CIO
Chefe das Operações TI	√
Chefe da Administração de TSI	√
Gestor de Serviços	x
Gestor da Segurança da Informação (ISM)	≈ CISO
Gestor da Continuidade de Negócio	x
Diretor da Privacidade	x
Externo	
Investidores	x
Seguradoras	√
Autoridade Legal	√
Reguladoras	√
Parceiros do Negócio	x
Vendedores/Fornecedores	√
Auditores Externos	x

√ presente | x não existe | ≈ função associada a

Tabela 6.10 Checklist de stakeholders baseada nas recomendações do COBIT5SI

Como já verificado aquando a análise das práticas, 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. No entanto, verifica-se que o CIO acaba por apoiar o CISO em todo o tipo de informação, ainda que esta função não tenha um foco maior na associação das práticas de segurança na organização verificada anteriormente. Em termos de importância nos tipos de informação, seguem-se o administrador de sistemas e o chefe de projeto, sendo que, neste caso, nenhum deles se encontra numa posição onde

poderá aprovar algum tipo de informação. No que toca a gestão de topo, com base na informação recolhida, esta tem uma posição acima de tudo de aprovação, participando de modo ativo unicamente na definição dos requisitos de segurança da informação. Aliás, este tipo de informação é o único que recebe *input* de todos os *stakeholders* do centro hospitalar. Relativamente ao *input* dos *stakeholders* externos, no geral, marcam presença na origem da estratégia, plano e requisitos de segurança da informação, uma vez que estes se tratam da grande base desta área.

Na verdade, não existe uma solução para esta matriz, mas é importante ter conhecimento de onde atuam os *stakeholders* da organização, podendo perceber-se se a alocação dos mesmos está a ser bem feita ou não. Esta informação pode ser uma mais-valia para a organização utilizar na distribuição de tarefas pela sua estrutura organizacional.

		Tipo de Informação									
Stakeholder		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

Tabela 6.11 Matriz Stakeholders vs. Tipos de Informação de Segurança da Informação da organização em análise baseada nas recomendações do COBIT5SI

7. Conclusão

Sendo a segurança da informação uma preocupação constantemente presente no dia-a-dia das organizações, esta dissertação focou-se em desenvolver este tópico apresentando vários conceitos, exemplos práticos e sistemas de gestão aplicados nesta temática. Para além da segurança da informação, apresenta-se também uma vertente de auditoria, a qual permite o desenvolvimento teórico sobre os diferentes normativos a aplicar neste tópico. Pretendeu-se, desta forma, conjugar num só documento informações acerca do que é segurança da informação e do que se entende por sistema de gestão de segurança da informação, e a apresentação de normativos que têm como objetivo apoiar as organizações no desenvolvimento e implementação desses mesmos sistemas.

Para que fosse possível espreitar um pouco a realidade, desenvolveu-se também um caso de estudo, baseado num dos normativos estudados, o COBIT, analisando princípios e políticas implementadas em determinada organização, assim como a fase de desenvolvimento dos processos postos em prática, as estruturas organizacionais e práticas adjacentes, e ainda tipos de informação e *stakeholders* presentes na organização. O desenvolvimento do caso de estudo permitiu pôr em prática algumas técnicas de auditoria e percecionar como a teoria se aplica na vida real.

7.1 Discussão de Resultados

Em termos teóricos, pretendeu-se identificar quais os normativos que apresentavam um forte âmbito em segurança da informação, e verificou-se que grande parte da revisão bibliográfica efetuada indicava os mesmos três normativos: a norma internacional ISO27001, a libraria ITIL e o *framework* COBIT.

Posteriormente, foi efetuada uma breve análise do que cada um destes normativos representava, para se finalizar a abordagem teórica da presente dissertação com uma pequena comparação entre os mesmos. Essa análise comparativa permitiu concluir que, tanto a libraria ITIL como o *framework* COBIT se encontram alinhados à norma internacional direcionada ao sistema de gestão de segurança da informação, a ISO27001. Esta situação representa uma mais-valia para as organizações, pois, apresentando os três normativos âmbitos diferentes, as organizações têm a oportunidade de serem certificadas com a norma ISO27001, extremamente focada na área da segurança da informação, e de conseguirem implementar um *framework* com um maior foco na gestão de serviços, como é o caso da ITIL, ou com mais enfoque na governança e gestão da organização, como se verifica com o COBIT.

Em suma, dentro da temática de segurança da informação, é uma mais-valia para as organizações considerarem estes três normativos, pois a ISO27001 apresenta controlos específicos em segurança da informação, a ITIL disponibiliza um processo focado no desenvolvimento de um sistema de gestão da segurança da informação, e o COBIT alinha os seus diferentes processos, estruturas, políticas, etc., com os objetivos da organização, permitindo uma governança e gestão adequadas da segurança da informação.

Já na análise da parte prática efetuada, com base nas informações que obtivemos do entrevistado, deduz-se que a organização em análise tem presentes na sua atividade grande parte das recomendações assinaladas no COBIT5SI, pois os princípios e políticas analisados encontram-se presentes nas preocupações do departamento de SI, os processos recomendados estão todos a ser implementados, e os diferentes tipos de informação estão intrínsecos nas atividades do dia-a-dia da organização. De notar, que o entrevistado referiu que a organização cumpre com os requisitos da norma internacional ISO27001, e verifica-se que grande parte das recomendações prestadas pelo COBIT5SI vão ao encontro do que está a ser implementado na organização.

Como pontos de melhoria, verifica-se que a organização da documentação no que toca a princípios e políticas poderia ser otimizada, para que fosse mais fácil a toda a organização ter acesso à mesma informação, e recomenda-se que em termos de processos se comece a definir objetivos para além das práticas associadas a cada um deles, por forma a conseguirem monitorizar o desempenho dos mesmos, acompanhando assim a evolução a nível processual na área de segurança da informação.

Ainda relativamente a pontos a melhorar, ressaltou que em termos de estrutura organizacional o departamento de SI se encontra com alguma indefinição nas funções desempenhadas, sendo que pelo que foi apurado, grande parte das tarefas são alocadas ao CISO, acabando por esta função se encontrar sobrecarregada. No entanto, a organização poderá utilizar a matriz disponibilizada na secção 6.2.5, como base para a alocação de funções ou tarefas aos diferentes colaboradores do departamento de SI.

Verifica-se que tanto em termos teóricos como em termos práticos, a utilização de diferentes normativos numa organização é uma mais-valia, pelo menos quando a temática se trata de segurança da informação, visto que, como cada normativo 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.

7.2 Limitações e Trabalhos Futuros

Com a presente dissertação, foi possível, numa vertente pessoal, adquirir mais conhecimentos numa temática que me atrai e compreender um pouco mais do que se trata o processo de auditoria. O trabalho de pesquisa, preparação, execução e posterior análise permitiu-me pôr em prática os conhecimentos adquiridos ao longo do mestrado, o que só me motiva ainda mais para continuar por este caminho.

No entanto, verificaram-se algumas dificuldades no desenvolvimento da presente dissertação. O facto deste trabalho se focar na área de segurança da informação, que constava ser uma área na qual os conhecimento técnicos e de conceitos, inicialmente, era limitado, manifestou-se como uma limitação. O estudo e adjacente revisão bibliográfica nesta área permitiram a aquisição de conhecimentos, ainda que numa perspetiva teórica e não prática.

Outra limitação que interessa referir, centra-se na dificuldade sentida no contacto com os diferentes hospitais. Arranjar parcerias para o desenvolvimento desta dissertação foi mais difícil do que se estava à espera, sendo que o contacto referido ao longo desta dissertação traduz-se na única resposta positiva obtida, limitando assim a realização do caso de estudo a uma única entidade.

Para trabalhos futuros, existem várias abordagens que podem ser tomadas:

- Elaboração de um questionário junto dos utilizadores do SI da organização em análise na presente dissertação, com o intuito de se analisar como a comunicação das políticas, princípios, processos de segurança da informação, entre outros, está a ser efetuada, avaliando a forma como todos estes elementos são conhecidos e aplicados;

- Utilizar a mesma abordagem para avaliar outras organizações de saúde presentes no SNS, para se conseguir perceber a forma como a gestão da segurança da informação está a ser efetuada e gerida em organizações deste tipo;

- Dar continuidade a este caso prático, fazendo mais duas análises; uma com base na norma internacional ISO27001, e outra com base no *framework* ITIL. Dessa forma, poder-se-ia fundamentar ou confrontar as conclusões teóricas com uma componente prática.

Referências Bibliográficas

Amaral, L. (1994). Planeamento de Sistemas de Informação, Universidade do Minho.

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

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. Florida, University of South Florida

Bocij, P., A. Greasley and S. Hickie (2008). Business Information Systems: Technology, Development & Management, Pearson Education Limited.

BSI (2008). BSI-Standard 100-1 Information Security Management Systems (ISMS).

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.

Carneiro, A. (2009). Auditoria e Controlo de Sistemas de Informação, FCA - Editora de Informática.

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

Carvalho, J. Á. (1996). Desenvolvimento de Sistemas de Informação: da Construção de Sistemas Informáticos à Reengenharia Organizacional, Universidade do Minho.

Carvalho, J. Á. (2000). "Information System? Which one do you mean?" Kluwer Academic Publishers.

Cascarino, R. (2007). Auditor's Guide to Information Systems Auditing, John Wiley & Sons.

Champlain, J. J. (2003). Auditing Information Systems, John Wiley & Sons.

Clinch, J. (2009). ITIL V3 and Information Security - White Paper, Best Management Practice.
CMMIInstitute (2006). CMMI for Development. v1.2.

Costa, C. B. d. (2010). Auditoria Financeira - Teoria & Prática, Rei dos Livros.

Dimitriadis, C. K. (2011). "Information Security From a Business Perspective: A Lottery Sector Case Study " ISACA Journal 1.

Falkenberg, E. D., W. Hesse, P. Lindgreen, B. E. Nilsson, J. L. H. Oei, C. Rolland, R. K. Stamper, F. J. M. V. Assche, A. A. Verrijn-Stuart and K. Voss (1998). A Framework of Information System Concepts, International Federation for Information Processing.

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.".

Günther, H. (2006). "Pesquisa Qualitativa Versus Pesquisa Quantitativa: Esta É a Questão?" Psicologia: Teoria e Pesquisa 22(201-210).

ISACA (2010). Certified Information Systems Auditor - Review Manual 201 0, ISACA.

ISACA (2010). IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals, ISACA.

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

ISACA (2012). CoBIT 5 for Information Security.

ISO (2005). ISO/IEC 27001:2005 - Information technology — Security techniques — Information security management systems — Requirements.

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

ITGI (2007). COBIT 4.1, IT Governance Institute.

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

ITProcessMaps (2013). ITIL® and the ITIL® Process Map, IT Process Maps GbR

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.

Livesey, C. (2006). The relationship between Positivism, Interpretivism and sociological research methods, Sociology Central.

Lucey, T. (2005). Management Information Systems, Thomson.

Mack, N., C. Woodsong, K. M. MacQueen, G. Guest and E. Namey (2005). Qualitative Research Methods: A Data Collector's Field Guide Family Health International.

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.

Moresi, E. (2003). Metodologia da Pesquisa, Universidade Católica de Brasília

Musaji, Y. F. (2001). Auditing and Security, John Wiley & Sons.

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

Oliveira, J. A. (2006). Método de Auditoria a Sistemas de Informação, Porto Editora.

Oliveira, W. (2001). Segurança da Informação: Técnicas e Soluções, Centro Atlântico.

Oz, E. (2009). Management Information System, Thomson.

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

Piattini, M. (2000). Auditing Information Systems, Idea Group Publishing.

Raupp, F. M. and I. M. Beuren (2004). Metodologia da pesquisa aplicável às ciências sociais. Como elaborar trabalhos monográficos em contabilidade. Atlas.

Ray, A. K. and T. Acharya (2004). Information Technology: Principles and Applications, Prentice-Hall of India - Private Limited.

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.

Santos, R. A. (2009). Data Warehouse: Modelo de Auditoria e Controlo Interno.

Sayana, S. A. (2002). "The IS Audit Process " ISACA Journal 1.

Seeram, S. K. (2012). "Introduction to COBIT 5." ITSM Portal.

Senft, S. and F. Gallegos (2009). Information Technology Control and Audit, Taylor & Francis Group.

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.

Silva, P. T., H. Carvalho and C. B. Torres (2003). Segurança dos Sistemas de Informação: Gestão Estratégica da Segurança Empresarial, Centro Atlântico.

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 System Standards: A Comparative Study of the Big Five." International Journal of Electrical & Computer Sciences Vol: 11 No: 05.

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

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.

Yin, R. K. (2009). Case Study Research - Design and Methods, SAGE Publications.

Anexo I - Linhas gerais da entrevista

Caraterização da Empresa

No website da organização, obtive algumas das informações que necessitava para a caraterização da empresa.

Qual o nome da organização?

- Centro Hospitalar

Localização

- (Confidencial)

Missão

- Tem por missão prestar, com elevados níveis de qualidade e eficiência, cuidados de saúde diferenciados, em articulação com a rede de saúde primária e com hospitais do Serviço Nacional de Saúde, apostando na motivação e satisfação dos seus profissionais.
Faz, igualmente, parte da sua missão o ensino pré e pós–graduado, bem como o desenvolvimento de formação considerada necessária ao desenvolvimento dos seus colaboradores.
A investigação e o desenvolvimento científico em todas as áreas das ciências da saúde fazem também parte da missão do Centro Hospitalar.

Visão

- A visão assenta no continuado desenvolvimento e aperfeiçoamento técnico e científico nas valências que integra, na qualidade da assistência prestada aos utentes e na experiência na gestão clínica. Isto, mediante a avaliação sistemática de procedimentos e resultados nesta área, numa lógica de transparência e de responsabilização.

Objetivos Estratégicos

- Tendo em conta o enquadramento e posicionamento do Centro Hospitalar, o Conselho de Administração assume os seguintes objectivos estratégicos e define as acções a desenvolver, bem como as medidas a implementar para obter os resultados que deseja atingir:

  - Clarificação e potenciação do posicionamento estratégico do Centro Hospitalar na rede de oferta de cuidados de saúde nas áreas do Grande Porto e de Entre Douro e Vouga;
  - Gestão clínica activa;
  - Atenção permanente aos processos clínicos fundamentais;
  - Preocupação permanente com a satisfação dos utentes;
  - Reforço do nível de integração com a comunidade em que o Centro Hospitalar está inserido;
  - Melhoria do processo de gestão das pessoas, de forma a motivar continuamente as equipas que integram o Centro Hospitalar;

- Adequação da liderança de topo e intermédia e da estrutura organizacional às exigências da empresarialização do Centro Hospitalar;
- Protecção do ambiente e reforço da segurança, considerando estas áreas como transversais a toda a organização;
- Desenvolvimento dos sistemas de informação, da gestão orçamental e do controlo de gestão;
- Gestão eficiente das instalações e dos equipamentos;
- Gestão criteriosa dos custos com impacto imediato em várias áreas, nomeadamente: aquisições, aprovisionamento e logística;
- Aplicação de regras correspondentes a uma boa gestão financeira para atingir o equilíbrio económico;
- Fomento da comunicação aos níveis interno e externo;
- Melhoria dos níveis de qualidade nos serviços prestados, nomeadamente ao nível dos indicadores de qualidade acordados com a tutela.

Ficando a faltar as seguintes questões:

Qual o Classificação das Atividades Económicas (CAE)?

Qual o ano de início de atividade?

Numa pequena descrição, indique quais as principais atividades e serviços agregados?

Trata-se de uma micro, pequena, média ou grande empresa?

Qual a designação da empresa em termos jurídicos? (Pública, privada, ...)

Organigrama da Empresa e de TSI

Tive acesso ao organigrama da empresa no website da instituição

Gostaria de saber qual a estrutura organizacional que serve de base no departamento de TSI?

Processos

O Cobit 5 está estruturado numa base de domínios e processos. Assim sendo, de uma forma não muito aprofundada, vamos tentar perceber quais os processos que têm implementados na vossa organização e em que fase de implementação se encontram, caso existam.

Checklist dos processos

Processos - Se existirem, escala de 1 a 5 (tendo como base a escala utilizada nos nivéis de maturidade 1- Inicial; 2- Repetível, todavia intuitivo; 3- Definido; 4- Gerido e Mensurável; 5- Otimizado)

Governança	**Avaliar, Dirigir e Monitorizar (EDM)**		
	EDM 01	Assegurar a definição e manutenção de um framework de governança	
	EDM 02	Assegurar a entrega de benefícios	
	EDM 03	Assegurar a otimização de risco	
	EDM 04	Assegurar a otimização de recursos	
	EDM 05	Assegurar a transparência dos stakeholders	

Gestão	**Alinhar, Planear e Organizar (APO)**		
	APO 01	Gerir o framework de gestão de TSI	
	APO 02	Gestão da estratégia	
	APO 03	Administrar a estrutura organizacional	
	APO 04	Gerir a inovação	
	APO 05	Gestão de portfólio	
	APO 06	Gestão de orçamentos e custos	
	APO 07	Gestão dos recursos humanos	
	APO 08	Gerir relações	
	APO 09	Administrar acordos de serviços	
	APO 10	Gerir fornecedores	
	APO 11	Gestão da qualidade	
	APO 12	Gestão de risco	
	APO 13	Gestão da segurança	

Gestão	**Construir, Adquirir e Implementar (BAI)**		
	BAI 01	Gestão de programas e de projetos	
	BAI 02	Gerir a definição de requisitos	
	BAI 03	Administrar a identificação e construção de soluções	
	BAI 04	Gestão de disponibilidade e de capacidade	
	BAI 05	Administrar a capacitação para a mudança na organização	
	BAI 06	Gestão da mudança	
	BAI 07	Gerir a aceitação e a transição da mudança	
	BAI 08	Gestão de conhecimento	
	BAI 09	Gestão de ativos	
	BAI 10	Gerir a configuração	

Gestão	Entrega, Serviço e Suporte (DSS)	
	DSS 01	Gestão de operações
	DSS 02	Gerir solicitações de serviços e administrar incidentes
	DSS 03	Gestão de problemas
	DSS 04	Gestão da continuidade
	DSS 05	Gerir serviços de segurança
	DSS 06	Gerir os controlos dos processos de negócio

Gestão	Monitorizar, Avaliar e Aferir (MEA)	
	MEA 01	Monitorizar, avaliar e aferir o desempenho e a conformidade
	MEA 02	Monitorizar, avaliar e aferir o sistema de controlo interno
	MEA 03	Monitorizar, avaliar e aferir a conformidade com requisitos externos

Políticas, Princípios e Frameworks

Um dos facilitadores referidos no COBIT5SI é a existência de mecanismos de comunicação que transmitam instruções dos órgãos sociais e dirigentes à restante organização. Vamos tentar perceber o que existe definido na área de Segurança da Informação, tendo como o base o referido no COBIT5SI.

Existem documentos formais? Podemos ter acesso? Se não existir, perguntar se têm preocupações nesse sentido.
Por exemplo: em controlo de acesso tem alguma coisa definida? o quê e de que forma é aplicada e transmitida?

Princípios	Suporte ao Negócio	
	Foco no Negócio	
	Fornecer qualidade e valor aos stakeholders	
	Cumprir com os requisitos legais e regulamentares relevantes	
	Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação	
	Avaliar atuais e futuras ameaças à informação	
	Promover a melhoria contínua da segurança da informação	

Princípios	Defender o Negócio	
	Adotar uma abordagem baseada no risco	
	Proteger informação confidencial	
	Concentrar-se nas aplicações de negócio críticas	
	Desenvolver sistemas de forma segura	

Princípios	Promover um comportamento responsável de segurança da informação	
	Agir de forma ética e profissional	
	Fomentar uma cultura positiva de segurança da informação	

Outros Princípios	

Políticas	Impulsionadas pela função de segurança da informação	
	Controlo de acesso	
	Pessoal de segurança de informação	
	Meio físico e ambiental de segurança de informação	
	Resposta a incidentes	

Outras Políticas	

Esta parte das políticas não é preciso ser efetuada de forma muito aprofundada. O objetivo é compreender se o departamento de informática tem conhecimento da existência destas políticas, também para percebermos se a comunicação é transversal, e se o órgãos superiores têm o cuidado de transmitir a todos os seus departamentos as políticas base existentes.

Políticas	Impulsionadas por outras funções dentro da organização	
	Continuidade do negócio e recuperação de desastres	
	Gestão de ativos	
	Regras de comportamento (uso aceitável)	
	Adquirir sistemas de informação, desenvolvimento e manutenção de software	
	Gestão de fornecedores	
	Gestão das operações e da comunicação	
	Conformidade	
	Gestão de Risco	

Documentos Relevantes	
Estratégia de Segurança da Informação	
Orçamento de Segurança da Informação	
Plano de Segurança da Informação	
Requisitos de Segurança da Informação	
Material de consciencialização	
Relatórios de Avaliação de Segurança da Informação	
Painel de Segurança da Informação	

Outros Documentos

Neste capítulo, o COBIT5SI apresenta-nos um modelo de estrutura organizacional, com exemplos de papéis e estruturas frequentemente encontradas nas organizações, e também nos direciona para algumas práticas cuja responsabilidade de definição e implementação está associada a certos papéis. Vamos tentar perceber o que se verifica nesta organização, baseando a nossa análise neste capítulo.

se não existirem com esta denominação, obter outros nomes de papéis dentro da organização com aquele tipo de funções

Processos de Governança	Funções em Segurança da Informação	
	CISO (Diretor de Segurança da Informação)	
	ISSC (Comité de Direção de Segurança da Informação)	
	ISM (Gestor de Segurança de Informação)	
	ERM (Gestão do Risco da Empresa) Comité	
	Responsáveis pela Informação / Proprietários da empresa	

Outras Funções em Segurança da Informação	

Caso a função ISSC esteja prevista na estrutura da organização

Perceber quais os papéis pertencentes ao comité

Processos de Governança	Representantes no ISSC	
	CISO (Diretor de Segurança da Informação)	
	ISM (Gestor de Segurança de Informação)	
	Responsáveis pela Informação / Proprietários da empresa	
	Gestor de TSI	
	Representantes de funções especializadas	

Outros Representantes	

Cheklist das práticas associadas a cada função – R (Responsável pela Definição) A (Responsável pela Implementação) C (Consultado) I (Informado)

- Cada prática é efetuada?
- Quem faz cada prática? – o que o COBIT5SI prevê ou outra pessoa (delegação)

	CISO (Chief Information Security Officer)	Nível de Envolvimento
Práticas	Identificar e comunicar as ameaças de segurança da informação, assim como os comportamentos desejados e as mudanças necessárias para enfrentar as mesmas. Função A -	
	Garantir que a gestão do ambiente e das instalações se adequa aos requisitos de segurança da informação. Função A -	
	Proteger contra malware. Função A -	
	Gerir a segurança na conectividade e de rede. Função A -	
	Gerir a segurança de terminais. Função A -	
	Gerir a identidade dos utilizadores e o acesso lógico. Função A -	
	Gerir o acesso físico a ativos de TSI. Função A -	
	Monitorizar a infraestrutura para eventos relacionados com a segurança. Função A -	
	Proporcionar meios para melhorar a eficiência e eficácia da função de segurança da informação (por exemplo, através da formação do pessoal de segurança da informação; documentação de processos, tecnologias e aplicações; e padronização e automatização do processo). Função A -	
	Acompanhar a gestão de riscos de TSI. Função R -	
	Definir e comunicar uma estratégia de segurança da informação que esteja alinhada com a estratégia da organização. Função R -	
	Pesquisar, definir e documentar os requisitos de segurança da informação. Função R – equipa de sistema	
	Validar os requisitos de segurança da informação com os stakeholders, patrocinadores do negócio e pessoal de execução técnica. Função R – chefe do projeto, da parte de informática	

Caso a função ISSC esteja prevista na estrutura da organização

Se não existir, tentar perceber quais as funções que cobrem estas práticas dentro do RACI

	ISSC (Information Security Steering Committee)	Nível de Envolvimento
Práticas	Definir e comunicar uma estratégia de segurança da informação que esteja alinhada com a estratégia da organização. Função A - CISO	
	Pesquisar, definir e documentar os requisitos de segurança da informação. Função A - CISO	
	Validar os requisitos de segurança da informação com os stakeholders, patrocinadores do negócio e pessoal de execução técnica. Função A – chefe do projeto da solução de negócios	
	Desenvolver políticas e procedimentos de segurança da informação. Função A - CISO	
	Desenvolver um plano de segurança da informação que identifica o ambiente de segurança da informação e os controlos a serem implementados pela equipa do projeto para proteger os ativos da organização. Função A – chefe do projeto	
	Garantir que o impacto potencial das mudanças é avaliado. Função A – chefe do projeto	
	Recolher e analisar dados de desempenho e conformidade relacionados à segurança da informação e à gestão de riscos da informação. Função A – chefe do projeto	
	Estabelecer, acordar e comunicar o papel do CISO e do ISM. Função R – conselho de administração até nomeação da equipa do ISMC	
	Aumentar a visibilidade da função de segurança da informação dentro da empresa e, potencialmente, fora da mesma. Função R – CISO + núcleo de gestão de riscos	
	Contribuir, em toda a organização, nos esforços de gestão da continuidade do negócio. Função R – CISO + núcleo de gestão de riscos	

	ISM (Information Security Manager)	Nível de Envolvimento
Práticas	Desenvolver e comunicar uma visão comum para a equipa de segurança da informação que esteja alinhada com a visão da organização. Função R - CISo	
	Gerir a alocação do pessoal de segurança da informação de acordo com os requisitos do negócio. Função R - CISO	
	Realizar avaliações de risco da informação e definir o perfil de risco da mesma. Função R – resp. da aplicação correlacionada com a informação	
	Gerir funções, responsabilidades, direitos de acesso e níveis de autoridade. Função R – gestor de projeto da parte informática + diretor do projeto (utilizador)	
	Desenvolver um plano de segurança da informação que identifica o ambiente de segurança da informação e os controlos a serem implementados pela equipa do projeto para proteger os ativos da organização. Monitorizar esses controlos internos e ajustar/melhorar quando necessário. Função R – chefe do projeto	
	Identificar e comunicar os pontos fracos de segurança da informação, assim como os comportamentos desejáveis e as mudanças necessárias para enfrentar os mesmos. Função R - CISO	
	Proporcionar meios para melhorar a eficiência e eficácia da função de segurança da informação (por exemplo, através da formação do pessoal de segurança da informação; documentação de processos, tecnologias e aplicações; e padronização e automatização do processo). Função R – CISO + resp. aplicativos	
	Recolher e analisar dados de desempenho e conformidade relacionados à segurança da informação e à gestão de riscos da informação. Função R - CISO	
	Garantir que a gestão do ambiente e das instalações se adequa aos requisitos de segurança da informação. Função R - CISO	

	ERM (Enterprise Risk Management) Comité	Nível de Envolvimento
Práticas	Aconselhamento sobre a estratégia de segurança da informação definida pelo ISSC. Função R -	
	Estabelecer os níveis de tolerância ao risco da organização. Função A – Cons. De Administração	
	Definir e implementar a avaliação de risco e as estratégias de resposta. Função A -	
	Rever a avaliação de risco da informação e os perfis de risco. Função A - CISO	

	Responsáveis pela Informação / Proprietários da empresa	Nível de Envolvimento
Práticas	Comunicar, aconselhar e coordenar os esforços da gestão de risco de informações com os chefes hierárquicos. Função R – (e A) administrador informático da aplicação	
	Reportar as mudanças nos processos e/ou nas estratégias de negócio (isto é, novos produtos ou serviços) ao ISSC. Função R – responsável pela aplicação do lado do utilizador	
	Aumentar a visibilidade da função de segurança da informação e das políticas e procedimentos de segurança da informação dentro da empresa. Função R - CISO	

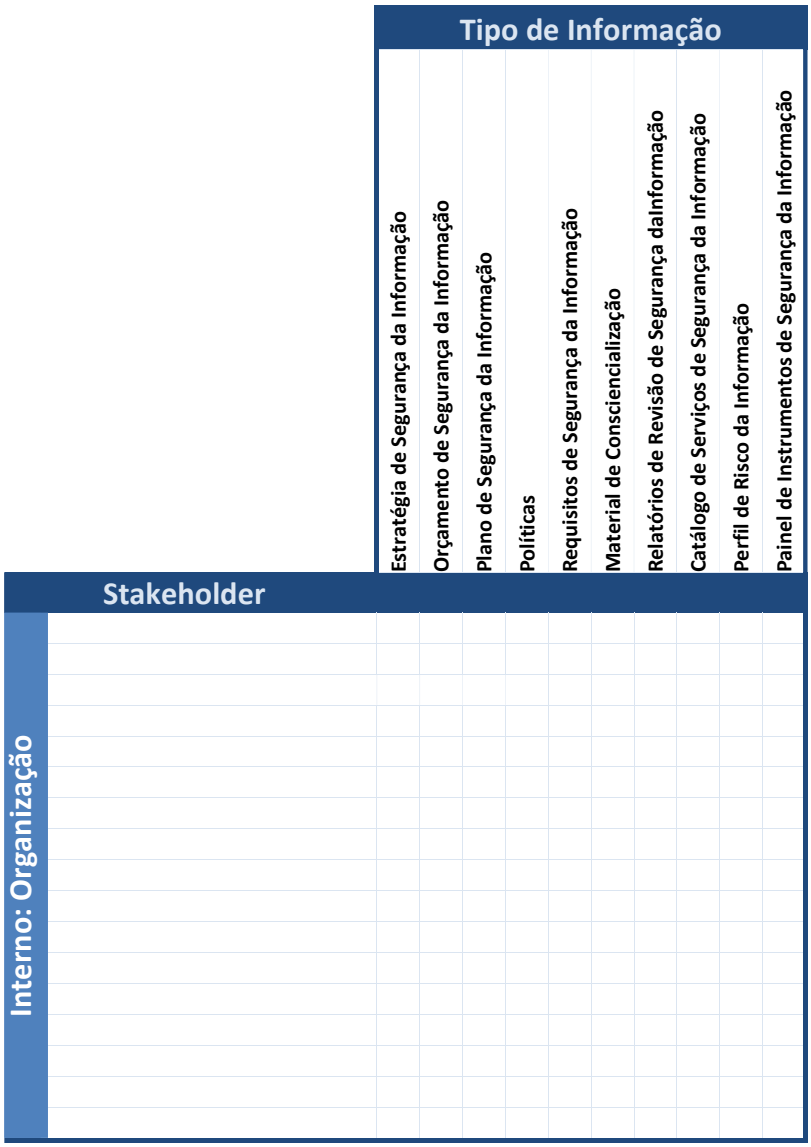
Informação

Nos dias que correm a informação é o recurso chave para o sucesso de qualquer organização. Como tal é importante saber como esta está incorporada na organização e como pode ser usada para gerir a segurança da informação. Para isso vamos tentar perceber como esta estruturada na organização relativamente aos stakeholders.

Reconfigurar Lista de Stakeholders com o Entrevistado

Stakeholders		
Int.: Organização	Conselho Geral	
	(Presidente e Diretor Executivo) CEO	
	(Diretor Executivo de Finanças) CFO	
	(Diretor de Operações) COO	
	(Diretor de Risco) CRO	
	(Comité de Direção de Segurança da Informação) ISSC	
	(Diretor de Segurança da Informação) CISO	
	Empresários	
	Proprietários do Processo de Negócio	
	Comités de Direção de Projetos e Programas	
	Direção da Estrutura	
	Comité de (ERM) Gestão do Risco da Empresa	
	Chefe de Recursos Humanos	
	Consultoria	
	Auditoria	
	(Gabinete de Gestão de Projetos e Programas) PMO	
	(Gabinete de Gestão de Valor) VMO	
Interno: TSI	Comité de Estratégia (executivo de TSI)	
	(Diretor Executivo de Informação) CIO	
	Chefe da Estrutura	
	Chefe de Desenvolvimento	
	Chefe das Operações de TSI	
	Chefe da Administração de TSI	
	Gestor de Serviços	
	(Gestor de Segurança de Informação) ISM	
	Gestor da Continuidade do Negócio	
	Responsável pela Privacidade	
Externo	Investidores	
	Seguradoras	
	Autoridades (aplicação da lei)	
	Reguladores	
	Sócios	
	Vendedores/Fornecedores	
	Auditories Externos	

Preencher Informação vs Stakeholders – Perceber quem é que aprova (A), origina (O), é informado (I), ou usa (U) determinado tipo de informação



Anexo II - Descrição dos princípios e políticas do COBIT5SI

Princípios – Suporte ao Negócio

Foco no Negócio
Garantir que a segurança da informação está integrada nas atividades essenciais da organização.
Fornecer qualidade e valor aos stakeholders
Certificar-se de que a segurança da informação agrega valor e atende aos requisitos de negócios.
Cumprir com os requisitos legais e regulamentares relevantes
Certificar-se de que as obrigações legais são cumpridas, que as expectativas dos stakeholders são geridas e que as penalidades civis ou criminais são evitadas.
Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação
Fornecer suporte aos requisitos do negócio e gerir o risco da informação.
Avaliar atuais e futuras ameaças à informação
Analisar e avaliar as ameaças emergentes de segurança da informação para que seja possível atuar de forma informada e em tempo útil, conseguindo assim mitigar os riscos.
Promover a melhoria contínua da segurança da informação
Reduzir os custos, melhorar a eficiência e eficácia e promover uma cultura de melhoria contínua na segurança da informação.

Princípios – Defender o Negócio

Adotar uma abordagem baseada no risco
Certificar-se de que o risco é tratado sistematicamente e de forma eficaz.
Proteger informação confidencial
Evitar a divulgação de informações classificadas (ou seja, confidenciais ou sensíveis) para pessoas não autorizadas.
Concentrar-se nas aplicações de negócio críticas
Priorizar recursos escassos de segurança da informação, protegendo as aplicações de negócio onde um incidente de segurança da informação teria um maior impacto no negócio.
Desenvolver sistemas de forma segura
Criar qualidade, sistemas de custo-benefício nos quais os empresários podem confiar (por exemplo, que são consistentemente robustos, precisos e confiáveis)

Princípios – Promover um comportamento responsável de segurança da informação

Agir de forma ética e profissional
Garantir que atividades relacionadas à segurança da informação são feitas de forma confiável, responsável e eficaz.
Fomentar uma cultura positiva de segurança da informação
Proporcionar uma influência positiva na segurança da informação, aplicando-a no comportamento dos utilizadores finais; reduzir a probabilidade de ocorrerem incidentes de segurança da informação, e limitar o seu impacto potencial no negócio.

Políticas – Impulsionadas pela função de segurança da informação

Controlo de acesso
Ministra o acesso adequado dos stakeholders, internos ou externos, para atingir os objetivos de negócios; deve garantir que o acesso de emergência é adequadamente permitido e revogado de forma oportuna.
Pessoal de segurança de informação
Executar uma verificação regular do background de todos os funcionários e pessoas nas posições mais críticas; adquirir informações sobre o pessoal mais importante nas posições de segurança da informação; desenvolver um plano de sucessão para todas as posições críticas na área de segurança da informação; verificar se todo o pessoal de segurança da informação tem as habilidades necessárias, atualizadas e pertinentes, e as certificações relacionadas.
Meio físico e ambiental de segurança de informação
Fornecer orientação sobre a proteção dos locais físicos e sobre os controlos relacionados com o meio ambiente que proporcionam recursos que servem de apoio nas operações; contribui para a otimização de custos de seguros.
Resposta a incidentes
Aborda a necessidade de responder a incidentes atempadamente, para recuperar as atividades empresariais o mais rápido possível.

Anexo III - Descrição dos processos do COBIT5SI

Processos de Governança - Avaliar, Dirigir e Monitorizar (EDM)

EDM 01	**Assegurar a definição e manutenção de um framework de governança**
	Analisar e articular os requisitos de governança de TSI da organização, e executar e manter estruturas, princípios, processos e práticas base eficazes, havendo claridade no que diz respeito às responsabilidades e autoridades associadas, para se conseguir atingir a missão, meta e objetivos da entidade.

EDM 02	**Assegurar a entrega de benefícios**
	Otimizar a contribuição de valor para o negócio a partir dos processos de negócio, dos serviços de TSI e dos ativos de TSI, resultante de investimentos realizados pela área de TSI a custos aceitáveis.

EDM 03	**Assegurar a otimização de risco**
	Garantir que o apetite e a tolerância de risco da empresa são compreendidos, articulados e comunicados, e que o risco para o valor da empresa relacionado com o uso de TSI é identificado e gerido.

EDM 04	**Assegurar a otimização de recursos**
	Certificar que estão disponíveis recursos adequados e suficientes relacionados a TSI (pessoas, processos e tecnologia), que apoiem os objetivos da empresa de forma eficaz a um custo ideal.

EDM 05	**Assegurar a transparência dos stakeholders**
	Garantir que a medição e relatórios de desempenho e conformidade da área de TSI são transparentes, e que existe a aprovação dos stakeholders nas metas, métricas e ações corretivas necessárias.

Processos de Gestão - Alinhar, Planear e Organizar (APO)

APO 01	**Gerir o framework de gestão de TSI**
	Esclarecer e preservar a missão e visão da governança de TSI. Implementar e manter mecanismos e jurisdição que tratem da gestão da informação e do uso de TSI na organização, que sustentem os objetivos de gestão, cumprindo com os princípios e políticas delineados.

APO 02	**Gestão da estratégia**
	Fornecer uma visão holística do negócio atual, do ambiente de TSI, do sentido a tomar na organização e das iniciativas necessárias para migrar do estado atual para o ambiente futuro desejado. Alavancagem dos elementos essenciais e componentes da arquitetura da empresa, incluindo os serviços prestados externamente e recursos relacionados, com vista a se atingir uma resposta ágil, confiável e eficiente aos objetivos estratégicos.

APO 03	**Administrar a estrutura organizacional** Estabelecer uma arquitetura comum, consistindo-a em processos de negócios, informação, dados, e níveis de arquitetura de aplicações e tecnologia, para uma realização empresarial e das estratégias de TSI eficaz e eficiente, através da criação de modelos e práticas chave que descrevam a linha de base e o objetivo da estrutura. Definir os requisitos para a taxonomia, normas, diretrizes, procedimentos, modelos e ferramentas, e proporcionar uma ligação entre esses componentes. Melhorar o alinhamento, aumentar a agilidade, aprimorar a qualidade da informação e criar potenciais reduções de custos através de iniciativas, tais como a reutilização dos componentes dos elementos constitutivos.

APO 04	**Gerir a inovação** Preservar uma consciência da tecnologia da informação e da evolução dos serviços relacionados, identificar oportunidades de inovação e planear como se pode beneficiar dessa inovação no que toca às necessidades do negócio. Analisar quais as oportunidades empresariais de inovação e melhoria que podem ser criadas pelas tecnologias e serviços emergentes, ou pela inovação de negócio baseada em TSI, bem como através de tecnologias já existentes e estabelecidas e pelo processo de inovação da empresa e de TSI. Influenciar o planeamento estratégico e as decisões da estrutura corporativa.

APO 05	**Gestão de portfólio** Executar o direcionamento estratégico definido para os investimentos em linha com a visão da estrutura corporativa e com as características desejadas para o investimento e serviços relacionados; e considerar as diferentes categorias de investimentos e as restrições de recursos e de financiamento. Avaliar, priorizar e equilibrar programas e serviços, gerindo a procura no âmbito das restrições de recursos e de financiamento, com base no seu alinhamento com os objetivos estratégicos, com o valor da empresa e com o risco. Ativar programas selecionados e transferi-los para serviços prontos para execução. Monitorar o desempenho do portfolio geral de serviços e programas, propondo os ajustes necessários em resposta aos desempenhos registados, ou mudando as prioridades da empresa.

APO 06	**Gestão de orçamentos e custos** Administrar as atividades financeiras relacionadas à TSI, tanto nas funções de TSI como do negócio em geral, abrangendo a gestão do orçamento, dos custos e dos benefícios, e a priorização dos gastos com o uso de práticas formais de orçamento e de um sistema justo e equitativo de alocação de custos para a empresa. Consultar os stakeholders para identificar e controlar os custos totais e os benefícios no contexto dos planos estratégicos e táticos de TSI, e iniciar ações corretivas onde necessárias.

APO 07	**Gestão dos recursos humanos** Proporcionar uma abordagem estruturada para garantir que a estruturação, a atribuição, os direitos de decisão e as competências dos recursos humanos são os ideias. Isso inclui, comunicar os papéis e responsabilidades definidos, os planos de aprendizagem e de crescimento, e as expectativas de desempenho, suportados por pessoas competentes e motivadas.
APO 08	**Gerir relações** Gerir o relacionamento entre o negócio e TSI de uma maneira formal e transparente, que garanta o foco na realização de uma meta comum de conseguir obter com sucesso resultados empresariais tendo em vista os objetivos estratégicos e as limitações relativas aos orçamentos e à tolerância ao risco. Basear a relação numa confiança mútua, usando termos compreensíveis e linguagem comum e uma complacência em tomar o direito e responsabilidade pelas decisões importantes.
APO 09	**Administrar acordos de serviços** Alinhar os serviços que utilizam o TSI e os níveis de serviço com as necessidades e expectativas da empresa, incluindo identificação, especificação, desenho de projeto, publicação, acordo, e acompanhamento de serviços de TSI, dos níveis de serviço e dos indicadores de desempenho.
APO 10	**Gerir fornecedores** Gerir serviços relacionados a TSI providenciados por todos os tipos de fornecedores para atender às necessidades da organização, incluindo a seleção de fornecedores, a gestão de relacionamentos, a gestão de contratos, e a revisão e monitorização do desempenho do fornecedor, para a efetividade e conformidade.
APO 11	**Gestão da qualidade** Definir e comunicar os requisitos de qualidade em todos os processos, procedimentos e resultados da empresa relacionados, incluindo controlos, monitorização contínua, e o uso de práticas e normas comprovadas na melhoria contínua e esforços de eficiência.
APO 12	**Gestão de risco** Identificar, avaliar e reduzir de forma continuada os riscos relacionados a TSI dentro dos níveis de tolerância estabelecidos pela direção executiva da empresa.
APO 13	**Gestão da Segurança** Definir, operacionalizar e monitorar um sistema para a gestão de segurança da informação.

Processos de Gestão - Construir, Adquirir e Implementar (BAI)

BAI 01	**Gestão de programas e de projetos** Gerir todos os programas e projetos da área de investimentos que estejam alinhados com a estratégia da empresa, de uma forma coordenada. Iniciar, planear, controlar e executar programas e projetos, e fechar com uma revisão pós-implementação.
BAI 02	**Gerir a definição de requisitos** Identificar soluções e analisar os requisitos antes da aquisição ou criação para garantir que estão em linha com as necessidades estratégicas da empresa, que cobrem os processos de negócios, aplicações, informação/dados, infraestruturas e serviços. Coordenar com os stakeholders afetados a revisão de opções viáveis, incluindo custos, benefícios e análise de risco adjacentes, e a aprovação de requisitos e soluções propostas.
BAI 03	**Administrar a identificação e construção de soluções** Estabelecer e manter as soluções identificadas que estejam em conformidade com os requisitos da empresa, abrangendo design, desenvolvimento, aquisição/procura e parcerias com fornecedores/vendedores. Administrar a configuração, a preparação dos testes e a gestão dos mesmos, os requisitos de gestão e a manutenção dos processos de negócio, aplicações, informação/dados, infraestruturas e serviços.
BAI 04	**Gestão de disponibilidade e de capacidade** Equilibrar as necessidades atuais e futuras da prestação de serviços a baixo custo com tópicos como a disponibilidade, o desempenho e a capacidade. Incluir a avaliação dos recursos atuais, a previsão das necessidades futuras com base nos requisitos do negócio, a análise de impactos no negócio e a avaliação de risco, tendo em vista planear e implementar ações para atender as necessidades identificadas.
BAI 05	**Administrar a capacitação para a mudança na organização** Maximizar a probabilidade de implementar com sucesso uma mudança organizacional, em toda a empresa, sustentável, de forma rápida e com risco reduzido, cobrindo o ciclo de vida completo da mudança e todos os stakeholders do negócio e de TSI que sejam afetados.
BAI 06	**Gestão da mudança** Gerir todas as mudanças de uma maneira controlada, incluindo as padrão e as de manutenção de emergência relacionadas com os processos de negócio, aplicações e infraestruturas. Isto inclui mudanças de normas e procedimentos, da avaliação de impacto, da priorização e autorização, mudanças de emergência, de rastreamento, de relatórios, de encerramento e de documentação.

BAI 07	**Gerir a aceitação e a transição da mudança** Aceitar formalmente e criar novas soluções operacionais, incluindo planeamento de implementação, conversão de sistemas e de dados, testes de aceitação, comunicação, preparação de lançamento, promoção para produção de processos de negócio ou de TSI novos ou alterados, suporte de produção precoce, e uma revisão pós-implementação.

BAI 08	**Gestão de conhecimento** Manter a disponibilidade de conhecimento relevante, atual, validado e confiável para suportar todas as atividades do processo e facilitar a tomada de decisão. Plano para a identificação, compilação, organização, manutenção, utilização e retirada de circulação de conhecimento.

BAI 09	**Gestão de ativos** Gerir os ativos de TSI através de seu ciclo de vida para se certificar de que o seu uso agrega valor a um custo ideal, de que eles permanecem operacionais (apto para o efeito), de que eles são responsabilizados e protegidos fisicamente, e que os ativos que são fundamentais para apoiar a aptidão do serviço são confiáveis e estão disponíveis. Administrar licenças de software para garantir que é adquirido, mantido e implementado um número ideal de licenças tendo em conta a necessidade do seu uso no negócio, e que o software instalado está em conformidade com as licenças acordadas.

BAI 10	**Gerir a configuração** Definir e manter as descrições e relações entre os principais recursos e capacidades necessárias para prestar serviços que utilizam TSI, incluindo a coleta de informação de configuração, o estabelecimento de linhas de base, a verificação e auditoria da informação de configuração, e atualizar o repositório de configurações.

Processos de Gestão - Entrega, Serviço e Suporte (DSS)

DSS 01	**Gestão de operações** Coordenar e executar as atividades e procedimentos operacionais necessários para prestar serviços internos de TSI assim como os de outsourcing, incluindo a execução de procedimentos operacionais padrão pré-definidos e de atividades de vigilância necessários.

DSS 02	**Gerir solicitações de serviços e administrar incidentes** Fornecer uma resposta rápida e eficaz às solicitações dos utilizadores e uma resolução de todos os tipos de incidentes. Restaurar o serviço normal; registar e atender às solicitações dos utilizadores; e registar, investigar, diagnosticar, escalar e resolver incidentes.

DSS 03	**Gestão de problemas** Identificar e classificar os problemas e a raiz das suas causas, e providenciar soluções atempadas para prevenir incidentes recorrentes. Indicar recomendações de melhorias.

DSS 04	**Gestão de continuidade** Estabelecer e manter um plano que vise permitir que o negócio e a TSI respondam a incidentes e interrupções, a fim de garantir que os processos críticos de negócio e os serviços de TSI necessários continuam operacionais e de manter a disponibilidade da informação a um nível aceitável para a organização.

DSS 05	**Gerir serviços de segurança** Proteger a informação da empresa para manter o nível de risco de segurança da informação aceitável para a organização, de acordo com a política de segurança. Estabelecer e manter as funções de segurança da informação e os direitos de acesso, e realizar a monitorização de segurança.

DSS 06	**Gerir os controlos dos processos de negócio** Definir e manter controlos adequados dos processos de negócio com o intuito de assegurar que as informações relacionadas e tratadas pelos processos de negócios internos ou externos, satisfazem todos os requisitos de controlo de informação relevante. Identificar os requisitos de controlo de informação relevante e gerir e operacionalizar os controlos adequados para garantir que a informação e o seu processamento satisfazem esses requisitos.

Processos de Gestão - Monitorizar, Avaliar e Aferir (MEA)

MEA 01	**Monitorizar, avaliar e aferir o desempenho e a conformidade** Recolher, validar e avaliar os negócios, a TSI e os objetivos e métricas dos processos. Monitorizar esses processos para confirmar que estão a ser realizados de encontro às metas e métricas de desempenho e conformidade e fornecer relatórios sistemáticos e oportunos.

MEA 02	**Monitorizar, avaliar e aferir o sistema de controlo interno** Monitorizar e avaliar continuamente o ambiente de controle, incluindo auto-avaliações e análises de garantia independentes. Permitir à gestão identificar deficiências de controle e ineficiências, e iniciar ações de melhoria. Planear, organizar e manter normas para a avaliação do controlo interno e para atividades de consultoria.

MEA 03	**Monitorizar, avaliar e aferir a conformidade com requisitos externos** Avaliar se processos de TSI e processos de negócios suportados por TSI estão em conformidade com as leis, regulamentos e exigências contratuais. Obter a garantia de que os requisitos foram identificados e respeitados, e integrar a conformidade de TSI com a conformidade da empresa no geral.

Anexo IV - Descrição das funções e/ou estruturas organizacionais do COBIT5SI

CISO (Chief Information Security Officer)
Responsabilidade geral pelo programa de segurança da informação da empresa.
ISSC (Information Security Steering Committee)
Garantir, através de monitorização e avaliação, que são aplicadas boas práticas de segurança da informação de forma eficaz e consistente em toda a empresa.
ISM (Information Security Manager)
Responsabilidade geral pela gestão dos esforços desenvolvidos na área de segurança da informação.
ERM (Enterprise Risk Management) Comité
Responsável pela tomada de decisão da empresa para avaliar, controlar, otimizar, financiar e monitorizar o risco de todas as fontes, com a finalidade de aumentar o valor da empresa para os seus stakeholders a curto e longo prazo.
Guarda da Informação / Proprietário da empresa
Elo de ligação entre o negócio e as funções de segurança da informação.

Anexo V - Descrição dos documentos de segurança do COBIT5SI

Estratégia de Segurança da Informação
Deve ser o estado de arte e estar em consonância com os princípios geralmente reconhecidos. A estrutura e o design da mesma devem ser alinhados à arquitetura corporativa da organização e sua situação específica; devem ser abrangentes e completos; para além de conter todas as informações necessárias, passíveis a recurso, a um nível adequado de detalhe.
Orçamento de Segurança da Informação
Deve ser adequado (garantindo recursos apropriados), preciso e conter montantes corretos e realistas para todos os itens que sejam considerados no mesmo. Além disso, o orçamento deve ser compreensivo, abrangente, completo e alinhado às exigências de segurança corporativa da organização e ao apetite de risco global.
Plano de Segurança da Informação
Deve ser preciso, abrangente e completo, e conter as ações, corretas e realistas, a serem seguidas com base na estratégia de segurança da informação. Além disso, deve ser alinhado à arquitetura corporativa e situação específica da organização, tendo em conta o apetite de risco global.
Requisitos de Segurança da Informação
Devem ser precisos, realistas e alinhados às necessidades de negócio e regulamentares. Para além disso, devem ser disponibilizados atempadamente.
Material de consciencialização
Devem ser precisos e conter instruções corretas e realistas sobre o risco e as práticas. Devem de ser compreendidos e adaptados para o maior número possível de funções de trabalho (tendo em consideração o custo associado). É necessária a existência de formação, a nível geral e ao nível de cada função, para os funcionários. Os incentivos aos empregados devem estar relacionados com a conscientização de segurança da informação.