FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Planeamento e Implementação de um Sistema de Gestão da Segurança da Informação

Bruna Patrícia Ribeiro Alves da Silva

Versão Final

Relatório de Dissertação

Mestrado em Ciência da Informação

Orientador: Engº Tito Carlos Soares Vieira

21 de Julho de 2011

Planeamento e Implementação de um Sistema de Gestão da Segurança da Informação

Bruna Patrícia Ribeiro Alves da Silva

Relatório de Dissertação

Mestrado em Ciência da Informação

Aprovada em provas públicas pelo júri:

Presidente: Doutora Maria Cristina de Carvalho Alves Ribeiro, Professora Auxiliar do Departamento de Engenharia Informática da FEUP;

Vogal Externo: Doutor João Manuel Pereira Barroso, Professor Auxiliar com Agregação no Departamento de Engenharias da UTAD;

Orientador: Engenheiro Tito Carlos Soares Vieira, Especialista de Informática Grau 3 Nível 2.

_____

21 de Julho de 2011

Agradecimentos

Começo por agradecer à minha família, em especial à minha mãe, e amigos pelo apoio constante e incondicional que me prestaram no decorrer desta dissertação, sem os quais este trabalho não teria sido possível.

Gostaria também de deixar o meu sincero agradecimento ao meu orientador, Professor Tito Vieira, pela disponibilidade e acompanhamento, realçando a confiança depositada em todo este processo e as sugestões e críticas que permitiram a melhoria contínua desta dissertação até ao seu estado final.

Queria ainda deixar uma palavra de agradecimento aos colaboradores da MULTICERT pela simpatia, disponibilidade, e pela fácil integração que me proporcionaram na instituição. Em especial, gostaria de agradecer à minha orientadora na empresa, Sara Loja, pelo acompanhamento constante durante o decorrer deste projecto, pela confiança depositada e pela oportunidade que me proporcionou de participar activamente neste projecto.

A todos o meu muito obrigado!

Resumo

A segurança da informação consiste num problema de gestão, e não de tecnologia. Neste sentido, a tecnologia assume o papel de responder "como" será garantida a segurança da informação, enquanto a gestão pretende responder ao que será feito para garantir a segurança da informação.

Esta dissertação apresenta a temática do Planeamento e Implementação de um Sistema de Gestão da Segurança da Informação em ambiente empresarial. Assim, esta foi desenvolvida em duas fases: a primeira debruçada sobre a pesquisa bibliográfica e elaboração do estado da arte sobre a temática do ISMS, onde foram abordados os temas da Segurança da Informação, Planeamento Estratégico de Sistemas de Informação, e por último o Sistema de Gestão da Segurança da Informação.

Ao longo desta dissertação apresenta-se um enfoque teórico das etapas do ISMS implementadas em contexto empresarial, referindo-se os seguintes aspectos: Modelo PDCA, Compromisso da Gestão de Topo, Âmbito de Protecção, Políticas do ISMS, BPM (*Business Process Management*), Gestão da Documentação, Classificação da Informação, Análise do Risco, Declaração de Aplicabilidade, e por último foi referido o Plano e Tratamento do Risco.

Os resultados práticos apresentados são provenientes do planeamento e implementação do ISMS na empresa MULTICERT, tendo sido desenvolvidos os seguintes itens: Modelo PDCA, Compromisso da Gestão de Topo, Âmbito de Protecção, Políticas do ISMS, BPM, Gestão da Documentação, Classificação da Informação, Análise do Risco, Declaração de Aplicabilidade e o Plano de Tratamento do Risco.

Em epílogo, podem ser enfatizadas algumas conclusões extraídas deste trabalho: (1) A segurança da informação não passa apenas pela solução tecnológica, mas sim por uma gestão contínua e eficaz dos riscos associados à informação e aos recursos informacionais; (2) O ISMS permite gerir a segurança da informação através de um método que proporciona uma eficácia garantida pela sua abordagem que possibilita atingir uma melhoria contínua deste sistema.

Palavras-chave: ISMS; Segurança da Informação; Ciência da Informação; Gestão da Informação; ISO/IEC 27001.

Abstract

Information Security is a management problem, not a technology one. In this way, the role of technology is to answer "how" will be guaranteed the information security, while management seeks to answer to what will be done to ensure information security.

This dissertation presents the theme of Planning and Implementation of an *Information Security Management System* in an enterprise environment. Therefore, this dissertation was developed in two phases: the first one related to literature research and development of the state of art on the theme of the ISMS, which addressed the topics of Information Security, Strategic Planning of Information Systems, and finally the Information Security Management System.

Throughout this dissertation is presented a theoretical approach of ISMS steps implemented in organizational context, referring to the following aspects: PDCA Model, Management Commitment, Scope, ISMS Policies, BPM (*Business Process Management*), Documentation Management, Classification of Information, Risk Analysis, Statement of Applicability, and finally the Risk Treatment Plan.

The practical results presented are from the planning and implementation of ISMS in MULTICERT enterprise, having been developed the following items: PDCA Model, Management Commitment, Scope, ISMS Policies, BPM, Documentation Management, Classification of Information, Risk Analysis, Statement of Applicability, and Risk Treatment Plan.

In the epilogue, some conclusions can be emphasized drawn from this study: (1) Information security is not achieved by technological solutions, but by a continuous and effective management of risks associated to information and information resources; (2) The ISMS allows you to manage information security through a method that provides a guaranteed efficacy for its approach that allows to achieve continuous improvement of this system.

Keywords: ISMS; Information Security; Information Science; Information Management; ISO/IEC 27001.

Sumário

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

API – Application Programming Interface

BCM – Business Continuity Management

BCMS – Business Continuity Management System

BCP – Business Continuity Plan

BIA – Business Impact Analyze

BPM – Business Process Management

BS – British Standards

BSI – British Standards Institution

CA – Certification Authority

CI – Ciência da Informação

CISO – Chief Information Security Office

ENISA – European Network and Information Security Agency

EPC – European Payments Council

EU – European Union

FEUP – Faculdade de Engenharia da Universidade do Porto

IEC – International Electrotechnical Commission

IMP – Incident Management Plan

ISO – International Organization for Standardization

ISM – Information Security Management

ISMS – Information Security Management System

ITIL – Information Technology Infrastructure Library

OECD – Organization for Economic Co-operation and Development

PAS 99 – Publicly Available Specification

PTR – Plano de Tratamento do Risco

RPO – Recovery Point Objective

RTO – Recovery Time Objective

RTP – Risk Treatment Plan

SDD Core Scheme – SEPA Core Direct Debit Scheme

SEPA – Single Euro Payments Area

SGSI – Sistema de Gestão da Segurança da Informação

SI – Segurança da Informação

SoA – Statment of Applicability

STORK – Secure Identity Across Borders Linked

TIC – Tecnologias de Informação e Comunicação

TPC – Terceira Parte de Confiança

TSL – Trust Service Status List

1. Introdução

Esta dissertação encontra-se enquadrada no âmbito da unidade curricular anual Projecto, integrada no segundo ano do mestrado em Ciência da Informação. Na possibilidade de escolher entre uma dissertação de cariz mais científico/investigação ou um projecto de cariz mais prático/profissional desenvolvido em ambiente empresarial, optei pela segunda, por me possibilitar o contacto directo com o mundo do trabalho, permitindo-me assim experienciar a actividade profissional. Assim, esta dissertação possibilita interligar o estudo teórico, conceptual e científico com a experiência da prática profissional.

Esta temática foi proposta pela empresa MULTICERT e a minha escolha recaiu sobre esta pelo interesse que o tema me despertou, essencialmente pelos conteúdos apreendidos na unidade curricular de Segurança da Informação, leccionada no primeiro semestre do primeiro ano de mestrado.

A MULTICERT, Serviços de Certificação Electrónica, S.A. iniciou a sua actividade em 2002, posicionando-se no mercado como fornecedor de soluções completas de segurança e/ou certificação digital para todo o tipo de transacções electrónicas que exigem segurança (*e-commerce*, *e-banking*, *e-government*, e-mail, etc). Actualmente, a MULTICERT desenvolve a sua actividade nas seguintes áreas de negócio: documentos de identificação seguros, certificados digitais, factura electrónica, gestão documental, transacções seguras, API`s (*Application Programming Interface*), e recentemente as TSL`s (*Trust Service Status List*). Uma descrição mais pormenorizada será apresentada no capítulo 4 desta dissertação.

Relativamente a este projecto/dissertação – Planeamento e Implementação de um ISMS (*Information Security Management System*) – este resulta da estratégia da MULTICERT de acrescentar às áreas de negócio que já integra, uma nova área relacionada com a gestão e operação de TSL`s. Assim sendo, este projecto terá como âmbito o planeamento e implementação de um ISMS aplicado às TSL`s, que inicialmente serão geridas e operadas pela MULTICERT para o seu cliente EPC (*European Payments Council*).

Este ISMS, cuja implementação resulta de um projecto estratégico da empresa, pretende conter no seu âmbito de protecção as TSL`s, prevendo-se num futuro próximo

expandir o âmbito de protecção à actividade de emissão de certificados digitais da MULTICERT.

A questão de investigação proposta – Qual o contributo da certificação de um Sistema de Gestão da Segurança da Informação para a credibilidade de uma organização? – enquadra-se no âmbito da Segurança da Informação, relacionando-se com a certificação de sistemas de gestão da segurança da informação. Neste sentido, será planeado e implementado um sistema baseado num conjunto de políticas, processos, procedimentos, etc, que permitem à organização gerir eficazmente a segurança da sua informação, controlando e minimizando o risco associado à informação e aos recursos informacionais, e planeando a continuidade do seu negócio em caso de incidentes ou desastres.

Esta dissertação encontra-se estruturada em 6 capítulos. Neste primeiro capítulo é feita a Introdução, onde são enunciadas as motivações que estiveram na origem da escolha do tema, seguindo-se uma breve apresentação da empresa acolhedora, e terminando com a apresentação da estrutura da dissertação.

No segundo capítulo – Enquadramento Teórico e Conceptual – são explanadas questões do foro metodológico, situando desde logo esta dissertação na Ciência da Informação, em específico na área da Segurança da Informação, sendo que das três grandes áreas da Ciência da Informação, esta dissertação toca na Gestão da Informação e no Comportamento Informacional. De seguida é adoptado e explicado o método utilizado para conduzir esta dissertação – o método quadripolar, e são feitos esclarecimentos teóricos e metodológicos que caracterizam esta problemática. Assim sendo, este capítulo contém dois subcapítulos: a Ciência da Informação e a Gestão da Informação; e o Contributo da Ciência da Informação para o ISMS.

O terceiro capítulo – Estado da Arte – reflecte uma revisão da investigação até aqui desenvolvida sobre a Segurança da Informação, tendo obviamente em consideração o âmbito e contexto desta dissertação. Assim, é feita uma introdução para contextualizar os leitores, seguindo-se uma abordagem sobre a Segurança da Informação, desenvolvendo os seus conceitos centrais, as áreas da SI (Segurança da Informação), os seus pilares, os conceitos de vulnerabilidade, ataque, risco e defesa, e por fim abordando a questão das políticas e mecanismos de segurança. De seguida é abordado o Planeamento Estratégico de Sistemas de Informação, onde é focado o ciclo do

desenvolvimento estratégico. Por último, este capítulo termina abordando o Sistema de Gestão da Segurança da Informação e as normas relacionadas com o mesmo.

Relativamente ao quarto capítulo – O Caso de Estudo – este apresenta o planeamento e implementação do ISMS na MULTICERT, sendo feito o contexto organizacional, onde é apresentada a MULTICERT e o projecto estratégico em que está envolvida e que fará parte do âmbito de protecção do ISMS – a TSL – inicialmente emitida para o EPC (*European Payments Council*); será feita a descrição e objectivos desta dissertação; apresentadas as actividades e o cronograma; o método e normas utilizadas (onde se aborda a recolha de informação, as normas ISO/IEC 27001, 27003, 27005 e BS 25999, e os requisitos de segurança da informação da MULTICERT); e por último, é desenvolvido o Sistema de Gestão da Segurança da Informação, onde é explanado em termos teóricos o modelo PDCA (*PLAN-DO-CHECK-ACT*), o compromisso da gestão de topo, o âmbito de protecção (e os seus processos, actividades e recursos), as políticas do ISMS, o BPM (*Business Process Management*), a gestão da documentação (e a classificação da informação), a análise e avaliação do risco, a declaração de aplicabilidade e por último o plano de tratamento do risco.

No capítulo 5 serão então desenvolvidos os aspectos práticos do planeamento e implementação do ISMS na MULTICERT, sendo abordado o modelo PDCA, o compromisso da gestão de topo, âmbito de protecção, políticas do ISMS, o BPM, a gestão da documentação, classificação da informação, análise e avaliação do risco, declaração de aplicabilidade, e por último o plano de tratamento do risco.

O capítulo 6 apresenta as conclusões resultantes desta dissertação e as perspectivas futuras.

2. Enquadramento Teórico e Conceptual

Cabe neste capítulo fazer o enquadramento teórico e conceptual da ciência que engloba a segurança da informação. Serão então abordados alguns aspectos cruciais da Ciência da Informação para este âmbito.

A Ciência da Informação e o seu objecto científico – a informação – ganham maior relevância em meados dos anos 60, impulsionadas pelos avanços tecnológicos, que tornam mais visível a importância da informação e não do documento, como até então se entendia. A primeira definição apresentada para esta ciência emergente, e que até hoje reúne um grande consenso por parte da comunidade científica, foi a definição apresentada nas conferências do Georgia Institute of Technology (1962), e mais tarde aperfeiçoada por Harold Borko, em 1968, em que definem a Ciência da Informação como sendo "*a disciplina que investiga as propriedades e o comportamento da informação, as forças que regem o fluxo informacional e os meios de processamento da informação para optimização do acesso e uso. Está relacionada com um corpo de conhecimento que abrange a origem, colecta, organização, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação. (…) Trata-se de uma ciência interdisciplinar derivada e relacionada com vários campos como a matemática, a lógica, a linguística, a psicologia, a tecnologia computacional, as operações de pesquisa, as artes gráficas, as comunicações, a biblioteconomia, a gestão e outros campos similares. Tem tanto uma componente de ciência pura, que indaga o assunto sem ter em conta a sua aplicação, como uma componente de ciência aplicada, que desenvolve serviços e produtos*" (SILVA, 2006).

A CI (Ciência da Informação) é assim a ciência que tem como objecto científico a informação, que consiste num "*conjunto estruturado de representações mentais codificadas (símbolos significantes) socialmente contextualizadas e passíveis de serem registadas num qualquer suporte material (papel, filme, banda magnética, disco compacto, etc.) e, portanto, comunicadas de forma assíncrona e multidireccionada*" (SILVA ; RIBEIRO, 2002). Esta ciência ocupa-se e preocupa-se essencialmente com a informação: quer enquanto processo que inclui o comportamento informacional e um conjunto subjacente de etapas: criação, uso, difusão, organização, armazenamento, colecção, pesquisa e interpretação; quer enquanto fenómeno info-comunicacional que emerge da "coisa" (código e suporte); que possui propriedades essenciais (SILVA ; RIBEIRO, 2002): estruturação pela acção (humana e social), pois é através do acto

(individual ou colectivo) que a informação é criada/modelada; integração dinâmica, as condições/circunstâncias internas e externas condicionam o sujeito que pratica o acto informacional; pregnância (temática), potenciadora da pertinência; quantificação, independentemente da codificação da informação, toda ela é passível de ser mensurada quantitativamente; reprodutividade, toda a informação pode ser reproduzida ilimitadamente; e por último, transmissibilidade, a informação produzida ou replicada pode ser potencialmente transmitida/comunicada.

A informação é cada vez mais encarada pelas organizações como um recurso/activo de extremo valor, pois esta representa não só a memória organizacional, como também desempenha um papel estratégico crucial. Cada vez mais a tecnologia deixa de ser um diferencial, pois com a sua difusão, e por conseguinte o seu menor custo de aquisição e manutenção, esta deixa de ser encarada pelas organizações como um factor de competitividade e como uma mais-valia, o que permite às organizações terem uma percepção mais clara da real importância da informação. Este fenómeno acontece de forma semelhante ao sucedido em tempos mais remotos, onde era dada maior importância ao documento em detrimento da informação, pois esta acabava por estar "camuflada" pelo seu suporte. Assim, uma vez mais a informação ganha maior relevância do que o suporte onde esta é registada, quer seja analógico ou digital.

Apresentado o objecto científico da CI, e antes de passarmos à explanação do seu método, importa ainda referir as principais áreas da CI que compõem o seu campo de estudo: a Gestão da Informação, o Comportamento Informacional, e por último a Organização e Representação da Informação. Esta dissertação aborda essencialmente duas destas áreas: a Gestão da Informação e o Comportamento Informacional. A gestão da informação está presente em todo este processo, pois a finalidade pretendida consiste na implementação de um sistema, baseado num conjunto de medidas, processos, fluxos de informação, procedimentos, políticas, etc, que permitem à organização gerir a segurança da sua informação de forma eficaz e eficiente, possibilitando assim um maior controlo sobre a mesma. Ressalve-se que a gestão da segurança da informação é planeada/implementada em estrita colaboração com a gestão da informação, devido ao seu relacionamento. Por outro lado, a implementação de um ISMS implica que existam mudanças na cultura organizacional e no comportamento informacional dos utilizadores, a gestão da segurança da informação só funciona eficazmente se todos os *stakeholders* que com ela lidam, a compreendam e a coloquem em prática. A SI está, em

muito, relacionada com o comportamento dos utilizadores, a forma como usam a informação, o que fazem com ela, etc. Aliás, deles depende não só a segurança da informação, mas também a sua insegurança, como poderemos constatar mais à frente.

Feita esta achega, importa agora abordar o método que será adoptado para conduzir esta investigação científica. Qualquer campo de saber, para que possa ser ciência, necessita entre outras coisas, ter um corpo teórico, conceptual, metodológico consistente, necessita do estabelecimento de fronteiras, definição de um objecto de estudo, e ainda da adopção de um método científico ajustado às suas especificidades/necessidades. Sendo a CI uma ciência social necessita, à semelhança de outras ciências sociais e humanas, de um método adequado às suas especificidades, isto é, um método adequado às características da informação, que enfatize o aspecto qualitativo sem descurar, por outro lado, o aspecto quantitativo.

Desta forma, importa aqui referir que o dispositivo metodológico utilizado para conduzir esta investigação científica é o Método Quadripolar, por ser um método que promove o debate entre o quantitativo e o qualitativo, por promover o intercâmbio interdisciplinar, e por permitir um dinamismo, interacção e abertura permanente entre os seus pólos (RIBEIRO, 2006):

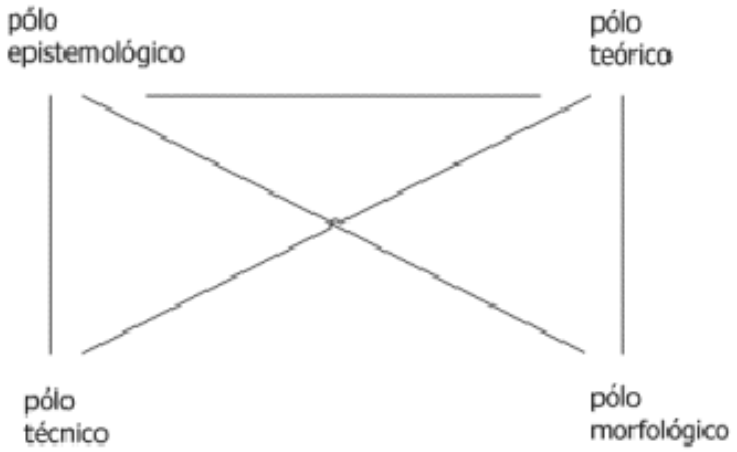

Figura 1 – Método Quadripolar

Dito isto, passemos a uma breve explicitação sobre os pólos que constituem o método quadripolar antes de passarmos ao caso prático.

Comecemos pelo pólo epistemológico, apelidado também como o pólo da vigilância crítica da pesquisa, ocupa-se por um lado "*do exame do processo de produção dos objectos científicos – lógica da descoberta – por outro lado cuida da*

análise dos procedimentos lógicos de validação e da proposição de critérios de demarcação para as práticas científicas – lógica da prova" (MARTINS ; THEÓPHILO, 2007). Este pólo funciona assim como ponto de partida, sendo aqui que é construído o objecto científico e é delimitada a problemática da investigação. A epistemologia geral – resultante da troca interdisciplinar das reflexões de diversas disciplinas – rege-se por alguns princípios, considerando algumas concepções fundamentais para o processo de geração de conhecimento científico: causalidade e significância dos achados.

Neste projecto, a primeira etapa consistiu na delimitação do campo de acção através da elaboração da proposta de projecto e sua adequação ao campo de estudo em que nos situamos. Relativamente ao objecto de investigação, como foi referido acima, trata-se da informação. Por fim, ainda neste pólo deve ser assumido o paradigma (modo de ver) sobre o qual abordaremos a problemática. Com o intuito de contextualizar, refira-se o paradigma custodial, historicista, patrimonialista e tecnicista, que devido à sua ruptura fez emergir um novo paradigma, designado pós-custodial, dinâmico, científico e informacional. Ressalve-se no entanto, que a emergência de um novo paradigma não significa, de todo, uma ruptura total com o paradigma anterior. Muito pelo contrário, ambos podem perfeitamente coexistir. Dito isto, o paradigma custodial é marcado por traços fortes de um empirismo patrimonialista/tecnicista. Este paradigma é muito marcado pelo primado do documento, da técnica, onde prevalece o "saber fazer" e a "lógica custodial" (conservar/guardar em serviços próprios manuscritos, impressos, gravuras, etc) (SILVA, 2000).

No entanto, dada a conjuntura actual, muito impulsionada pela gestão e pela informática, emerge um novo paradigma denominado pós-custodial, dinâmico, científico e informacional. Este é o paradigma aqui claramente assumido, um paradigma vincado pela abordagem científica e atitude pós-custodial (armazenamento virtual, difusão multinível e multimédia, etc).

No pólo teórico são formulados os conceitos operatórios, hipóteses e teorias (plano da descoberta) e subsequente verificação ou refutação do "contexto teórico" formulado (plano de prova) (SILVA, 2000). A teoria tem como objectivo a "*reconstrução conceitual das estruturas objectivas dos fenómenos, a fim de compreendê-los e explicá-los. Dentro do contexto da pesquisa, as teorias orientam a busca dos factos, estabelecem critérios para a observação, seleccionando o que deve*

ser observado como pertinente para testar hipóteses e buscar respostas às questões de uma dada pesquisa" (MARTINS ; THEÓPHILO, 2007).

Relativamente a este pólo, esta dissertação enquadra-se mais especificamente na área da Segurança da Informação, sendo que relativamente às principais áreas da CI, este projecto "toca" nas áreas da Gestão da Informação e Comportamento Informacional. Relativamente aos conceitos, importa aqui referir o trinómio que compõe os pilares centrais da SI – confidencialidade, integridade e disponibilidade. Poderão ainda ser referidos dois outros conceitos que no contexto deste projecto desempenham um papel relevante – a autenticidade e o não-repúdio.

Ainda neste pólo, importa ainda referir um outro elemento pertencente ao pólo teórico – o modelo – que "*consiste na especificação de uma teoria científica que consente a descrição de uma zona restrita e específica do campo coberto pela própria teoria*" (MARTINS ; THEÓPHILO, 2007).

Neste projecto será adoptado o modelo PDCA (*Plan-Do-Check-Act*), que consiste num ciclo composto por um conjunto de acções sequenciais, que visam atingir essencialmente duas metas: manter o sistema, e melhorar o sistema:

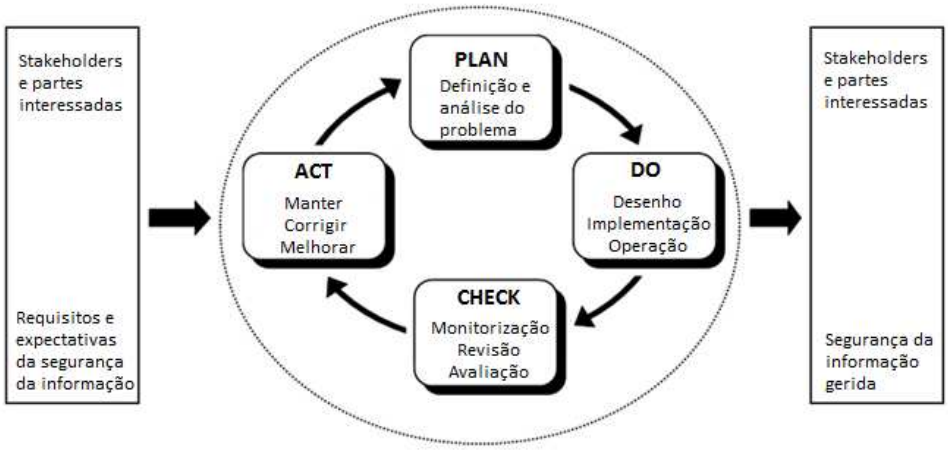

Figura 2 – Modelo PDCA

Através deste modelo, a ISO/IEC 27001 fornece uma framework de um sistema de gestão da segurança da informação para implementação dos princípios dispostos pela OECD (*Organization for Economic Co-operation and Development`s*) (VAN BON ; VERHEIJEN, 2006): sensibilização, responsabilidade, resposta, avaliação do risco, desenho e implementação da segurança, gestão da segurança e reavaliação.

Por sua vez, é no pólo técnico que se estabelece a relação entre a construção do objecto científico e a realidade objectivada. É através deste contacto, por via instrumental, do investigador com a realidade que se verifica ou refuta o contexto teórico, jogando-se assim a capacidade probatória do dispositivo metodológico.

No contexto desta dissertação foram utilizadas concomitantemente diversas técnicas/estratégias de pesquisa. Foi utilizada a pesquisa bibliográfica, para elaboração/explanação do capítulo neste contexto desenvolvido e que corresponde ao pólo teórico; pesquisa documental, observação participante e estudo de caso para a aplicação da teoria ao caso prático, isto é, para a implementação do ISMS na MULTICERT.

Por último, no pólo morfológico reflecte-se a eficácia das operações até aqui realizadas, assumindo-se a análise/avaliação dos dados recolhidos, partindo para a configuração do objecto científico e expondo o processo que permitiu a sua construção. Neste pólo trata-se a organização e apresentação dos dados, devidamente criticados no pólo teórico, operacionalizados no pólo técnico, e harmonizados pelo pólo epistemológico, o que demonstra o pendor interactivo deste método.

2.1.A Ciência da Informação e a Gestão da Informação

Como foi referido anteriormente, a Gestão da Informação constitui uma das grandes áreas da Ciência da Informação, que "*significa lidar, administrar, encontrar soluções práticas desde a génese até ao efeito multiplicador do fluxo da informação e compreende um conjunto diversificado de actividades, a saber: produção, tratamento, registo e guarda, comunicação e uso da informação. E cada uma delas encerra problemáticas específicas que são ou podem e até devem ser estudadas cientificamente pelos actuais profissionais da informação encarregues, na prática quotidiana, de agilizar o fluxo e a intensificação do uso da informação*" (SILVA, 2005). Ressalve-se, no entanto, a estrita relação que esta área tem com as restantes grandes áreas da CI – o comportamento informacional, e a organização e representação da informação.

Quando se refere a Gestão da Informação, em pleno contexto da Sociedade da Informação, importa desde logo mencionar algumas questões fulcrais: a gestão da plataforma tecnológica de informação e comunicação, a gestão dos recursos de

informação e a gestão do ciclo de vida da informação e actividades subjacentes, sendo no entanto essencial referir a interligação entre a organização e a sua própria dinâmica evolutiva, pois a "*organização aprende se, através do seu processamento de informação, o âmbito dos seus potenciais procedimentos for alterado. Assim, o objectivo principal da Gestão da Informação é aproveitar recursos de informação e capacidades de informação de modo a que a organização aprenda e se adapte ao seu meio ambiente em mudança*" (CHOO, 2003).

Existe uma proliferação de definições atribuídas à gestão da informação, consequência até da própria perspectiva do autor que a define, que faz o recorte da realidade segundo a sua ciência e ponto de vista. Porém, existem alguns significados mais comummente utilizados que, segundo Choo, se concentram em: gestão de recursos informacionais, gestão de políticas informacionais, gestão de tecnologia da informação, e gestão de processos informacionais.

Existem inúmeros modelos propostos no contexto da gestão da informação, modelos esses criados não só com o intuito de representar este fenómeno que é a gestão da informação, mas também com a finalidade de procurar estabelecer um padrão de comportamento que pode ser replicado mediante o cumprimento de determinadas premissas.

Davenport, em 1998 propõem um modelo para a gestão da informação que contempla quatro etapas: a primeira diz respeito à determinação das exigências, em que se identificam as informações em função do factor humano; na segunda etapa prevê-se a obtenção da informação, é definida a fonte e a informação obtida é classificada, esta fase está portanto muito dependente da intervenção humana; a terceira etapa diz respeito à fase de distribuição/disseminação da informação, onde devem ser analisadas alternativas entre levar a informação ao utilizador ou divulgar a existência dessa informação, permitindo por conseguinte o acesso a quem se interessar e a quem estiver devidamente autorizado para tal; por último, a quarta etapa consiste no uso da informação, em que se valida o modelo ao se controlar a efectividade das informações obtidas.

Por outro lado, Choo descreve-nos um modelo onde são identificadas sete etapas: necessidade da informação; aquisição da informação; produtos e serviços de informação; distribuição da informação; organização e armazenamento da informação; utilização da informação; e por último, comportamento adaptativo (CHOO, 1998):

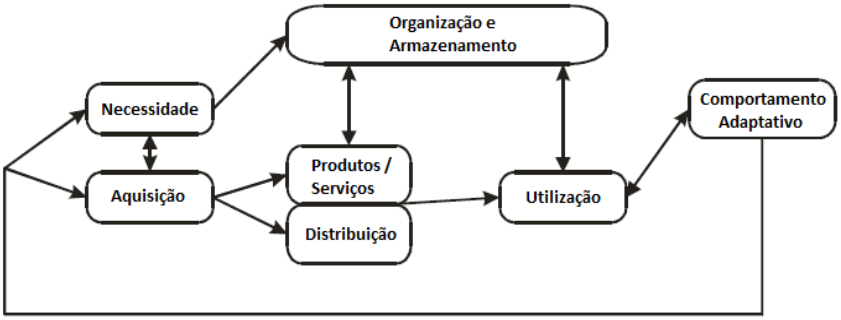

Figura 3 – Ciclo de Gestão da Informação

Como já foi referido, existe uma proliferação de modelos de gestão da informação, não cabendo no entanto neste contexto adoptar um deles, mas sim oferecer uma contextualização.

2.2. Contributo da Ciência da Informação para o ISMS

Como já foi referido anteriormente, o objecto de estudo da CI é a informação, possuindo assim esta área profissionais (profissional da informação) que possuem competências e habilitações específicas para poderem contribuir nos processos relacionados com o uso da informação e do conhecimento. Este profissional está devidamente habilitado com competências que lhe permitem recolher, processar e disseminar informação, atendendo prontamente às necessidades da informação crítica/vital, possibilitando assim que a informação desempenhe um papel crucial, tornando-se numa vantagem competitiva para qualquer organização.

Afunilando a perspectiva, por sua vez a Gestão da Informação é considerada a base para se administrar/gerir os activos/recursos da informação, uma vez que o seu objectivo é obter, tratar e organizar a informação com a finalidade de fomentar a sua posterior recuperação e disseminação, tudo isto realizado com economia de tempo e de recursos financeiros.

Um Sistema de Gestão da Segurança da Informação pressupõe essencialmente a protecção/garantia dos pilares da Segurança da Informação (confidencialidade,

integridade e disponibilidade), mas também a protecção dos activos/recursos da informação. Nesse sentido, poderá embeber algumas das principais ferramentas/boas práticas da Gestão da Informação, que lhe permitem elucidar e contribuir, quer para o tratamento e organização da informação, quer para a salvaguardar dos activos/recursos informacionais de determinada organização, e por conseguinte auxiliar a constituição do ISMS.

A identificação das necessidades de informação e a sua incorporação no Sistema de Gestão da Informação permite delinear determinadas acções de tramitação quando lidamos com a informação. Uma vez identificada e feita a sua classificação, a informação tanto pode ser incluída num fluxo de trabalho que culmina no seu posterior arquivamento, como pode ser imediatamente eliminada, dependendo dos resultados da análise/reconhecimento da sua pertinência. Neste sentido, já existe uma interligação evidente entre a Gestão da Informação e a Segurança da Informação, pois para se obter a segunda torna-se necessário proceder, tanto à classificação dos activos/recursos da informação, como à informação propriamente dita, sendo que esta actividade vai determinar o fluxo informacional.

Desta forma, pressupõem-se que na gestão da informação corporativa se torne imprescindível a gestão dos fluxos de produção e uso da informação. É portanto crucial estabelecer uma Política de Gestão da Informação, onde devem ser integrados os pilares da Segurança da Informação: confidencialidade, integridade e disponibilidade. Neste sentido, a Gestão da Informação poderá dar um contributo importante no processo de concepção do Sistema de Gestão da Segurança da Informação, fornecendo assim aos activos/recursos da informação uma gestão mais eficaz dos mesmos.

Com o intuito de melhor compreendermos a natureza da gestão da informação no contexto das organizações, importa aqui referir que a informação produzida no âmbito de uma organização reflecte não só o seu funcionamento, como também a sua natureza, as suas actividades, a sua estrutura, funcionalidade, propósito e a sua memória organizacional.

Relativamente ao Sistema de Gestão da Segurança da Informação, este tem como uma das suas principais etapas a classificação dos activos/recursos da informação. Para além do código de classificação, descritores, número de protocolo e número de registo, a captura de informação pode prever a adição de outros elementos de meta-

informação, nomeadamente: a data e hora de criação, de transmissão e de recepção da informação; nome do autor, criador e do destinatário, entre outros. Essa meta-informação pode ser registada em vários níveis de detalhe, dependendo das necessidades originadas pelos procedimentos da organização e pelas suas obrigações jurídicas e administrativas. A meta-informação constitui um elemento fundamental para a identificação da informação, de modo inequívoco, podendo até mesmo ser utilizada como uma forma de garantir a integridade da informação.

Voltando um pouco à questão da classificação da informação, importa ainda referir que é através desta que é iniciado o processo de Gestão da Segurança da Informação. Embora a primeira etapa crucial para o arranque do planeamento do Sistema de Gestão da Segurança da Informação seja a definição do âmbito de protecção sobre o qual será implementado o sistema, o facto é que, no que toca à Gestão da Segurança da Informação, esta inicia-se na etapa de classificação dos activos/recursos da informação. Dito isto, a fase da classificação permite tornar evidente quais os activos de informação e também quais as suas necessidades de protecção, resultando desta actividade a classificação da informação relativamente ao grau de sigilo (confidencialidade) que a mesma terá. Neste aspecto, mais uma vez, a gestão da segurança da informação poderá embeber metodologias, métodos e/ou técnicas que a gestão da informação utiliza para o mesmo fim – o de classificar devidamente a informação.

Uma outra actividade importante para a Gestão da Informação está relacionada com a avaliação, constituindo esta um processo de análise da informação, com o intuito de estabelecer directrizes para o destino/finalidade da mesma. Esta operação consiste na categorização da natureza da informação, estabelecendo assim a natureza do conteúdo, a sua função e contexto, e por conseguinte, classificar a mesma consoante a sua função e uso organizacional. Para realizar esta actividade, podem ser utilizados planos de avaliação da informação, que permitam, por exemplo, categorizar a mesma com base no seu ciclo de vida.

Porém, não é só a segurança da informação que pode e deve embeber metodologias/métodos/técnicas na gestão da informação. O inverso também se torna muito vantajoso para a organização, devendo as duas disciplinas manterem uma inter-relação permanente. Boa parte dos controlos dispostos na norma ISO/IEC 27001 são aplicados no âmbito da segurança lógica, o que abrange por exemplo o controlo de

acessos. Neste sentido, torna-se oportuno destacar a importância de também a Gestão da Informação se integrar com a Segurança da Informação e com as suas normas, criando uniformidade. Esta integração pode e deve ser feita a vários níveis, nomeadamente no que concerne às restrições e níveis de acesso, às ferramentas utilizadas para o tratamento e organização da informação, etc. Esta integração/uniformidade acarreta inúmeras vantagens para a organização que a pratica, ajudando por um lado no planeamento e implementação do Sistema de Gestão da Segurança da Informação, e por outro lado permitindo uma Gestão da Informação mais eficaz, que acima de tudo assegura a informação, mas também os seus activos/recursos.

3. Estado da Arte

O objectivo central desta dissertação é explorar a temática dos sistemas de gestão da segurança da informação. Para tal, é necessário enquadrar este tema e analisar a produção científica já existente sobre o mesmo. Para a realização desta revisão da literatura foram feitas pesquisas em determinados recursos de informação que garantem rigor científico. Essencialmente as pesquisas centraram-se em bases de dados disponibilizadas pela FEUP, designadamente: Scopus, CiteSeerX, Web of Science, Compendex, Inspec, Proquest, etc.

Assim sendo, este levantamento do estado da arte começará por abordar a segurança da informação, seguindo-se uma breve contextualização sobre o planeamento estratégico de sistemas de informação e terminará com a abordagem dos sistemas de gestão da segurança da informação.

3.1. Segurança da Informação

A preocupação com a segurança da informação não é uma questão recente. Na verdade esta preocupação existiu desde os tempos mais longínquos: o arquitecto Khnumhote, que construiu o monumento do faraó Amenemhet II, documentou a sua localização num documento escrito numa tablete de argila, codificando determinados trechos dessa documentação através da substituição de palavras para que, caso esse documento fosse roubado, o ladrão não descobrisse o caminho que o levaria ao tesouro(SILVA, 2009); Júlio César também já utilizava algoritmos de cifragem por substituição nos seus documentos, para que estes não pudessem ser interpretados por pessoas não autorizadas para o efeito.

Durante a segunda guerra mundial, os exércitos necessitavam de comunicar informação pelo rádio de forma mais compacta e segura. Para tal, foram desenvolvidos algoritmos que permitiam atingir estes dois objectivos: o de comunicar a mesma informação mas numa menor quantidade de caracteres; e o de comunicar a informação num determinado código criptográfico que permitisse garantir a confidencialidade da informação transmitida.

No entanto, o grande impulso da segurança da informação aconteceu despoletado essencialmente pela proliferação dos computadores ligados em rede e pelo

uso, cada vez maior, da internet. A utilização global da internet e das redes de computadores em geral trouxeram uma nova forma de comunicar informação, porém também abriram portas para novas ameaças à SI (Segurança da Informação), o que implicava a necessidade de desenvolver e implementar uma gestão apropriada e políticas de segurança que permitissem manter a autenticidade, confidencialidade e integridade da informação transmitida. Esta nova realidade implicava que os modelos de SI até então existentes ficassem obsoletos e necessitassem de ser reformulados, para poderem responder eficazmente às novas problemáticas. O novo modelo de SI tem como objectivo proteger os sistemas de informação das organizações e garantir o seu ambiente operacional. Parte deste novo desafio é a crescente importância atribuída à componente de ISM (*Information Security Management*), a gestão do risco, que de resto é uma das temáticas mais exploradas pela comunidade científica que investiga SI.

Inicialmente, as organizações pensavam os seus objectivos de segurança com base no seu histórico de incidentes, juntamente com base nas competências e experiência dos seus *stakeholders* internos, utilizando como meio para atingir os seus objectivos um conjunto de práticas de segurança desenvolvidas internamente(NNOLIM, 2007). No entanto, a crescente utilização das tecnologias nas organizações acarretava também um aumento dos riscos para a informação, e como consequência as questões da SI ganhavam uma outra complexidade (quanto maior a organização, maior a complexidade) relativamente à sua gestão. Estavam assim criadas as condições para que se repensasse a segurança da informação nas organizações, que mais que uma componente a pensar nas TIC, deveria ser uma componente transversal, pensada e integrada em cada etapa do ciclo de vida de desenvolvimento dos sistemas de informação. Deve portanto, ser pensada do ponto de vista da gestão organizacional(MA, 2004).

A SI passaria assim a ser encarada como algo a ter em consideração de forma transversal em todos os sistemas de informação da organização, deveria ser assumida pelos gestores de topo e comunicada a todos os seus *stakeholders*, tendo sempre em consideração duas questões centrais: a gestão da informação e o comportamento informacional.

Nesta altura, as organizações já tinham consciência da importância que a SI tinha nos seus negócios, inclusive a nível monetário. Agora, o que necessitavam era saber como implementar uma ISM eficaz, ou seja, era necessário um conjunto de

normativas que permitissem implementar as políticas e mecanismos da SI. Pode-se aqui salientar desde logo o papel da ITIL (*Information Technology Infrastructure Library*), que disponibiliza publicações direccionadas para a gestão de organizações de TIC, apresentando um conjunto abrangente de processos (incluindo o processo de gestão da segurança da informação) e procedimentos de gestão, organizados por assuntos, com os quais uma organização pode planear a sua gestão táctica e operacional com vista ao alcance do alinhamento estratégico com os negócios.

Em 2005 foi criada a ENISA (*European Network and Information Security Agency*) para dar resposta às questões de SI na União Europeia. Tem como objectivo a disseminação de informação relativa a boas práticas e conhecimentos sobre SI. Presta serviços de assessoria em SI aos estados membro da EU, recolhe e analisa informação sobre incidentes e riscos emergentes na SI, promove métodos para a gestão e avaliação do risco para que as organizações estejam capazes de lidar com as ameaças de SI, e promove acções de sensibilização e cooperação entre os diferentes actores da SI, incluindo o desenvolvimento de parcerias entre o sector público e o privado.

Tanto a ITIL como a ENISA visam a comunicação de um conjunto de boas práticas em SI, e não um conjunto de normas que permitam a certificação das organizações. Este papel de normalizar é ocupado essencialmente por duas instituições com reconhecimento internacional: a ISO/IEC e a BS, que disponibilizam um conjunto de normas que permitem às organizações: planear e implementar um conjunto de processos e procedimentos que visam garantir a gestão eficaz e eficiente da SI nas organizações; cumpridos os requisitos, as organizações podem pedir uma certificação reconhecida internacionalmente, e que lhes traz um conjunto de benefícios que serão explorados mais à frente.

3.1.1. Conceitos Centrais

A informação tornou-se num factor crítico para a estratégia e sucesso das organizações, esta consciencialização deu-se principalmente após a intensificação do uso da internet e da utilização do comércio electrónico. Como tal, este bem/recurso das organizações necessita ser devidamente protegido. Este é o papel da segurança da informação.

Wilson Oliveira define SI como o "*processo de protecção de informações e activos digitais armazenados em computadores e redes de processamento de dados*", complementa ainda dizendo que a SI tem como finalidade "*garantir disponibilidade, sigilo, integridade, autenticidade, controlo de acesso e não-repúdio das informações* (…) *com a segurança da informação temos a garantia de que a informação estará disponível para o acesso, no momento desejado*".(OLIVEIRA, 2001).

Destas definições podemos desde já tirar algumas ilações: em primeiro lugar, Wilson Oliveira restringe a SI como uma área que actua essencialmente sobre a informação em suporte digital, no entanto, e apesar da esmagadora maioria da informação ser produzida e comunicada por via digital, uma grande parte dessa mesma informação acaba por ser impressa, o que implica que a SI se preocupe essencialmente com a informação, independentemente do seu suporte (analógico ou digital), por exemplo, na área de segurança física deve se ter em consideração a segurança da informação que está impressa e armazenada nos arquivos da organização; em segundo lugar, Oliveira fala-nos de 4 grandes pilares da SI: confidencialidade, integridade, autenticidade e disponibilidade, apesar de misturar outros conceitos que estão relacionados com estes pilares, mas que não estão ao mesmo nível, por exemplo, o controlo de acessos é uma medida/propriedade que permite garantir a autenticidade. No entanto, ressalve-se o enquadramento que Oliveira atribui a SI, afirmando que esta área não se trata de uma questão técnica, mas sim "*uma questão estratégica e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem formar e consciencializar o nível administrativo da empresa e todos os seus funcionários*".

Nesta dissertação será assumida a definição dada pela ISO/IEC 27001, que define SI como uma área que pretende garantir a "*preservação da confidencialidade, integridade e disponibilidade da informação. Em adição, outras propriedades como a autenticidade, responsabilidade, não-repúdio e confiabilidade podem também estar involvidos*"(ISO/IEC 27001, 2005).

No entanto, a SI não envolve apenas um conjunto de medidas de cariz tecnológico para garantir o cumprimento dos pilares acima referidos. A SI, como referido anteriormente, deve ser transversal à organização, pois a SI é muito mais abrangente do que apenas a implementação de controlos tecnológicos. A SI deve ser perspectivada também como uma componente de gestão a ser pensada em todo o ciclo de vida dos sistemas de informação, e deve ainda compreender e lidar com os

comportamentos das pessoas que utilizam as tecnologias implementadas, visto que um dos principais factores de insegurança da informação, segundo as estatísticas(DOLYA, 2007) está relacionado com os comportamentos das próprias pessoas internas à organização.

3.1.1.1. Áreas da Segurança da Informação

Relativamente às áreas de SI, diferentes autores fazem diferentes divisões. Existem autores que defendem uma divisão em segurança física e segurança lógica. Estes mesmos autores afirmam que, apesar de nos dias de hoje a segurança se centrar muito na parte lógica, é necessário cuidar também a parte física, pois só existe uma protecção da informação eficaz se estas duas áreas estiverem asseguradas.

Segundo Oliveira(OLIVEIRA, 2001), a segurança física implica um conjunto de "*medidas usadas para garantir a protecção física dos recursos contra ameaças voluntárias e involuntárias*", assim deve-se ter em atenção as "*ameaças sempre presentes, mas nem sempre lembradas: incêndios, desabamentos, relâmpagos, inundações, problemas na rede eléctrica, acesso indevido de pessoas ao Datacenter, formação inadequada de funcionários, etc*". Apesar de o autor referir que a segurança lógica só é eficaz se a segurança física também for garantida, a verdade é que a segurança lógica exige maior estudo e maior investimento em, por exemplo, software de segurança.

Relativamente à segurança lógica, Oliveira define-a como sendo um "*sistema de informação baseado em mecanismos que permitem aos gestores de sistemas controlar o acesso e o uso dos recursos de informação informatizados*". Assim, esta área preocupa-se essencialmente com os problemas causados por "*vírus, acesso de bisbilhoteiros (invasores de rede), programas de backup desactualizados ou feitos de maneira inadequada, distribuição de códigos secretos de acesso, etc*". O autor refere ainda a utilização da criptografia como uma medida que permite garantir a segurança da informação de possíveis acessos indevidos pelos "*bisbilhoteiros*", no que à segurança lógica concerne.

Por sua vez, Pedro Silva (SILVA, e tal., 2003) divide a segurança da informação em: segurança física, segurança do pessoal e segurança lógica. Nesta abordagem já se

denota claramente uma preocupação acentuada na componente dos *stakeholders* da organização. Aqui já é demonstrada uma preocupação com a componente humana, pois como iremos ver mais à frente, esta é uma componente crucial para o sucesso da segurança da informação na organização. À semelhança de Oliveira, também Pedro Silva considera que a segurança física diz respeito às instalações da organização e a todo o hardware onde a informação é produzida, disseminada ou armazenada. Entrando num maior nível de detalhe, o autor apresenta algumas questões a ter em consideração para garantir a segurança física (SILVA, et al., 2003):

- **Áreas –** embora a escolha da área esteja limitada (principalmente nos meios urbanos), a localização da organização constitui uma componente importante para a construção de um ambiente seguro. Para além desta questão, a própria divisão das instalações deve ser pensada do ponto de vista da SI em moldes "*concêntricos e de profundidade*", para que sejam incrementados os níveis de protecção contra acessos não autorizados. Assim sendo, os bens mais preciosos devem encontrar-se mais perto do centro das instalações, para obrigar à passagem por diversos níveis de validação. Por outro lado, os componentes menos valiosos ou mais facilmente substituíveis poderão ficar situados em zonas mais periféricas, e por conseguinte, não necessitarem de tantos meios de validação para serem acedidos;
- **Localização dos *Datacenters* –** seguindo a linha de pensamento apresentada no ponto anterior, aqui o autor especifica quais as características que o local onde é acondicionado o *datacenter* tem que ter. Em 1º lugar o autor refere as condições óptimas, caso as instalações estejam a ser pensadas de raiz. Porém, isso nem sempre é possível, e nesse caso é necessário "*uma boa dose de bom senso e sensibilidade para os factores que podem afectar adversamente a informação*" para que se planeie as condições de localização do *datacenter* com as instalações existentes;
- **Controlo de Acessos –** embora este conceito também seja descrito na segurança lógica, neste âmbito refere-se ao controlo de acesso (quem entra e quem sai) das instalações físicas da organização. É fundamental a criação e utilização de medidas de controlo de acesso físico às

instalações, principalmente quando falamos de acesso a áreas sensíveis, como é o caso dos centros de dados, arquivos centrais, etc. As medidas a implementar devem ser pensadas e adequadas a cada caso, ou seja, quanto mais sensível a informação, mais complexo deverá ser o controlo de acessos ao local onde a informação está localizada. No entanto, o autor ressalva ainda a importância de sensibilizar os colaboradores da empresa para as questões da SI, pois só assim as medidas de segurança passarão da teoria à prática;

- **Eliminação de Resíduos –** os resíduos (lixo) devem ser devidamente eliminados. O autor refere um popular ataque de *hackers*, intitulado "*dumpster diving*" e que consiste na procura de informação preciosa que por vezes pode ser resgatada de um caixote do lixo e ser utilizada para futuros ataques informáticos ou físicos que podem ser levados a cabo através de, por exemplo, engenharia social;
- **Rasto –** consiste no registo (gravações de vídeo, áudio, registos biométricos, cartões de acesso, etc) de qualquer actividade monitorizada nas instalações da organização. É através do rasto que é possível reconstituir um qualquer evento, revelando quem fez o quê, quando e como.

Como foi referido acima, este autor cria uma outra área da SI, denominada segurança do pessoal. Embora muitas vezes a segurança se ocupe em grande parte das questões de ordem tecnológica, as estatísticas têm vindo a comprovar que a componente humana tem um grande impacto na SI, ou seja, muitas vezes a origem dos problemas não está nos meios tecnológicos, mas sim na utilização desses mesmos meios. São as pessoas que "*interagem diariamente com os sistemas, que têm acesso à informação neles contida, que condicionam o processamento dessa mesma informação, que a gerem*" (SILVA, et al., 2003), como tal, muitas vezes são essas pessoas que constituem a principal ameaça à SI. Esse é um facto que, cada vez mais, se tem denotado nas estatísticas, que comprovam exactamente a existência de um grande número de ataques consumados pelos *stakeholders* da organização, quer de forma premeditada, quer como resultado de acções mal executadas (erro humano). O autor refere-nos algumas questões a ter em conta nesta área:

- **Recrutamento –** é desde logo na fase de recrutamento de cada novo elemento na organização que lhe deve ser comunicado quais as componentes de segurança associadas à função para a qual concorre e qual a filosofia de segurança da empresa (política de segurança, acções aceitáveis, etc);
- **Documentação –** toda a política, normas e procedimentos devem estar devidamente documentados, de forma coesa, actual e apropriada. O primeiro e mais essencial passo consiste na adequada divulgação da política de segurança da organização a todos os *stakeholders*, através da entrega a cada elemento de um memorando interno que deverá incluir uma cópia integral dessa mesma política. Neste ponto existem dois factores essenciais a ter em conta: desde logo é crucial que a política de segurança não seja sujeita a interpretações ambíguas; por outro lado, a leitura da política de SI por cada elemento deve constituir apenas o início, e não o fim, da introdução destes à filosofia de SI da organização;
- **Boas Práticas –** o conjunto de boas práticas da empresa devem ser devidamente comunicadas a todos os colaboradores, de preferência desde logo no momento de contratação dos mesmos, quer se tratem de boas práticas formais, quer se tratem de boas práticas informais que fazem parte da cultura da organização. A explicação dessas balizas de comportamento é essencial para que as decisões desse campo não sejam deixadas ao critério de cada um;
- **Formação –** devem ser preparadas, em conjunto com o Departamento de Recursos Humanos, acções de formação sobre segurança, onde os utilizadores devem ser instruídos sobre "*como realizar as tarefas quotidianas que lhes competem, de modo a não afectar a segurança dos sistemas de informação*", devem ser apresentadas as tecnologias em utilização na organização, os seus objectivos e as implicações que essas medidas de protecção têm para quem as utiliza;
- **Sensibilização –** para além das acções de formação focadas em aspectos específicos da segurança dos sistemas de informação, devem também ser realizadas acções de sensibilização junto dos colaboradores sobre questões mais concretas, como por exemplo questões relacionadas com as palavras-chave, possíveis ataques de engenharia social, etc. A

sensibilização dos stakeholders "*levará a que estes exerçam o seu sentido crítico, tentando detectar atitudes suspeitas ou pedidos inusitados*";

- **Segregação de responsabilidades –** deve ser evitada a atribuição de funções ou processos vitais de uma organização a uma única pessoa, pois somos humanos, e como tal, estamos sujeitos a cometer erros. A organização deve sempre atribuir funções vitais a dois ou mais colaboradores, diminuindo assim a probabilidade da ocorrência de falhas ou erros que podem prejudicar o funcionamento da empresa.

Por último, falta ainda referir a área da segurança lógica, na perspectiva de Pedro Silva. Esta é provavelmente a área mais rica, complexa e difícil de gerir, pois abarca um alargado número de disciplinas. A crescente evolução das tecnologias e a complexidade que acarretam vêm dificultar ainda mais a tarefa de gerir esta área de segurança. Segundo o autor, podem-se destacar três grandes áreas que cobrem a totalidade dos temas desta disciplina: prevenção, protecção e reacção, que são constituídas por alguns dos seguintes sub-tópicos:

- **Autenticação e Controlo de Acesso –** são dois aspectos muito importantes nos sistemas de informação, pois é a autenticação e o controlo de acesso que asseguram que nós somos quem dizemos ser, e que nos permite aceder àquilo a que temos direito, tanto a nível de infra-estrutura (redes de comunicações e sistemas), como a nível aplicacional;
- **Criptografia –** este é um mecanismo utilizado desde os tempos de Júlio César, e que permite sobretudo garantir a confidencialidade da informação. A cifra "*é o processo através do qual se protege (encripta) um conjunto de dados, de modo a que este apenas possa ser desprotegido (desencriptado) por alguém que conheça um determinado segredo*". No fundo, tanto o remetente como o destinatário da informação têm a chave para cifrar/decifrar a informação, sendo que essas chaves podem ser simétricas ou assimétricas (chave privada/ chave pública);
- **Infra-Estrutura de Chaves Públicas –** é uma combinação de software, cifra e serviços que permite garantir a protecção e autenticação de comunicações digitais, através da gestão segura de chaves assimétricas.

Esta tecnologia integra certificados digitais, criptografia de chaves públicas e autoridades de certificação;

- **VPN**[1] **–** as redes privadas virtuais assentam na utilização de vários protocolos e medidas de segurança e permitem criar canais seguros de comunicação em ambientes públicos, como a internet. Toda a informação transmitida através desses canais é cifrada e possui controlo de integridade;
- **Filtragem de Conteúdos –** trata-se de ferramentas que permitem bloquear, quer a entrada, quer a saída, de determinados conteúdos;
- **Redundância –** consiste na criação de réplicas de informação ou infra-estruturas, como forma de evitar a indisponibilidade da informação;
- **Salvaguarda da Informação –** sendo a informação o bem mais precioso das organizações deve, como tal, ser devidamente salvaguardado. As organizações necessitam proteger um conjunto cada vez mais amplo e complexo de informação, dispersa por diferentes suportes e gerada por diversas aplicações. Como tal, necessitam ter soluções de salvaguarda, ou *backup*, que permitam responder satisfatoriamente à protecção da informação;
- **Detecção de Intrusões –** trata-se de sistemas que permitem analisar o tráfego e as actividades das redes, conseguindo assim detectar tentativas não autorizadas de acesso à infra-estrutura lógica. O objectivo destes sistemas é o de proporcionar uma visão do que acontece na rede;
- **Resposta a Ataques –** embora esta questão não seja exclusivamente da segurança lógica, assume aqui particular relevo, pois é nesta área que o responsável pela SI na organização terá que tomar decisões complexas. De forma sucinta, devem ser previstos um conjunto de procedimentos a accionar caso existam ataques aos sistemas da organização;
- **Segurança no Desenvolvimento –** no caso do desenvolvimento de software, os aspectos relacionados com a segurança do código devem ser verificados. Para além disso, devem ainda ser implementados, na fase de especificação, os controlos de segurança desejados.

[1] VPN – Virtual Private Network

No entanto, estas não são as únicas linhas de pensamento sobre as áreas de SI. Existem ainda autores que defendem uma divisão diferente e que vale a pena analisar. Na perspectiva de Zúquete, podem-se considerar três grandes áreas de actividade em SI, todas elas importantes e com as suas especificidades (ZÚQUETE, 2008):

- **Defesa contra catástrofes físicas –** tem como objectivo garantir a sobrevivência de determinado sistema de informação ou serviço que esse sistema preste, e por conseguinte, garantir a protecção da informação nele contida em caso de existir alguma catástrofe que acarrete consequências a nível físico. Podem ser:
    - Catástrofes ambientais – tremores de terra, inundações, incêndios, queda de raios, tempestades magnéticas, etc;
    - Catástrofes políticas – ataques terroristas, motins, etc;
    - Catástrofes materiais – degradação irreparável de equipamentos computacionais, como discos magnéticos, perda/roubo de equipamentos computacionais, etc.
- **Defesa contra faltas/falhas previsíveis –** visa minimizar o impacto de problemas que, embora tenham um impacto global normalmente menor, ocorrem com maior frequência. Exemplos disso são:
    - Quebra no fornecimento de energia eléctrica ou falha na fonte de alimentação de um equipamento computacional;
    - Bloqueio na execução de aplicações ou sistemas operativos;
    - Falhas temporárias de conectividade em troços de rede.
- **Defesa contra actividades não autorizadas –** nas áreas anteriores viram-se um conjunto de problemas causados por acontecimentos fortuitos que normalmente são resultado do acaso, e portanto, são acontecimentos previsíveis, embora o momento em que ocorram não o seja. Por outro lado, esta área abarca acontecimentos despoletados intencionalmente por sujeitos, cujo resultado será um conjunto de problemas/anomalias no normal funcionamento dos sistemas de informação. Por norma, são actos que não deixam rasto, e portanto devem ser previstos e contrariados de forma preventiva. Alguns exemplos são:

- Acesso a informação – reservada ou confidencial e que pode estar guardada num sistema ou pode estar em trânsito na rede;
- Alteração de informação – actividades que pretendem alterar ou eliminar sem autorização informação pertencente a terceiros guardada em sistemas ou em trânsito na rede;
- Utilização exagerada ou abusiva de recursos computacionais – recursos esses que podem ser de diversos tipos: tempo de processamento, memória primária ou secundária, tempo e material de impressão, ocupação de redes de comunicação, etc. O resultado desse uso exagerado/abusivo poderá ser a indisponibilidade dos recursos para terceiros.
- Impedimento de prestação de serviço (DoS[2]) – este é um caso extremo do resultado da utilização excessiva ou abusiva de recursos computacionais;
- Vandalismo – é um caso extremo de um ataque DoS e que consiste numa interferência com o normal funcionamento do sistema sem qualquer benefício, directo ou indirecto, para o sujeito causador.

3.1.1.2. Pilares da Segurança da Informação

Como já foi referido anteriormente, a SI tem como finalidade a protecção da confidencialidade, integridade e disponibilidade da informação. Grande parte dos autores referem exactamente este trinómio como constituindo os principais pilares que a SI pretende garantir. No entanto, existem autores que fazem uma divisão diferente, em que para além dos 3 pilares acima referidos (confidencialidade, integridade e disponibilidade) incluem ainda um quarto pilar – a autenticidade. Nesta última perspectiva, os autores que a defendem entendem que a SI pretende garantir a protecção da confidencialidade, integridade e autenticidade, sendo que a disponibilidade é considerada um "pré-requisito", ou seja, é mais abrangente, imprescindível até, e necessita estar sempre presente para que se garantam os outros pilares, pois se não houver disponibilidade não é sequer colocada a problemática de ter que se garantir os

[2] DoS – Denial of Service

outros pilares. Por exemplo, caso não tenhamos electricidade não podemos ligar o computador, logo não existe disponibilidade. Uma vez que não existe disponibilidade nem sequer se chega a colocar a questão/necessidade de garantir a confidencialidade, integridade ou autenticidade da informação.

Em suma, esta última perspectiva apresenta duas diferenças substanciais relativamente à primeira visão apresentada: nesta segunda perspectiva o pilar disponibilidade deixa de ser entendido como um pilar ao mesmo nível da confidencialidade e integridade e passa a ser encarado numa visão mais macro, sendo pré-requisito obrigatório para que se possam então garantir a confidencialidade e integridade; a segunda diferença substancial tem a ver com o facto de se encarar a autenticidade como um pilar ao mesmo nível da confidencialidade e integridade, ao contrário da primeira visão aqui apresentada, em que a autenticidade é vista como um dos conceitos (inter-relacionado) que permite garantir a integridade.

Neste âmbito será adoptada a primeira visão aqui apresentada, e que define três pilares para a SI: confidencialidade, integridade e disponibilidade, sendo que a autenticidade é vista como uma forma de garantir a integridade da informação, ressalvando-se, no entanto, que não é considerada menos importante do que as anteriores. Jim Clinch apresenta uma figura bastante elucidativa sobre a relação destes conceitos, num artigo redigido para a ITIL (CLINCH, 2009):

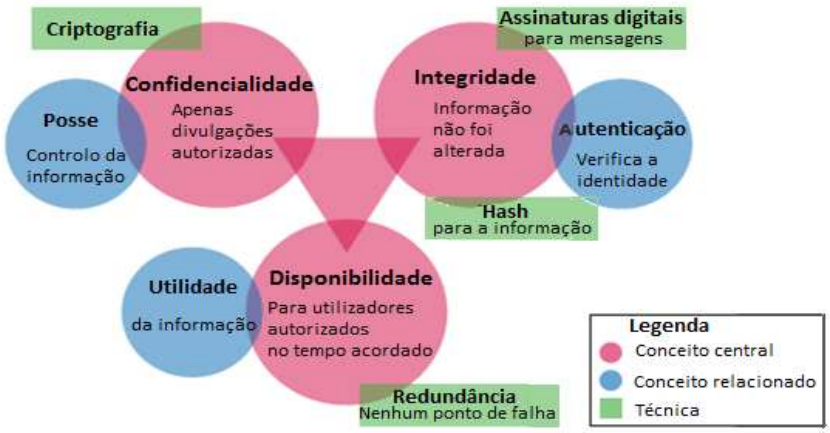

Figura 4 – Conceitos centrais e secundários da Segurança da Informação

A confidencialidade pretende garantir que apenas os destinatários e sistemas autorizados têm acesso à informação. A informação constitui uma vantagem competitiva para as organizações, e como tal esta nem sempre deve ser conhecida por todos os indivíduos. Ter confidencialidade significa ter a segurança de que o que foi dito ou escrito apenas será transmitido ou acedido por quem tiver autorização para tal.

Os requisitos da confidencialidade são definidos ou influenciados pela classificação da informação(SILVA, et al., 2003), pois é a classificação que nos permite percepcionar qual o valor da informação, e por conseguinte, qual o seu nível de confidencialidade. Alguns exemplos de violação da confidencialidade podem ser "*ler o email de outra pessoa, procurar conteúdo no lixo e anotar passwords*"(CLINCH, 2009).

O segundo pilar diz respeito à integridade da informação e o seu objectivo é garantir que a informação não é alterada ou modificada, intencionalmente ou casualmente, no seu armazenamento ou transmissão, excepto por pessoas autorizadas para o efeito. A integridade é um dos aspectos cruciais a garantir relativamente à informação processada, armazenada e transmitida pelos sistemas de informação, pois é através deste pilar que se garante que a informação é fidedigna. Deverão portanto, existir sistemas de validação da informação existente, que dependendo do grau de importância da informação, poderão ser automáticos (por exemplo regras automáticas de validação da introdução) ou manuais (por exemplo, podem ser instituídos procedimentos de revisão, por amostragem, da integridade da informação existente).

O acesso atempado à informação é crucial e dele depende a prossecução dos objectivos da organização, pois "*possuir a informação necessária mas não a ter disponível no momento adequado equivale a não possuir qualquer informação*"(SILVA, et al., 2003). É exactamente desse aspecto que trata o último pilar da SI. A disponibilidade pretende assim garantir que a informação está disponível aos utilizadores ou sistemas autorizados, no momento em que estes a querem aceder. Este pilar refere-se quer à disponibilidade da informação quer à estrutura física e tecnológica que permite o seu acesso, transmissão e armazenamento. Assim, a disponibilidade da informação permite que esta seja utilizada quando necessário, esteja ao alcance dos seus utilizadores e destinatários e possa ser acedida no momento pretendido.

Embora as medidas de protecção da informação devam contemplar aspectos que facilitem o seu acesso, por outro lado, devem também ser capazes de distinguir acessos autorizados de acessos não autorizados. Para tal, é necessário conhecer os utilizadores e criar regras para o uso da informação, através de, por exemplo, a classificação da informação conforme o seu valor para a organização.

Acima de tudo, é crucial criar um equilíbrio entre o acesso à informação e a preservação da confidencialidade da mesma. Assim, as medidas de protecção não

devem expor a informação (permitir o acesso indevido) nem devem impedir ou dificultar o seu acesso (devido).

Para proteger a disponibilidade são levadas em consideração muitas medidas, entre as quais se podem destacar:

- Configuração segura de um ambiente em que todos os utilizadores que fazem parte do processo comunicacional estejam dispostos de forma adequada a assegurar o sucesso da leitura, transmissão e armazenamento da informação;
- Criação de réplicas, que permitem a duplicação da informação, e por conseguinte, a duplicação dos locais de acesso. Assim, caso não seja possível aceder a informação num local/sistema, existe um segundo ponto de acesso;
- Estabelecer rotas alternativas para a disseminação da informação, para garantir o seu acesso e a continuidade dos negócios, inclusive quando alguns dos recursos tecnológicos não estejam em perfeitas condições de funcionamento.

Este último pilar da SI influencia os outros, na medida em que, caso a informação não esteja disponível, conforme se referiu anteriormente, também não existe a necessidade de garantir a sua confidencialidade e integridade, pois a informação não está sequer disponível.

Assim sendo, a informação deve estar sempre disponível, desde que seja salvaguardada a sua confidencialidade e integridade, ou seja, só deverá estar disponível aos utilizadores devidamente autorizados a acede-la e/ou alterá-la.

3.1.1.3. Vulnerabilidades, Ataques, Riscos e Defesas

Nos dias correntes assistimos a uma crescente utilização de sistemas computacionais ligados por redes, em particular pela internet, para armazenar e transmitir informação. Desta forma, a segurança dessa informação e dos sistemas que a guardam e disseminam ganha maior relevância, especialmente se o contexto for organizacional.

Se por um lado, a utilização de toda esta tecnologia permite uma maior dinâmica ao trabalho, por outro lado, acarreta também uma série de complexidades que necessitam ser pensadas para que estes benefícios não se tornem prejuízos.

É cada vez maior a percepção de que na segurança da informação não se tratam somente as questões de âmbito técnico ou tecnológico, sendo muito mais transversal e ampla, tratando-se também as questões de âmbito social. Com efeito, por um lado, trata-se de um problema técnico, pois os sistemas de informação são constituídos por arquitecturas de *hardware*, sistemas operativos, protocolos aplicacionais e requisitos aplicacionais, que fazem com que seja difícil pôr em prática e manter políticas de segurança em sistemas ligados à internet. Por outro lado, é um problema social pois a maioria dos utilizadores desses sistemas não conhecem, e por conseguinte, não estão conscientes dos problemas de segurança a que estão sujeitos nem de qual a melhor forma de lidar com eles.

Neste contexto impõe-se a definição de alguns conceitos que aqui são centrais para perceber esta problemática. Comecemos pelo conceito de vulnerabilidade, que segundo Zúquete é uma "*característica de um sistema que o torna sensível a certos ataques*"(ZÚQUETE, 2008), constitui assim uma fraqueza do sistema "*que poderia ser explorada por uma Ameaça. Por exemplo, uma porta firewall aberta, uma password que nunca é alterada*"(CLINCH, 2009).

Por sua vez, o ataque é constituído por um conjunto de passos executados com o intuito de concretizar uma acção ilícita através da exploração de uma vulnerabilidade do sistema. Apesar de muitas vezes se pensar que grande parte dos ataques provém do exterior, a verdade é que é exactamente através dos indivíduos internos que se verifica um grande número de ataques, correspondendo segundo as estatísticas, a cerca de 55%(DOLYA, 2007) das ocorrências de ataques nas organizações, e este é um número com tendência para aumentar ano após ano. Este tipo de ataques é praticado pelos *stakeholders* da organização que aproveitam determinadas vulnerabilidades dos sistemas, processos e aplicações com o intuito de obter "*(i) ganho pessoal e lucro tais como fraudes e golpes, roubo de informação e outros recursos, ou (ii) ter um comportamento irresponsável (se não tiver intenção de causar danos), danos mal-intencionados e/ou sabotagem (se intenciona causar dano) a nível corporativo, operacional ou tecnológico*"(HUMPHREYS, 2008).

Relativamente ao risco, este consiste nos danos que podem resultar de um ataque bem sucedido. A produção científica existente sobre SI estuda e aborda predominantemente as questões relacionadas com os riscos. Henrique São Mamede(MAMEDE, 2006) associa inclusive o termo riscos de segurança à sua prevenção e também à minimização desses riscos, referindo que segurança implica a capacidade para serem tomadas medidas preventivas capazes de evitar ocorrências inesperadas e/ou indesejadas. Segundo o autor, importa proceder a uma identificação dos elementos mais fracos do sistema a utilizar (vulnerabilidades), de modo a serem encontradas soluções adequadas que considerem os riscos e respectivos custos relacionados com a protecção dos sistemas e da informação.

O risco de uma ameaça é obtido a partir da combinação entre a probabilidade de ocorrer uma ameaça e a magnitude dos impactos que esta terá, conforme demonstra a seguinte figura (JOSANG ; ALZOMAI, 2007):

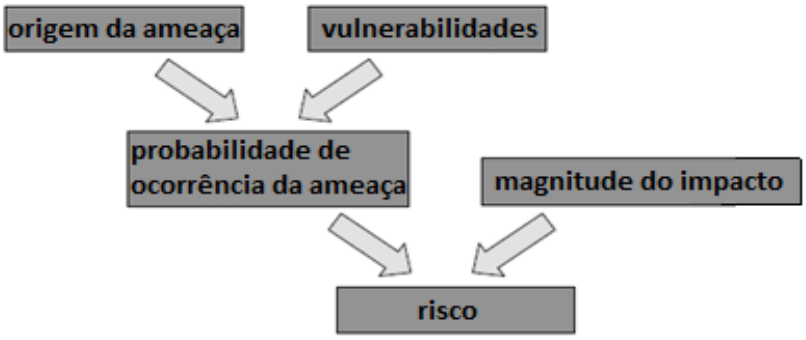

Figura 5 – Princípio para determinar o Risco

De acordo com o CSI (2008)(TINTAMUSIK, 2010), a média anual de perdas provocadas por ataques mais que duplicou de $168,000 em 2006 para $350,424 em 2007, o que reforça a importância de investir numa correcta análise e gestão do risco.

Por último, a defesa consiste no "*conjunto de políticas e mecanismos desenhados, concretizados e implantados para (i) diminuir as vulnerabilidades de um sistema, (ii) detectar e contrariar/anular ataques passados ou actuais e (iii) minimizar os riscos decorrentes de ataques bem sucedidos*"(ZÚQUETE, 2008). Uma boa defesa deve ter em consideração os três conceitos apresentados anteriormente. As vulnerabilidades devem ser minimizadas para evitar ataques, especialmente os automatizados; no entanto, é impossível erradicar totalmente as vulnerabilidades, pelo que a defesa deve sempre manter a vigilância sobre o estado e funcionamento dos sistemas para detectar possíveis anomalias provocadas por ataques; por fim, deve

sempre prever-se o pior dos cenários, que neste caso é um ataque bem sucedido, por isso é crucial fazer planos de contingência para minimizar os riscos decorrentes dos ataques. Os planos de contingência devem considerar formas de recuperação de bens e serviços que possam ser afectados pelos ataques.

No que concerne à segurança, a defesa pode ser aplicada segundo duas políticas: defesa de perímetro e defesa em profundidade. A defesa de perímetro consiste na definição de um perímetro protegido, onde é englobado um conjunto de máquinas e redes que devem ser protegidas de possíveis invasores externos. Se dermos o exemplo de uma organização, a sua defesa de perímetro consiste na defesa da sua estrutura em relação ao exterior. Por sua vez, a defesa em profundidade é mais complexa, porém talvez mais eficaz, e consiste em proteger os sistemas actuando em níveis e não em fronteiras. Pegando no exemplo anterior, a defesa em profundidade é feita dentro da organização, tendo em consideração os diferentes tipos de utilizadores e níveis de acesso.

3.1.1.4. Políticas e Mecanismos de Segurança

Pode dizer-se que, em termos estritos, os problemas de segurança estão intrinsecamente relacionados com a forma como a segurança é encarada no interior das organizações. Esta situação pode conduzir à emergência de algumas questões, de entre as quais se refere a necessidade de identificar quem decide a adopção de políticas de segurança. Esta situação, crucial para todas as actividades relacionadas com a segurança organizacional, requer um comprometimento inequívoco da gestão de topo, não apenas na designação do respectivo responsável, mas também na atribuição dos recursos essenciais ao desenvolvimento das actividades necessárias. Neste sentido, (MAMEDE, 2006) refere que "*a segurança de uma organização deve ser analisada num contexto alargado*", onde devem ser consideradas todas as perspectivas de modo a reflectir a multidisciplinaridade da segurança.

Segundo Clinch, a política de segurança pretende "*gerir a abordagem da organização à Gestão da Segurança da Informação*". A política existente numa organização vai influenciar as características dos seus sistemas de informação e, para

que seja eficaz, deve estar sempre alinhada com o planeamento estratégico dessa mesma organização.

Um aspecto fulcral para o sucesso das políticas de segurança é, para além do compromisso da gestão de topo, a comunicação dessas mesmas políticas a todos os elementos da organização, para que estes as compreendam, estejam sensíveis a elas e, por conseguinte, as cumpram. Deste modo, a política de segurança deve conter directrizes claras a respeito de, pelo menos, os seguintes aspectos(SILVA, 2009):

- Objectivos de segurança – devem explicar de forma rápida e sucinta a finalidade da política de segurança;
- A quem se destina – deve definir claramente quais as estruturas organizacionais às quais a mesma se aplica;
- Propriedade dos recursos – deve definir de forma clara as regras que irão reger os diversos aspectos relacionados com a propriedade dos recursos da informação;
- Responsabilidade – deve definir claramente qual o tipo de responsabilidades envolvidas com o manuseamento dos recursos da informação;
- Requisitos de acesso – deve indicar de forma clara quais os requisitos a serem atendidos para o acesso aos recursos da informação;
- Responsabilização – deve indicar as medidas a serem tomadas no caso das normas serem infringidas;
- Generalidades – nesta secção podem ser incluídos aspectos que não caibam nas demais secções. Pode-se incluir, por exemplo, a definição dos conceitos envolvidos, um glossário e uma indicação das normas acessórias.

Segundo Zúquete, a política de SI define um conjunto de requisitos que devem ser cumpridos, como por exemplo(ZÚQUETE, 2008):

- Autenticação de sujeitos ou serviços;
- Autorização de sujeitos ou serviços;
- Privilégios de sujeitos ou serviços;
- Monitorização e registo de actividades;
- Auditoria de registos de actividades.

Caso o sejam, surtem resultados como:

- Garantia de confidencialidade de informação reservada ou confidencial;
- Protecção de informação crítica;
- Continuidade de operação ou de prestação de serviço;
- Confiança na correcção de operação do sistema;
- Prova de correcção ou de autoria na troca de informação;
- Capacidade de auditoria de acções passadas;

Dito isto, pode-se concluir que as políticas consistem num conjunto de princípios que devem ser colocados em prática. Para tal, é necessário recorrer a um conjunto de mecanismos, cujo objectivo é exactamente o de materializar as políticas em contextos concretos. No entanto, o universo de mecanismos existentes é muito vasto e pode até mesmo ser contraditório. Tomemos como exemplo a implementação de um mecanismo de análise do tráfego da rede para detectar actividades não autorizadas, que caso seja implementado simultaneamente com um mecanismo de cifragem do tráfego sujeito a análise, poderá, em alguns casos, culminar na anulação dos efeitos que supostamente deveriam surtir, uma vez que a implementação do primeiro mecanismo pode resultar na anulação dos efeitos do segundo mecanismo. Isto para explicar que os mecanismos não devem ser seleccionados através de uma perspectiva muito pormenorizada das políticas, pois perderíamos a visão global e acabaríamos por não obter resultados, como o que foi exemplificado. Deve, portanto, ter-se uma visão global das políticas para se seleccionarem os mecanismos de segurança a implementar, sendo que estes devem apenas servir para aplicar as políticas não devendo interferir de outra forma com as actividades das pessoas e sistemas.

A selecção, instalação e manutenção dos mecanismos de segurança é uma tarefa complexa e que deve ser constante para que se acompanhe a evolução dos ataques e dos mecanismos de defesa, caso contrário estes acabam por se tornar obsoletos. A lista de mecanismos é extensa, mas podem-se considerar a título de exemplo os seguintes (ZÚQUETE, 2008):

- Mecanismos de confinamento – criam barreiras à difusão de actividades para além de barreiras de segurança, é o caso das *firewalls*, zonas desmilitarizadas (DMZ), etc;

- Mecanismos de controlo de acesso – permitem aferir se determinado sujeito pode ou não realizar determinada acção sobre um determinado objecto, é o caso das protecções no acesso aos dispositivos e à configuração do sistema operativo, protecção de ficheiros, etc;
- Mecanismos de execução privilegiada – destinam-se a conceder privilégios acrescidos a aplicações especiais que sejam executados por utilizadores que normalmente não têm tais privilégios;
- Mecanismos de filtragem – servem para realizar determinadas formas de confinamento ou controlo de acesso, isto é, servem para identificar actividades desnecessárias ou não autorizadas e evitar que as mesmas se concretizem. A filtragem de tráfego de rede é um exemplo deste tipo de mecanismo;
- Mecanismos de registo – produzem relatórios mais ou menos exaustivos de actividades solicitadas ou realizadas e servem para, por um lado, analisar se o sistema que os produz está a funcionar correctamente ou se estão a ocorrer erros, e por outro lado, serve para analisar sistemas atacados identificando a origem do problema e o *modus operandi* do atacante. Alguns exemplos são os ficheiros de registo (Linux) e o registo de eventos (Microsoft);
- Mecanismos de inspecção – estão permanentemente a observar o sistema de forma a detectar actividades inesperadas, ilegais ou ilícitas. São complementares a outros mecanismos, pois permitem detectar falhas na configuração destes. Um exemplo deste tipo é o sistema de detecção de intrusões;
- Mecanismos de auditoria – inspeccionam e analisam registos e permitem tirar conclusões após ter acontecido algo inesperado;
- Algoritmos criptográficos e afins – este tipo de mecanismo é insubstituível no que concerne à protecção da informação;
- Protocolos criptográficos – consistem em trocas ordenadas de dados entre entidades em que parte ou a totalidade desses dados são cifrados. Muitos dos mecanismos de segurança para sistemas distribuídos usam ou baseiam-se em protocolos criptográficos.

3.2. Planeamento Estratégico de Sistemas de Informação

Neste subcapítulo pretende-se abordar de forma sucinta a temática do planeamento estratégico de sistemas de informação, não se pretende portanto, ir a um nível exaustivo, mas sim apresentar uma visão geral.

O planeamento pode ser definido como uma programação de actividades, e não a descoberta de algo. Por sua vez, a estratégia consiste num processo de elaboração de algo, sendo portanto um processo criativo. Cassidy define estratégia como "*refere-se a um nível global de pensamento acerca dos sistemas de informação da organização e a sua integração com o resto da empresa*" (CASSIDY, 1998).

O planeamento estratégico está presente nas organizações desde logo na definição da sua missão e objectivos, sendo que no caso dos objectivos o planeamento estratégico é feito a três níveis (SOARES, 2009): nível operacional, onde são definidos os objectivos específicos e mensuráveis, normalmente definidos pelos níveis de gestão intermédia; a nível táctico, em que os objectivos normalmente são definidos pelos níveis de gestão intermédios para unidades de negócio ou departamentos; e por fim, a nível estratégico, onde são definidos os objectivos genéricos sobre os resultados pretendidos pela organização no futuro.

Mas o planeamento estratégico não se esgota aqui, ele constitui um processo muito mais amplo e complexo (SOARES, 2009):

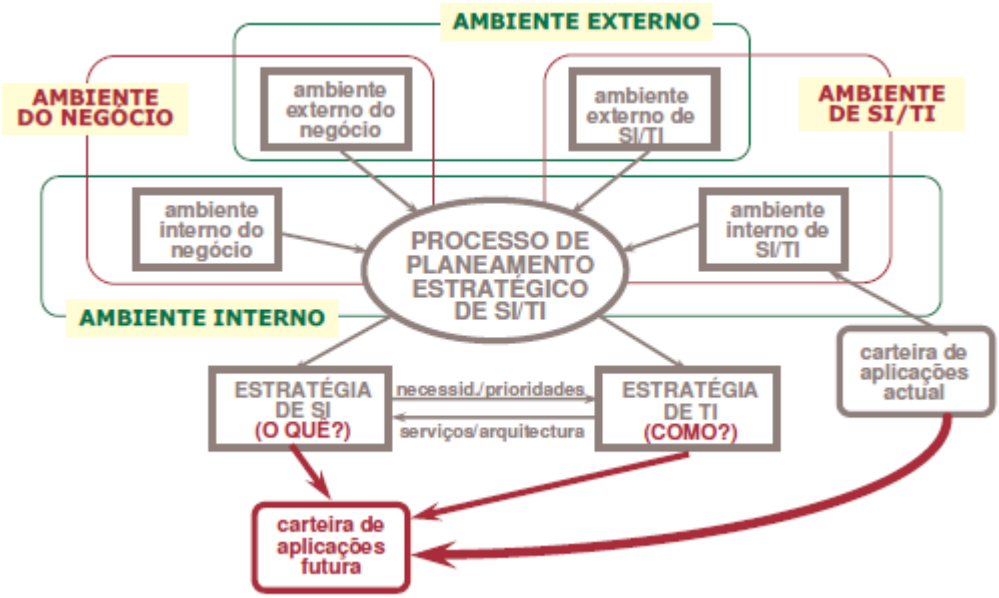

Figura 6 – Modelo para o Planeamento Estratégico de SI/TIC

Grande parte deste modelo será abordado no subcapítulo seguinte, aqui impõem-se ainda uma breve explicação sobre as características da estratégia de sistemas de informação e a estratégia de TIC (Tecnologias de Informação e Comunicação). De forma genérica, a estratégia do sistema de informação define: quais as necessidades futuras do negócio; quais as funções componentes do negócio; quais as necessidades de informação e de sistemas para o negócio; quais as prioridades, face aos imperativos do negócio; e quais os responsáveis pela satisfação dessas necessidades, ao nível do planeamento, desenvolvimento e implementação do sistema de informação. Por sua vez, a estratégia de TIC define: como é que as necessidades são satisfeitas, de acordo com as prioridades estabelecidas na estratégia do sistema de informação; como é que as aplicações são obtidas; e como é que as tecnologias e os recursos humanos que lhes estão associados são utilizadas e geridas.

As vantagens para o desenvolvimento do planeamento estratégico de sistemas de informação nas organizações são muitas e distintas dependendo do contexto, no entanto existem alguns benefícios comuns:

- Gestão efectiva dos recursos caros e críticos para a organização;
- Melhoria na comunicação e no relacionamento entre os negócios e os sistemas de informação da organização;
- Alinhamento das direcções e prioridades dos sistemas de informação com as direcções e prioridades do negócio;
- Identificação de oportunidades para a utilização da tecnologia como vantagem competitiva e aumentar o seu valor para o negócio;
- Planeamento do fluxo informacional e dos processos;
- Atribuição eficaz e eficiente dos recursos dos sistemas de informação;
- Redução do esforço e custo necessário ao longo do ciclo de vida dos sistemas.

Por outro lado, a falta de estratégia de sistemas de informação e TIC acarreta consequências às organizações, desde logo o incumprimento dos objectivos de negócio. Se não houver planeamento estratégico, a integração dos sistemas será mais difícil e essa falta de integração provoca duplicações de esforços, imprecisões, atrasos e uma gestão da informação deficiente. Relativamente aos sistemas, se estes não forem planeados o seu desenvolvimento acaba por se atrasar, custar mais do que o esperado e

poderão não cumprir as funções previstas. Os planos e prioridades são constantemente alterados se não forem planeados estrategicamente, acabando por reduzir a produtividade e criando conflitos entre os envolvidos no processo. Deve sempre existir um alinhamento entre os sistemas de informação, as TIC e o negócio, caso contrário estes poderão, não só não se integrarem no negócio, como podem constituir obstáculos ao sucesso do mesmo.

Assim, o planeamento estratégico dos sistemas de informação constitui uma prática crucial para o sucesso da organização e para a sua vantagem competitiva em relação à concorrência. São muitos os factores de sucesso, podendo-se destacar os seguintes(SOARES, 2009):

- Foco externo (e não interno) – olhar para os clientes, concorrentes, fornecedores e outras indústrias, compreendendo as relações de negócio e as semelhanças;
- Acrescentar valor, e não reduzir custos;
- Partilhar os benefícios – dentro da organização, com os fornecedores, clientes e mesmo com os concorrentes;
- Perceber os clientes – e o que fazem com o bem e/ou serviço;
- Orientação pela inovação do negócio, não pela inovação da tecnologia – as mais importantes falhas no uso das TIC são geralmente baseadas em tecnologia muito boa e uma visão de negócio muito má. Os sucessos vêm de tecnologia suficientemente boa e uma clara compreensão do cliente;
- Utilizar a informação adquirida pelos sistemas para desenvolver o negócio.

3.2.1. Ciclo de Desenvolvimento Estratégico

Nesta secção é abordado de forma sucinta o ciclo de desenvolvimento estratégico, que está implícito no processo de planeamento estratégico de Sistemas de Informação/Tecnologia de Informação (SOARES, 2009):

Figura 7 – Ciclo de Desenvolvimento Estratégico

A primeira etapa deste modelo consiste na análise estratégica do negócio, que é realizada através de um conjunto de técnicas e ferramentas que permitem esta análise: Análise SWOT, Análise do meio ambiente externo (análise do meio ambiente macro e modelo das 5 forças de Porter), Análise do meio ambiente interno (análise dos recursos, capacidades e competências centrais, cadeia de valor), Opções estratégicas, Carteira do negócio, Factores críticos de sucesso, e por último *Balanced Scorecard*. A segunda etapa diz respeito ao modelo de negócio, que inclui: Arquitectura, que caracteriza os *stakeholders* do negócio e respectivos relacionamentos esclarecendo os produtos, serviços, meios financeiros e informação que trocam; Proposta de valor, onde são descritos os potenciais benefícios para os diversos intervenientes; e o Modelo do rendimento, que descreve como são gerados os rendimentos. Actualmente existe uma enorme diversidade de modelos de negócio, um exemplo deste tipo de modelo é a cadeia de valor de Porter. A terceira etapa diz respeito à arquitectura da informação que permite especificar: de onde provém a informação (dentro e fora); como é que a informação é coligida e utilizada pelas diversas actividades da organização; quem deve ser o responsável pela gestão da informação; quem partilha a informação e com que finalidades; que necessidades existem de bases de dados e por quem são acedidas; que processos devem ocorrer primeiro e quais devem decorrer em paralelo; que interdependências existem entre sistemas e que temporizações; e que alteração das

responsabilidades organizacionais devem ocorrer para que sejam adequadas a uma visão do negócio fortemente suportado pela informação. Por último, temos a implementação e integração do sistema de informação. Após serem identificados os requisitos que o sistema de informação necessita ter, pode-se recorrer à carteira de aplicações de MacFarlan. Esta carteira permite classificar os sistemas de informação de acordo com o modo como contribuem para o sucesso do negócio e tem especial utilidade no auxílio da identificação das prioridades na aquisição ou desenvolvimento de aplicações.

3.3.Sistema de Gestão da Segurança da Informação

O desenvolvimento e expansão das TIC (Tecnologias de Informação e Comunicação) e a disseminação da internet não só mudaram estilos de vida e a gestão dos negócios, como também impulsionaram a criação de novos negócios. No entanto, acarretaram consigo mudanças e efeitos adversos, tais como o rápido aumento do *hacking*, vírus e roubo da informação.

Esta realidade transformou o modo como as organizações olham a gestão da segurança da informação, que neste contexto se tornou um factor a considerar na gestão dos negócios. Por vezes, as organizações despendiam recursos na aquisição de *firewalls*, *proxys*, antivírus, mecanismos de detecção de intrusos, assinaturas digitais, dispositivos especiais de internet e protocolos, etc, assumindo que a segurança da informação poderia ser assegurada através da aquisição de soluções tecnológicas. Porém, como já foi referido, esta é uma noção errada pois a gestão da SI "*é mais uma gestão do sistema end-to-end ao invés de apenas instalar soluções tecnológicas*"(DEY, 2007). Como outros sistemas, o ISMS implica a alocação de esforços, mudanças e recursos organizacionais, tais como recursos humanos, políticas, procedimentos, processos, normas e tecnologia.

A aceitação e desenvolvimento de um ISMS não é uma tarefa simples de efectuar, este constitui uma decisão estratégica e é desenvolvido e implementado tendo em consideração as necessidades e objectivos estratégicos da organização. Como tal, é necessário proceder a uma adequada análise e desenho de todo o sistema tendo em consideração os recursos acima mencionados. Começando pelos *stakeholders* da organização, estes devem desempenhar papéis adequados no planeamento e

implementação do ISMS, sendo que todos os colaboradores devem estar envolvidos neste processo, desde os gestores de topo até aos utilizadores finais. É necessário proceder à definição de processos com objectivos de negócio específicos para proteger os recursos da informação. As soluções tecnológicas também necessitam ser implementadas apropriadamente como resposta contra ataques e riscos, ou até mesmo como forma de automatizar determinados processos. É também necessária a definição de políticas e procedimentos que estabeleçam quem irá fazer o quê, quando e como, com o intuito de prevenir ataques, detectá-los caso ocorram e tomar medidas correctivas para corrigir os possíveis danos.

De forma geral, é necessário existir uma mudança cultural na organização na forma como esta olha para a informação e para a SI, uma mudança que deve ser aceite e praticada por todos os *stakeholders* da organização. Na perspectiva da organização é necessário ainda um investimento adicional para a implementação do ISMS, esse investimento está dependente das "*vulnerabilidades, os factores de risco associados ao negócio e ao seu tipo e tamanho*"(DEY, 2007). No entanto, este é um investimento cada vez mais frequente nas organizações, as razões e retornos são muitos, desde logo o ISMS é visto como "*uma oportunidade para inovar as suas operações e melhorar a satisfação do cliente e a confiança do público através do aumento da qualidade do serviço*"(PARK, et al., 2010), porém a certificação e o que isso significa também se torna num factor motivante para as organizações, pois "*ao adoptar linhas orientadoras oficiais, as organizações podem demonstrar o seu compromisso com práticas seguras de negócio; as organizações podem depois solicitar a certificação, credenciação, ou a classificação de maturidade da segurança atestando a sua conformidade com um conjunto de regras e práticas*"(SIPONEN ; WILLISON, 2009).

O ISMS pode ser definido como "*parte do sistema global de gestão, baseado numa determinada abordagem de risco do negócio, através do qual é estabelecida, implementada, analisada, monitorizada e melhorada a segurança da informação. Este sistema inclui estruturas organizacionais, políticas, planeamento de actividades, práticas, processos e recursos*"(MIRELA ; MARIA, 2008).

3.3.1. Normas

Existem diversas normas internacionais que propõem linhas orientadoras para o planeamento e implementação de ISMS, exemplo disso são a TCSEC/*Orange Book*, GMITS, CobiT, IT *Baseline Protection Manual*, *Generally Accepted Information Security Principles* (GAISP), *System Security Engineering* CMM (SSE-CMM), porém as mais usuais são a BS7799 e a sua derivante ISO/IEC 17799:2000, que foi substituída pela ISO/IEC 27001:2005.

Nos pontos seguintes apresentam-se de forma sintética as principais normas que se aplicam neste domínio. Contudo e tendo em consideração que esta dissertação consiste no planeamento e implementação de um ISMS segundo as normas ISO/IEC 27001:2005, ISO/IEC 27003:2010, ISO/IEC 27005:2008 e BS 25999:2007, estas serão alvo de uma apreciação mais profunda nas respectivas secções.

3.3.1.1. TCSEC

A TCSEC (*Trusted Computer System Evaluation Criteria*), frequentemente referida como *Orange Book* é uma norma que foi publicada em 1985 pelo Departamento de Defesa dos Estados Unidos da América e é usada para avaliar, classificar e seleccionar sistemas computacionais que são utilizados para processar, armazenar e recuperar informação sensível ou confidencial. Esta norma está estruturada em 4 classes (D, C, B e A (refere-se ao nível mais elevado de segurança)), sendo que cada divisão representa um nível diferente na confiança que um indivíduo ou organização pode ter no seu sistema. Embora esta norma já esteja ultrapassada teve um impacto significativo na medida em que constituiu um marco inicial na procura e estabelecimento de um conjunto de medidas que permitissem um ambiente computacional ser qualificado como seguro.

3.3.1.2. ISO 13555

A ISO 13555 (GMITS – *Guidelines for the Management of Information Technology Security*) é uma norma publicada em 1996 pela ISO e que descreve um método quantitativo de análise de risco dos recursos da informação com base no

valor/importância do recurso da informação e a probabilidade de ameaças e vulnerabilidades do recurso. Esta norma está estruturada em 5 linhas orientadoras para a gestão da segurança das TIC, cobrindo aspectos como a política, planeamento, avaliação de risco, redução e controlo do risco. Esta norma foi posteriormente actualizada e publicada em 2004, e apesar de manter o mesmo número alterou a sua designação para MTICS (*Management of* TIC *Security*).

3.3.1.3. CobiT

A CobiT (*Control Objectives for* IT), desenvolvido pela ISACA (*Information Systems Audit and Control Association*) e publicado pela primeira vez em 1996 é um guia para a gestão de TIC desenhado para actuar como uma *framework* de controlo que funciona com objectivos de controlo e ferramentas de apoio. Esta norma inclui um sumário executivo, uma *framework*, objectivos de controlo, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gestão. O CobiT é orientado para o negócio na medida em que os seus indicadores chave identificam e medem os resultados dos processos, avaliando o seu desempenho e alinhamento com os objectivos de negócio da organização. A sua estrutura cobre quatro domínios: Planeamento e Organização, constituído por 10 processos; Adquirir e Implementar, composto por 7 processos; Entrega e Suporte, constituído por 13 processos; e por último, Monitorar e Avaliar constitui o último domínio e é composto por 4 processos. Esta norma já vai actualmente na versão 5, cujo ano de publicação está previsto para 2011.

3.3.1.4. IT Baseline Protection Manual

A IT *Baseline Protection Manual* foi elaborada pela *Federal Office for Information Security* da Alemanha em 1994, sendo a sua actualização mais recente de 2005. Esta norma fornece um método para as organizações estabelecerem um ISMS. É composta por recomendações genéricas de segurança das TIC para estabelecer e aplicar o processo de segurança e recomendações técnicas detalhadas para alcançar o nível de segurança da informação necessário num domínio específico. O processo de segurança das TIC proposto por esta norma consiste nos seguintes passos: inicialização do

processo; criação do conceito de segurança de TIC; implementação do planeamento e execução; manutenção, monitorização e melhoria do processo; certificação IT-Grundschutz (opcional). A abordagem desta norma consiste em proporcionar uma *framework* para a gestão da segurança TIC, oferecendo informação sobre os componentes mais comummente utilizados em TIC. Esses componentes ou módulos incluem listas de ameaças relevantes e as contra medidas (a um nível relativamente técnico) necessárias. Ressalve-se que na norma está explícito que apesar de utilizarem o conceito segurança de TIC, segundo os autores porque é um termo comum entre a comunidade científica, na realidade pretendem referir-se a segurança da informação.

3.3.1.5. GAISP

A GAISP (*Generally Accepted Information Security Principles*) foi criada pela ISSA (*Information Systems Security Association*) e publicada em 2004. É uma norma resultante de um consenso sólido e baseada na construção de um processo que é essencial para o sucesso desta abordagem. São desenvolvidos princípios a todos os níveis por profissionais de segurança da informação que compreendem as questões subjacentes às práticas documentadas e à sua aplicação no mundo real. De seguida, esses princípios serão revistos e avaliados por especialistas em segurança da informação e autoridades que irão garantir que cada princípio é: preciso, completo e consistente; compatível com o objectivo especificado; tecnicamente razoável; bem apresentado, gramaticalmente e editorialmente correcto; está em conformidade com as normas e directrizes. O princípio básico da GAISP consiste em três categorias de princípios: princípios universais (ou fundamentais), são 9 princípios básicos baseados no controlo da organização e fornecem linhas orientadoras a nível estratégico (gestão/conselho de administração); princípios gerais funcionais, são cerca de 14 princípios mais detalhados e definem tácticas recomendadas na perspectiva da gestão; e, por último, princípios de segurança detalhados, que descrevem abordagens específicas e detalhadas, escrito para os profissionais de segurança e auditoria e orientado para a segurança operacional e gestão do risco.

3.3.1.6. SSE-CMM

A SSE-CMM (*System Security Engineering Capability Maturity Model*) é um modelo cuja manutenção está a cargo da ISSEA (*International Systems Security Engineering Association*) desde 1999. Este modelo é orientado para os processos usados para atingir a Segurança da Tecnologia de Informação, mais especificamente na maturidade desses processos. É focado nos requisitos para a implementação da segurança num sistema ou conjunto de sistemas relacionados que são do domínio da Segurança da Tecnologia de Informação. Descreve a engenharia dos sistemas de segurança essenciais e a gestão de tarefas que toda a organização necessita realizar. Este modelo tem a intenção de ser usado como: ferramenta para as organizações de engenharia avaliarem as práticas de engenharia de segurança e definirem o melhoramento das mesmas; mecanismos de normalização para os clientes avaliarem a capacidade do fornecedor de engenharia de segurança; base para a avaliação da engenharia de segurança da organização para estabelecer a capacidade de confidências da organização.

3.3.1.7. ISO/IEC 27001

A ISO/IEC 27001 é uma norma reconhecida internacionalmente que apresenta os requisitos de auditoria para um Sistema de Gestão da Segurança da Informação de acordo com a estrutura organizacional, políticas, actividades de planeamento, responsabilidades, práticas, procedimentos, processos e recursos. Define ainda um ISMS como parte do sistema global de gestão, baseado numa abordagem de risco, para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação. Essa abrangência faz com que uma norma ISO/IEC 27001 potencie a interacção entre várias áreas da empresa, tais como: Recursos Humanos, Legal, Auditorias, Instalações, Continuidade de Negócios, Operações, Segurança Física.

Esta norma identifica 5 áreas de controlo, 12 objectivos de controlo e 78 controlos. Cada um é definido como um requisito sujeito a uma auditoria. É importante referir que a implementação de um controlo pode envolver a interacção com outros departamentos e programas mencionados anteriormente. As áreas de controlo da ISO/IEC 27001 estão resumidas a seguir, seguindo a estrutura apresentada pela própria norma (ISO/IEC 27001, 2005):

- *Information Security Management System* – esta área de controlo enfoca a necessidade de estabelecer, implementar, operar, monitorar, rever, manter e melhorar um ISMS bem documentado de acordo com o contexto das suas actividades de negócio e riscos que enfrenta. Todo este processo é gerido segundo o modelo PDCA (*Plan-Do-Check-Act*):
    - Definir e Gerir o ISMS – através da criação e gestão do processo de condução/guia de riscos estabelecendo políticas, objectivos, procedimentos e processos:
        - [*Plan*] Estabelecer o ISMS – através do estabelecimento de políticas, objectivos, processos e procedimentos relevantes para a administração do risco e a melhoria da segurança da informação, para entregar resultados de acordo com a estratégia da organização;
        - [*Do*] Implementação e Operação – através de um conjunto de políticas, controlos, processos e procedimentos;
        - [*Check*] Monitorização e Revisão – medição do desempenho dos processos em comparação com as políticas do ISMS, objectivos e experiências práticas, sendo reportados os resultados à gestão para análise;
        - [*Act*] Manter e Melhorar – tomada de acções preventivas e correctivas baseadas nos resultados das auditorias internas do ISMS e demais informação advindas da gestão ou demais fontes relevantes.
    - Requisitos da documentação do ISMS – onde devem ser criadas evidências/registos das decisões da gestão, assegurando que as acções são rastreáveis para as decisões da gestão e políticas. É importante demonstrar a relação entre os controlos seleccionados, os resultados da avaliação do risco e o processo de tratamento do risco, e posteriormente a política e objectivos do ISMS.
- Responsabilidade da Gestão, esta segunda área de controlo aborda a necessidade de demonstrar claramente as responsabilidades da gestão para com o ISMS, incluindo:

- Compromisso da gestão – devem-se providenciar evidências do compromisso da gestão de topo relativamente ao estabelecimento, implementação, operação, monitorização, revisão, manutenção e melhoria do ISMS;
- Gestão de recursos – a organização deve determinar e providenciar os recursos necessários a todas as actividades do ISMS, inclusive as mencionadas no compromisso da gestão, no suporte dos procedimentos de segurança da informação, no cumprimento dos requisitos legais e regulamentares, etc.

- Auditorias internas, esta área de controlo aborda a necessidade de existir capacidade interna de auditoria ao ISMS, incluindo um procedimento de auditoria documentado que aborda os critérios de auditoria, âmbito, frequência, metodologia e responsabilidades;
- Avaliação da gestão ao ISMS, esta área de controlo aborda a necessidade de proceder à avaliação do ISMS em intervalos planeados com o objectivo de assegurar a continuidade, adequação e eficácia do ISMS. Esta avaliação deve incluir oportunidades de alcançar melhorias e a necessidade de se efectuarem mudanças no ISMS, incluindo alterações na política e objectivos da segurança da informação. Os resultados desta avaliação devem ser devidamente documentados e devem ser mantidos registos, de forma a obter-se evidências de que estas actividades foram efectuadas;
- Melhoria do ISMS, esta última área de controlo aborda a necessidade da organização melhorar a eficácia do ISMS continuamente através do uso da política de segurança da informação, objectivos de SI, resultados das auditorias, análises dos eventos monitorizados, acções preventivas e correctivas e da avaliação da gestão de topo.

3.3.1.8. ISO/IEC 27003

O objectivo da norma ISO/IEC 27003 é proporcionar um guia ao desenvolvimento de um plano de implementação de um ISMS, de acordo com a norma ISO/IEC 27001. Desta forma, esta norma foca os aspectos críticos necessários para o sucesso do desenho e implementação de um ISMS, descrevendo o processo de especificação e desenho do sistema. Nesta norma é ainda descrito o processo para obter

aprovação da gestão para a implementação do ISMS, define o projecto para implementar o ISMS e apresenta-nos um guia sobre como planear um projecto de ISMS, resultando num plano de implementação final do projecto do sistema. Esta norma está estruturada em 5 fases(ISO/IEC 27003, 2010):

- Obter aprovação da gestão para iniciar o projecto do ISMS;
- Definição do âmbito, limites e política do ISMS, nesta fase devem ser definidos detalhadamente o âmbito e limites do ISMS, deve ainda ser definida a política do ISMS, e por último deve ser obtido o aval da gestão;
- Realização da análise dos requisitos de segurança da informação, importante para averiguar qual a situação actual da organização: os requisitos existentes e os recursos de informação que devem ser tidos em conta aquando da implementação do ISMS. As actividades desta fase devem ser realizadas em paralelo com as actividades da fase anterior, por razões de eficiência e praticabilidade. Esta fase tem como objectivo definir os requisitos a serem apoiados pelo ISMS, identificar os recursos de informação, e obter o estado actual da segurança da informação;
- Realização da avaliação do risco e do plano de tratamento de risco, nesta fase deve ser definida a metodologia de avaliação de risco, identificados, analisados e avaliados os riscos de segurança da informação para seleccionar as opções de tratamento de risco, os objectivos de controlo e os controlos. Assim, desta fase deve resultar a escrita de um aviso da aprovação da gestão para a implementação do ISMS, o plano de tratamento de risco e a elaboração de uma Declaração de Aplicabilidade, que inclui os objectivos de controlo e os controlos seleccionados;
- Desenho do ISMS, desta última fase resulta o Plano de implementação do projecto do ISMS. Com base neste plano, o projecto do ISMS pode ser lançado na organização como parte da primeira fase do “DO” (ciclo PDCA). Para ser alcançado este plano final de implementação do ISMS, é necessário desenhar a segurança da organização com base, quer na selecção das opções de tratamento de risco, quer nas exigências relacionadas com o registo de documentos, o desenho dos controlos integrados nas disposições de segurança para as TIC, processos físicos e organizacionais, e o desenho dos requisitos específicos para o ISMS.

3.3.1.9. ISO/IEC 27005

A norma ISO/IEC 27005 contém a descrição do processo e actividades da gestão de risco da segurança da informação. Pretende servir de suporte a alguns conceitos especificados na ISO/IEC 27001 e é estruturada de forma a auxiliar uma implementação satisfatória da segurança da informação baseada numa abordagem de gestão de risco. No entanto, esta norma não apresenta nenhuma metodologia em específico para a gestão de risco da segurança da informação, esta opção fica a cargo de cada organização, pois a escolha da metodologia depende, por exemplo, do âmbito do ISMS, contexto da gestão de risco ou sector industrial da organização(ISO/IEC 27005, 2008):

- Estabelecer o contexto, nesta fase deve ser estabelecido o contexto da gestão de risco da segurança da informação, que inclui a definição do critério básico necessário para a gestão de risco da segurança da informação, definição do âmbito e limites, e o estabelecimento da operação apropriada à organização para a gestão de risco da segurança da informação;
- Avaliação do risco da segurança da informação, nesta fase devem ser identificados os riscos, devem ser descritos quantitativamente ou qualitativamente, e devem ser estabelecidas prioridades nos riscos com base nos critérios da avaliação de risco e nos objectivos relevantes para a organização;
- Tratamento do risco da segurança da informação, devem ser seleccionados controlos para reduzir, reter, evitar ou transferir os riscos e deve ser definido um plano de tratamento de risco. Desta fase deve resultar o plano de tratamento de risco e os riscos residuais sujeitos à aprovação/decisão dos gestores da organização;
- Aceitação do risco da segurança da informação, a decisão de aceitar os riscos e as responsabilidades para a decisão devem ser tomadas e formalmente registadas. Desta fase deve resultar uma lista dos riscos aceitáveis com justificação para os riscos que não correspondem ao normal critério de aceitação de risco da organização;
- Comunicação do risco da segurança da informação, a informação sobre os riscos deve ser disseminada/partilhada entre o responsável pela tomada de decisão e os outros *stakeholders*. O objectivo desta fase é atingir a compreensão contínua dos resultados e processo da gestão de risco da segurança da informação da organização;

- Monitorização e avaliação do risco da segurança da informação, os riscos e os seus factores (valor dos recursos, impacto, ameaças, vulnerabilidades, probabilidade de ocorrência, etc) devem ser monitorizados e avaliados para que se identifiquem quaisquer mudanças ao contexto organizacional em qualquer etapa, mantendo-se assim uma visão geral do risco. Desta forma, o processo de gestão do risco da segurança da informação deve ser monitorizado, avaliado e melhorado continuamente sempre que necessário e apropriado.

3.3.1.10. BS 25999

A norma BS 25999 – Parte 1 apresenta-nos um conjunto de boas práticas a considerar quando se pretende planear e implementar numa organização um sistema BCM (*Business Continuity Management*), ou seja, é uma norma cujo propósito é disponibilizar uma base para compreender, desenvolver e implementar a continuidade de negócio numa organização, independentemente da sua área de negócio e/ou tamanho, proporcionar confiança nas relações da organização com os seus clientes e com outras organizações, e por último, permite à organização medir a sua capacidade de gestão da continuidade de negócio. Esta norma está estruturada em 8 capítulos(BS 25999-1, 2006):

- Resumo da Gestão da Continuidade de Negócio
    - O que é BCM – trata-se de um processo que define uma *framework* operacional e estratégica que:
        - Melhora a resistência da organização contra a ruptura da sua capacidade de atingir os objectivos cruciais;
        - Prevê um método para restaurar a capacidade da organização de produzir os seus bens/serviços centrais para um nível aceitável e num período temporal aceitável;
        - Comprovar a capacidade da organização gerir a ruptura do negócio e assim proteger a sua reputação.
    - BCM e a Estratégia da Organização – a compreensão da BCM na organização assegura que a sua capacidade de atingir os seus objectivos não seja comprometida por interrupções inesperadas. É ainda dado

ênfase à importância dos *stakeholders* para a estratégia da organização e para a compreensão da BCM.

- Relação da BCM com a Gestão do Risco – A BCM e a gestão de risco são complementares. A gestão de risco gere o risco inerente aos bens/serviços centrais da organização. Focando no impacto da interrupção, a BCM identifica esses bens/serviços cruciais para a sobrevivência da organização e define o que é crucial proteger (pessoas, tecnologia, informação, etc) para que a organização reponha o essencial para continuar a cumprir os seus objectivos.
- Porque a organização deve implementar BCM – todas as actividades de negócio estão sujeitas a interrupções, como falhas na tecnologia, inundações, rupturas propositadas, etc. A BCM proporciona a capacidade da organização reagir adequadamente a interrupções operacionais, protegendo o seu bem-estar e segurança. A BCM deve portanto ser encarada não como um custo, mas sim como algo que acrescenta valor à organização.
- Benefícios de um Programa eficaz de BCM – com um programa eficaz de BCM a organização é capaz de:
    - Identificar proactivamente o impacto de interrupções operacionais;
    - Tem uma resposta eficaz às interrupções, o que minimiza o seu impacto;
    - Mantém a capacidade de gerir os riscos;
    - Encoraja o trabalho em equipa;
    - Demonstra uma resposta credível através de um processo de exercício;
    - Pode melhorar a sua reputação;
    - Pode ganhar vantagem competitiva, demonstrando a sua capacidade de manter a produção/prestação de bens/serviços.
- Resultados de um Programa eficaz de BCM:

- Os bens/serviços centrais são identificados e protegidos, assegurando a continuidade do negócio;
- A capacidade de gestão de um incidente proporciona uma resposta eficaz;
- A compreensão da organização sobre si mesma, sobre as outras organizações, reguladores relevantes ou departamentos governamentais, autoridades locais e serviços de emergência são desenvolvidos, documentados e compreendidos apropriadamente;
- O *staff* é treinado, através de exercícios apropriados, para responder eficazmente a um incidente;
- Os requisitos dos *stakeholders* são compreendidos;
- O *staff* recebe suporte e comunicações adequadas no caso de ocorrência de incidentes;
- A cadeia de abastecimento da organização é assegurada;
- A reputação da organização é protegida;
- A organização mantém o seu cumprimento com as obrigações legais e regulamentares.

o Elementos do Ciclo de Vida da BCM – o ciclo de vida da BCM é composto por 6 elementos cruciais:

- Programa de Gestão da BCM – permite definir e manter a continuidade de negócio de forma apropriada ao tamanho e complexidade da organização;
- Compreender a Organização – as actividades previstas nesta etapa fornecem informação sobre a prioridade dos bens/serviços e sobre a urgência das actividades necessárias para os repor. Desta etapa resultam os requisitos que determinarão a selecção apropriada das estratégias BCM;
- Determinar a Estratégia da Continuidade de Negócio – disponibiliza uma série de estratégias para serem avaliadas. Permite escolher uma resposta adequada a cada bem/serviço, de tal forma que possibilite à organização continuar a produzir esses

bens/serviços a um nível operacional aceitável e num período temporal aceitável, durante ou após a ocorrência de uma interrupção;

- Desenvolver e Implementar uma Resposta BCM – resulta na criação de uma *framework* de gestão e numa estrutura de gestão de incidentes, plano de continuidade de negócio e plano de recuperação de negócio, que detalham os passos a seguir durante e após um incidente para manter ou restaurar operações;
- Exercitar, Manter e Rever o Regime BCM – o exercício, manutenção, revisão e auditoria da BCM habilita a organização para:
  - Demonstrar em que medida as estratégias e planos estão completos, actuais e precisos;
  - Identificar oportunidades de melhoria.
- Incorporar a BCM na Cultura da Organização – permite à BCM tornar-se parte dos valores centrais da organização e incutir confiança aos *stakeholders* na capacidade da organização lidar com rupturas.

- Política de Gestão da Continuidade de Negócio – a política BCM define os seguintes processos:
  - As actividades iniciais para estabelecer a capacidade de continuidade de negócio – estas actividades incorporam a especificação, desenho *end-to-end*, construção, implementação e exercício inicial da capacidade de continuidade de negócio;
  - Continuação da manutenção e gestão da capacidade de continuidade de negócio – estas actividades incluem a incorporação da continuidade de negócio na organização, planos regulares de exercício, a sua actualização e comunicação, em particular quando existem mudanças significativas nas suas premissas, pessoal, processo, mercado, estrutura tecnológica ou organizacional;

- Contexto – a organização deve adequar a política BCM à sua natureza, escala, complexidade, geografia e ao grau crítico das suas actividades de negócio. A política BCM define os requisitos do processo que assegura que o regime de continuidade de negócio continua a ir de encontro com as necessidades da organização em caso de ocorrer um incidente. A política deve garantir que a capacidade de continuidade de negócio é promovida na cultura organizacional;
- Desenvolvimento da Política de Continuidade de Negócio – a política estabelece os objectivos da BCM na organização e deve fornecer à organização os princípios documentados através dos quais esta se guiará e medirá a sua capacidade de continuidade de negócio. A política deve ser aprovada pela gestão de topo, regularmente revista e deve considerar os seguintes aspectos:
  - Definição do âmbito da BCM na organização;
  - Recursos da BCM;
  - Definição dos princípios da BCM, orientações e as normas mínimas para a organização;
  - Referências a normas, regulamentos ou políticas relevantes que devem ser incluídas ou podem ser usadas.
- Âmbito do Programa BCM – a gestão de topo pode determinar o âmbito do programa BCM através da identificação dos bens e serviços centrais que apoiam os objectivos da organização, obrigações e atribuições legais. A determinação do que é crucial/central para a organização deve ser consistente com os resultados da análise do impacto de negócio;
- Actividades Externas – a organização deve assegurar que qualquer parceiro externo de um bem, serviço ou actividade tem uma BCM eficaz.

- Gestão do Programa BCM – esta etapa faz parte do núcleo central do processo BCM e estabelece a abordagem da organização à continuidade de negócio. A participação da gestão de topo nesta etapa é crucial para garantir que o processo BCM é devidamente introduzido, suportado de forma adequada e é estabelecido como parte da cultura organizacional. O programa BCM deve ir de encontro com os objectivos definidos na política de continuidade de negócio, envolvendo

três passos: atribuindo responsabilidades; implementando a continuidade de negócio na organização; e a gestão constante da continuidade de negócio.

- Atribuição de Responsabilidades – a gestão da organização deve nomear uma pessoa com autoridade para ser responsável pela política e implementação da BCM. Deve ainda nomear um ou mais colaboradores para implementarem e manterem o programa BCM.
- Implementação da Continuidade de Negócio na Organização – as actividades para a implementação incluem o desenho, construção e implementação do programa. A organização deve: comunicar o programa aos *stakeholders*; organizar ou fornecer treino apropriado ao *staff*; e exercitar a capacidade de continuidade de negócio. A organização pode adoptar um método de gestão de projectos reconhecido para garantir maior eficácia na gestão da implementação.
- Gestão Contínua – as actividades de gestão contínua devem garantir que a continuidade de negócio está incorporada na organização. Cada componente da capacidade de continuidade de negócio, regime ou plano de BC (*Business Continuity*) da organização deve ser regularmente revisto, avaliado e actualizado.
- Manutenção Contínua – independentemente dos recursos que apoiam a BCM, existem algumas actividades que se devem pôr em prática na etapa inicial e na contínua, que podem incluir:
  - Definição do âmbito, regras e responsabilidades para a BCM;
  - Nomear uma pessoa apropriada ou equipa para gerir a continuidade da capacidade BCM;
  - Manter o programa de BCM actual e em prática;
  - Promover a continuidade de negócio na organização;
  - Administrar o programa de exercício;
  - Coordenar a revisão e actualização regular da capacidade de continuidade de negócio, incluindo a revisão ou reformulação da avaliação do risco e da análise de impacto de negócio;

        - Manter a documentação apropriada ao tamanho e complexidade da organização;
        - Monitorar o desempenho da capacidade de continuidade de negócio;
        - Gerir os custos associados à capacidade de continuidade de negócio;
        - Estabelecer e monitorar os regimes de mudança de gestão e sucessão da gestão.
    - Documentação BCM – as pessoas responsáveis pela manutenção da continuidade de negócio devem criar e manter a documentação da continuidade de negócio. Isto pode incluir:
        - Política BCM (declaração do âmbito do BCM e termos de referência do BCM);
        - Análise do Impacto de negócio;
        - Avaliação do risco e ameaça;
        - Estratégia(s) BCM;
        - Programa de sensibilização;
        - Programa de treino;
        - Planos de gestão do incidente;
        - Planos de continuidade de negócio;
        - Planos de recuperação de negócio;
        - Cronograma e relatórios do exercício;
        - Nível de acordos e contratos do serviço.
- Compreender a Organização – este elemento do ciclo de vida da BCM tem como objectivo ajudar à compreensão da organização, através da identificação dos seus bens/serviços centrais, das suas actividades críticas e dos recursos que as apoiam. É através deste elemento que se assegura o alinhamento entre o programa BCM e os objectivos, obrigações e atribuições legais da organização.

No contexto de continuidade de negócio, a compreensão da organização resulta de:

- Identificar os objectivos da organização, obrigações dos *stakeholders*, atribuições legais e o ambiente onde a organização está inserida;
- Identificar as actividades, activos e recursos, incluindo os externos à organização, que suportam a produção dos bens/serviços;
- Avaliar o impacto e consequências ao longo do tempo da falha dessas actividades, activos e recursos;
- Identificar e avaliar as ameaças conhecidas que podem interromper os bens/serviços centrais da organização e as actividades, activos e recursos críticos para o suporte desses mesmos bens/serviços.

É ainda importante que a organização compreenda: a interdependência das suas actividades; confiança que tenha em organizações externas, ou que as organizações externas tenham em si.

- Análise do Impacto de Negócio (BIA[3]) – este processo consiste na tarefa de determinar e documentar o impacto de interrupções nas actividades que suportam os bens/serviços centrais da organização.
- Identificação das Actividades Críticas – a organização deve categorizar as suas actividades de acordo com a sua prioridade de recuperação. As actividades cujo impacto da sua interrupção, segundo a BIA, é maior, devem ser consideradas "actividades críticas", e portanto, deve ser prioritária a sua recuperação.
- Determinar os Requisitos de Continuidade – a organização deve estimar quais os recursos (pessoas, premissas, tecnologia, informação, serviços ou fornecedores externos) necessários para que cada actividade seja reposta.
- Avaliar Ameaças às Actividades Críticas (procedendo a uma análise de risco) – a organização deve estar consciente das ameaças aos recursos (pessoas, premissas, tecnologia, informação, fornecedores), das

[3] BIA – Business Impact Analyze

vulnerabilidades de cada recurso e do impacto que uma ameaça concretizada pode ter em cada recurso.

- Determinar Escolhas – como resultado da análise de impacto de negócio e da avaliação do risco, a organização deve identificar medidas que: reduzam a probabilidade de interrupção, reduzam o período de tempo da interrupção e limitem o seu impacto nos bens/serviços centrais da organização. Estas medidas são conhecidas como redução de perdas e tratamento do risco. As escolhas consistem em:
  - Continuidade de negócio – neste caso deve ser estabelecido um objectivo de tempo de recuperação (RTO[4]) e devem ser avaliadas as estratégias de continuidade definidas na fase seguinte em comparação com este objectivo;
  - Aceitação – o risco pode ser aceite sem que seja necessário proceder a qualquer outra acção;
  - Transferência – para alguns riscos, a melhor resposta pode ser a sua transferência;
  - Alteração, suspensão ou fim – em algumas circunstâncias pode ser mais apropriado alterar, suspender ou terminar o bem, serviço, actividade, função ou processo, isto quando não houver interferência com os objectivos da organização;
  - *Sign-off* – a gestão de topo deve assinar o documento com a listagem dos bens/serviços centrais, a análise de impacto de negócio e a avaliação do risco para garantir que o trabalho foi bem feito e é adequado à organização.

- Determinar a Estratégia de Continuidade de Negócio – como resultado da fase anterior, a organização está agora preparada para escolher estratégias de continuidade apropriadas para atingir os seus objectivos. A abordagem para determinar as estratégias BCM deve: implementar medidas apropriadas para reduzir a probabilidade de ocorrência de incidentes e/ou reduzir o potencial impacto desses incidentes; ter em conta a capacidade das medidas de resistência

[4] RTO – Recovery Time Objective

e atenuação; fornecer continuidade para as actividades críticas durante e a seguir a um incidente; ter em conta as actividades que não foram consideradas críticas.

- Opções Estratégicas – a organização deve considerar opções estratégicas para as suas actividades críticas e para os recursos necessários para o seu recomeço.
- Pessoas – a organização deve seleccionar estratégias adequadas que mantenham as competências centrais e conhecimento. Esta análise deve estender-se a todos os *stakeholders* que possuam grandes capacidades e conhecimento.
- Premissas – a organização deve elaborar uma estratégia para reduzir o impacto da indisponibilidade dos locais de trabalho normais.
- Tecnologia – as estratégias para a tecnologia dependem da sua própria natureza e da sua relação com as actividades críticas.
- Informação – devem assegurar que a informação vital para as operações da organização está protegida e é recuperável, de acordo com os tempos previstos na análise do impacto de negócio.
- Fornecimentos – a organização deve identificar e manter um inventário dos fornecimentos cruciais para o suporte das suas actividades críticas.
- *Stakeholders* – quando são determinadas as estratégias BCM, a organização deve considerar e proteger os seus stakeholders centrais.
- Emergências Civis – as organizações que procurem determinar, implementar ou validar estratégias para a gestão de incidentes e para BCM devem-se tornar familiares com entidades oficiais locais.
- *Sign-off* – a gestão de topo deve assinar os documentos com as estratégias para confirmar que a determinação das estratégias de continuidade foram realizadas apropriadamente e respondem a causas e incidentes prováveis.

- Desenvolvimento e Implementação da Resposta BCM – este elemento do ciclo de vida da BCM preocupa-se com o desenvolvimento e implementação de planos e regimes apropriados para assegurar a continuidade das actividades críticas e a gestão de um incidente.

- Estrutura de Resposta ao Incidente – a organização deve definir uma estrutura de resposta ao incidente que permita dar uma resposta e permita uma recuperação eficaz ao incidente. Essa estrutura de resposta deve possibilitar à organização: confirmar a natureza e extensão do incidente; tomar o controlo da situação; conter o incidente; comunicar com os *stakeholders*.
- Conteúdo dos Planos – todos os planos devem ser concisos e estar disponíveis a todos os elementos que tenham responsabilidades definidas nesses planos. Deve fazer parte do conteúdo dos planos: o seu propósito e âmbito; os papéis e responsabilidades; invocação do plano; responsável pela produção e manutenção do documento; detalhes de contacto.
- Plano de Gestão do Incidente (IMP[5]) – o objectivo deste plano é gerir a fase inicial de um incidente. O IMP deve: ser flexível, viável e relevante; ser fácil de ler e compreender; fornecer as bases para a gestão de todas as questões possíveis, incluindo as questões externas e as relacionadas com os *stakeholders*, que a organização enfrenta no decorrer de um incidente. O IMP deve também: ter o suporte da gestão de topo; ser suportado e ter um orçamento apropriado para o desenvolvimento, manutenção e treino.
- Conteúdos do IMP – para além do conteúdo recomendado no "Conteúdo dos Planos", o IMP deve ainda conter a seguinte informação: listas das tarefas e acções, para gerir as consequências imediatas da interrupção do negócio; contactos de emergência; actividades das pessoas, com uma descrição sobre quem está responsável por quê; resposta aos media; gestão dos *stakeholders*, deve existir um processo para identificar e criar prioridades nas comunicações com os *stakeholders*; local da gestão do incidente, deve existir um local pré-seleccionado onde o pessoal se deve reunir em caso de incidente para dar resposta ao mesmo.
- Plano(s) de Continuidade de Negócio (BCP[6]) – o objectivo deste plano é possibilitar à organização recuperar ou manter as actividades após a ocorrência de um incidente para o seu estado normal. O(s) BCP é

[5] IMP – Incident Management Plan
[6] BCP – Business Continuity Plan

activado para dar suporte às actividades críticas necessárias para que a organização continue a alcançar os seus objectivos.

- Conteúdos de BCP – para além do recomendado em "Conteúdo dos Planos", o BCP deve ainda conter: planos de acção e listas de tarefas, ordenadas por prioridade; requisitos dos recursos, necessários para a continuidade do negócio e para a recuperação do negócio; pessoa(s) responsável, pelas etapas da gestão da continuidade do negócio e recuperação de negócio após a ocorrência de um incidente; formulários e anexos.

- Avaliar, Manter e Rever o regime da BCM[7] – este elemento do ciclo de vida da BCM pretende assegurar que o regime da BCM é validado através da sua avaliação e revisão e que está actualizado. Os regimes de continuidade de negócio da organização e gestão do incidente não podem ser considerados confiáveis até serem testados. A avaliação/teste é crucial para desenvolver o trabalho de equipa, competência, confiança e conhecimento, condições vitais no momento do incidente.

  - Programa de Avaliação/Teste – deve ser consistente com o âmbito do plano(s) de continuidade de negócio e deve ter em consideração legislação e regulamentos relevantes. O programa deve: testar os sistemas técnico, logístico, administrativo, processual e operacional do BCP; testar o regime e infra-estrutura BCM, incluindo papéis, responsabilidades, locais de gestão do incidente, zonas de trabalho, etc; validar a recuperação da tecnologia e telecomunicações, incluindo a disponibilidade e deslocalização do *staff*.

  - Avaliar/Testar o Regime BCM – os testes devem ser realistas, cuidadosamente planeados e aceites pelos *stakeholders*, para que exista um risco mínimo de ruptura com os processos de negócio. Cada teste deve ter especificado claramente os seus objectivos, a escala e complexidade dos testes deve ser proporcional aos objectivos de recuperação da organização, os planos de continuidade de negócio e gestão do incidente devem ser testados para assegurar que estes podem ser executados correctamente e contêm detalhes e instruções apropriadas.

[7] BCM – Business Continuity Management

- Manutenção do regime BCM – deve ser definido e documentado um programa de manutenção da BCM. Este programa deve assegurar que todas as mudanças (internas ou externas) que tenham impacto na organização sejam revistas tendo em conta a BCM. Devem ainda ser identificados, caso existam, novos bens/serviços e as actividades dependentes destes e devem ser incluídos no programa de manutenção da BCM.
- Revisão do regime BCM – a gestão de topo da organização deve rever, em intervalos adequados, a capacidade da BCM da organização para assegurar a sua contínua adequação e eficácia e deve documentar essa revisão. A revisão deve verificar que o cumprimento da política BCM da organização vai de encontro com o cumprimento de leis aplicáveis, normas, estratégias, *frameworks* e boas práticas. A revisão pode ser efectuada por auditoria interna ou externa, ou auto-avaliação.

- Incorporar a BCM na Cultura Organizacional – para que seja bem sucedida, a BCM deve ser parte integrante da cultura da organização. Construindo, promovendo e incorporando a cultura BCM na organização assegura que esta se torne parte dos valores centrais da organização e seja gerida eficazmente. Uma organização com uma cultura BCM positiva irá: desenvolver o programa BCM mais eficazmente; incutir confiança aos seus *stakeholders* na sua habilidade para lidar com as interrupções no negócio; aumentar a sua resistência ao longo do tempo ao assegurar que as implicações BCM são consideradas nas decisões da gestão de topo; e minimizar a probabilidade e impacto das interrupções.
  - Sensibilização – a organização deve ter um processo para identificar e disseminar os requisitos de sensibilização da BCM na organização e avaliar a eficácia da sua disseminação. A organização deve aumentar, melhorar e manter a consciência através da manutenção contínua do programa de educação e informação BCM para todo o *staff*. Este programa deve incluir: um processo de consulta com o pessoal em toda a organização sobre a implementação do programa BCM; discussão sobre a BCM nas *newsletters* ou revistas da organização; inclusão da BCM em sítios Web ou intranets relevantes; aprendizagem através de incidentes internos e externos; encarar o BCM como um objectivo a cumprir pela

equipa de trabalho; testar os planos de continuidade de negócio em localizações alternativas; visitas às localizações alternativas.

- Avaliação das Competências – a organização deve ter um processo para identificar e disseminar os requisitos de avaliação da BCM aos participantes relevantes e para avaliar a eficácia da disseminação. A organização deve realizar testes no: *staff* BCM, para tarefas como a gestão do programa BCM, realização das análises do impacto do negócio, desenvolvimento e implementação de BCPs, execução de programas de avaliação/teste de BCP, avaliação do risco e ameaças, comunicações *media*; *staff* não pertencente à BCM que requerem competências para desempenhar os seus papéis na resposta ao incidente ou na recuperação do negócio.

Por último, a norma BS 25999-Parte 2 especifica os requisitos necessários para a criação de um sistema de gestão da continuidade de negócio eficaz. Estes requisitos são necessários para o planeamento, implementação, operação, monitorização, avaliação, manutenção e melhoramento de um BCMS (*Business Continuity Management System*) documentado num contexto de gestão dos riscos globais da organização. A estruturação desta norma é feita seguindo o ciclo PDCA (*Plan-Do-Check-Act*)(BS 25999-2, 2007):

- [*Plan*] Planeamento do Sistema de Gestão da Continuidade de Negócio – esta primeira fase tem como propósito a definição dos limites do BCMS, assegurar que os objectivos são claramente especificados, entendidos e comunicados, demonstrado o compromisso dos gestores de topo com o BCMS, os recursos são distribuídos e garantir que os responsáveis pela BCM (*Business Continuity Management*) têm competências para desempenhar os seus papéis;
- [*Do*] Implementação e Operação do BCMS – a organização deve identificar as actividades críticas e os recursos necessários ao suporte dos seus produtos e serviços centrais/essenciais, compreender as ameaças que lhes estão inerentes e escolher tratamentos de risco apropriados;
- [*Check*] Monitorização e Avaliação do BCMS – assegurar que a gestão monitoriza e avalia a eficácia e eficiência do BCMS, avaliar a adequação da política, objectivos e âmbito da continuidade de negócio, determinar e autorizar acções para a recuperação e melhoria;

- [*Act*] Manutenção e Melhoria do BCMS – manter e melhorar continuamente a eficácia e eficiência do BCMS através de acções preventivas e correctivas, de acordo com o determinado na avaliação da gestão.

4. O Caso de Estudo

Neste capítulo será desenvolvido o caso de estudo, ou seja, será retratado o objecto de investigação desta dissertação. O objectivo primordial é o de planear e implementar um sistema de gestão da segurança da informação na empresa MULTICERT, de acordo com os parâmetros definidos na norma ISO/IEC 27001, integrando o ISMS com o BCM (*Business Continuity Management*). Mais ainda, pretende-se com esta investigação perceber "Qual o contributo da certificação de um Sistema de Gestão da Segurança da Informação para a credibilidade de uma organização".

Inicialmente estava previsto que pudesse acompanhar todo o processo de planeamento, implementação, manutenção e melhoria do ISMS, bem como a implementação do sistema de continuidade do negócio. No entanto, devido aos limites impostos pelo tempo, não foi possível ainda tratar o pedido de certificação à entidade certificadora ISO. Porém, isso não porá em causa o objectivo final desta dissertação, nem a obtenção da resposta à questão de investigação formulada.

Dito isto, neste capítulo será apresentada uma contextualização da organização envolvida neste processo de dissertação – a MULTICERT – e o projecto estratégico no qual esta está envolvida e sobre o qual será implementado o ISMS. Este capítulo termina com a exposição de todos os elementos do ISMS desenvolvidos na empresa acolhedora.

4.1. Contexto Organizacional: MULTICERT e o projecto estratégico TSL-EPC

A MULTICERT, Serviços de Certificação Electrónica, S.A. iniciou a sua actividade em 2002, sendo o seu corpo de accionistas composto pelas empresas SIBS (Sociedade Interbancária de Serviços, S.A.), CTT (Correios de Portugal, S.A.), INCM (Imprensa Nacional – Casa da Moeda, S.A.), PT-Prime (Soluções Empresariais de Telecomunicações e Sistemas, S.A.) e PT SGPS (Portugal Telecom SGPS, S.A.).

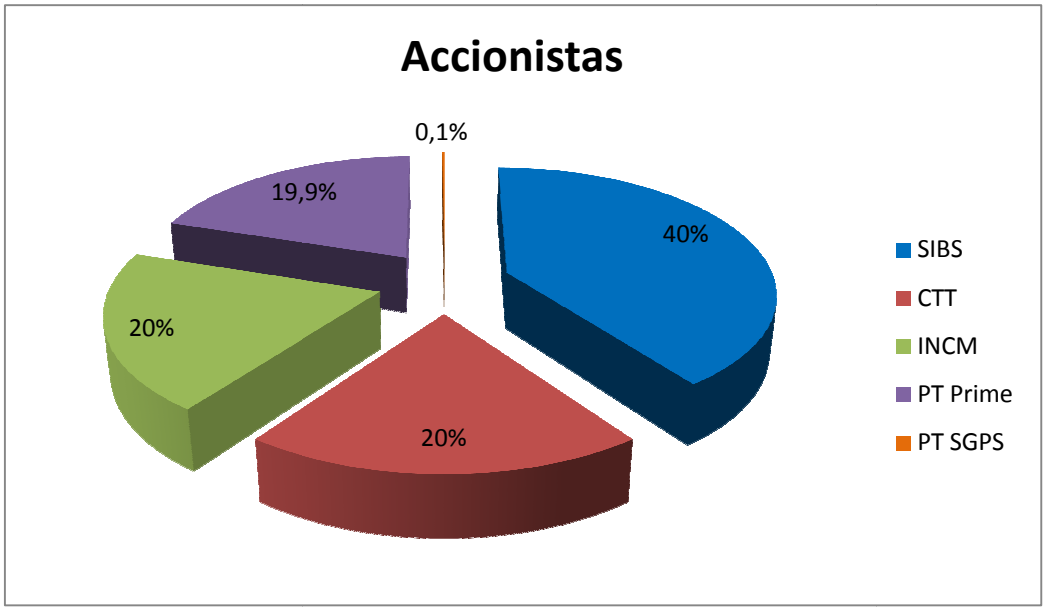

Figura 8 – Estrutura Accionista da MULTICERT

Esta empresa posiciona-se no mercado como fornecedor de soluções completas de segurança e/ou certificação digital para todo o tipo de transacções electrónicas que exigem segurança (*e-commerce*, *e-banking*, *e-government*, e-mail, etc). Actualmente, a MULTICERT desenvolve a sua actividade nas seguintes áreas de negócio: documentos de identificação seguros, certificados digitais, factura electrónica, gestão documental, transacções seguras, API`s (*Application Programming Interface*), e recentemente as TSL`s (*Trust Service Status List*), sobre a qual será implementado o ISMS.

Esta empresa de soluções tecnológicas e serviços de certificação electrónica tem a missão de participar activamente no desenvolvimento da Sociedade da Informação e na Economia Digital, tendo como objectivos: desenvolver soluções completas de segurança e certificação digital; apostar nos sectores de actividade que exigem segurança nas suas transacções electrónicas; apostar na aquisição de novos projectos; apostar no aumento de negócio em áreas que permitam gerar/obter receitas recorrentes; fornecer e desenvolver serviços e produtos inovadores; manter a vanguarda na área de actividade; criar parcerias com universidades e laboratórios de investigação, com o intuito de "Investigar para Inovar"; ser a entidade de certificação electrónica de referência que dinamize o desenvolvimento da Economia Digital no país; afirmar-se como empresa de desenvolvimento de projectos e soluções em segurança digital; fornecer serviços de cobertura nacional e visão internacional em termos geográficos e

sectoriais; e internacionalizar para potenciar o crescimento da empresa, tendo por base a sua experiência e *know-how* dos seus recursos humanos (MULTICERT, 2010c).

Em 2004 a equipa da MULTICERT era constituída por 16 colaboradores, ao passo que em 2009 registava já um aumento dos seus recursos humanos contabilizando 43 colaboradores. Actualmente, a orgânica desta empresa está estruturada da seguinte forma(MULTICERT, 2010a):

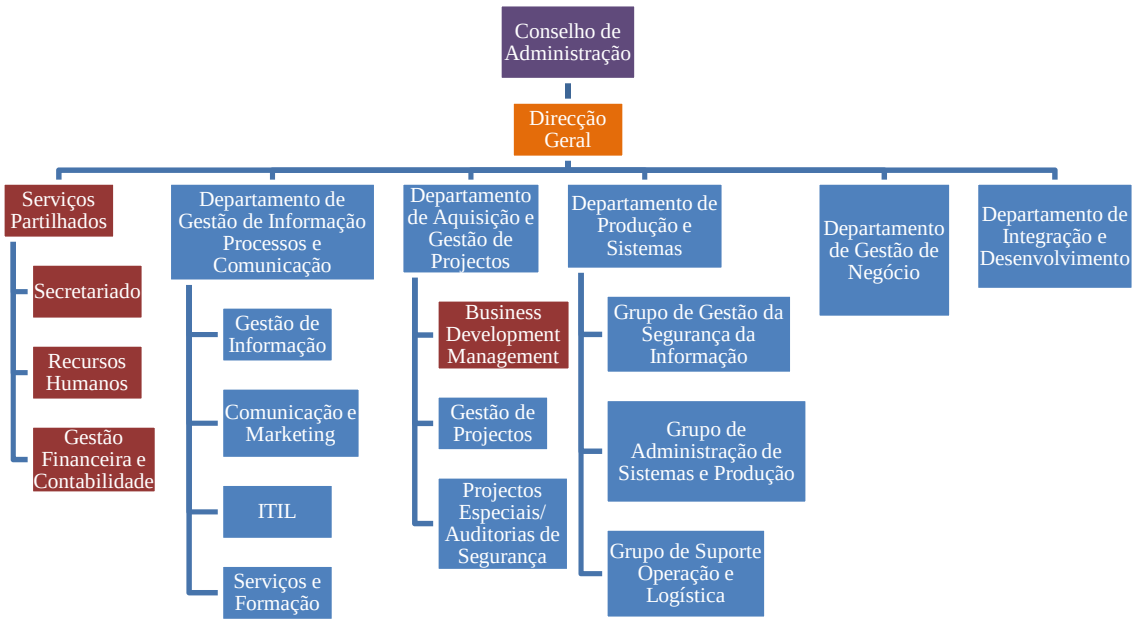

Figura 9 – Estrutura orgânico-funcional da MULTICERT

Actualmente, a MULTICERT desenvolve e executa vários projectos em segurança digital, a nível nacional e internacional, podendo-se destacar (MULTICERT, 2010d): o Cartão do Cidadão; Passaporte Electrónico Português e a Segunda Geração do Passaporte Electrónico Português; Título de Residência Português; STORK (*Secure Identity Across Borders Linked*); *E-Mandate Standards Development*; Voto Electrónico – Piloto de Legislativas UMIC; Voto Electrónico – Piloto de Eleições Europeias; Marca do Dia Electrónica (MDDE); Serviço de Autenticação Forte EMV/CAP SIBS; *HomeBanking* IGCP; Serviço de Factura Electrónica e4doc Grupo PT; e muito recentemente a TSL.

O ISMS desenvolvido no contexto desta dissertação terá inicialmente como âmbito de protecção as TSL`s, sendo que este serviço será gerido e operado pela

MULTICERT para o EPC (*European Payments Council*). Neste sentido, serão apresentados alguns conceitos que nos permitem uma elucidação mais clara sobre este projecto.

Antes de mais, impõe-se desde já apresentar o conceito de SEPA (*Single Euro Payments Area*), que pode ser definido como a área dentro da Europa onde os cidadãos, empresas e outros agentes económicos podem fazer e receber pagamentos (em euros), seja dentro ou fora das respectivas fronteiras geográficas sob as mesmas condições, direitos e obrigações, independentemente da sua localização. A abrangência geográfica da SEPA abrange os 27 estados membros da EU (*European Union*), Islândia, Liechtenstein, Noruega; Suíça e Mónaco.

Por sua vez, o EPC, cliente da MULTICERT, desenvolve esquemas e *frameworks* de pagamento necessárias para realizar a SEPA. Este Conselho define posições comuns para o espaço corporativo dos serviços de pagamento, prevê linhas orientadoras para a uniformização, formula regras, boas práticas e normas e apoia e fiscaliza a execução das decisões tomadas. O EPC é constituído por 74 membros representantes de Bancos, Comunidades de Bancos e Instituições de Pagamento.

Antes de prosseguimos com esta explanação impõe-se definir o conceito de SDD *Core Scheme* (SEPA *Core Direct Debit Scheme*), que como qualquer outro sistema de débito directo é baseado no princípio de que determinada pessoa/entidade (credor) pede dinheiro a outra pessoa/entidade (devedor), com a sua aprovação prévia, e credita esse dinheiro na sua conta, ou seja, este esquema permite a um credor recolher fundos da conta do devedor, desde que o devedor tenha assinado um mandato (*e-Mandate*) que permite esta acção ao credor.

O *e-Mandate* é um projecto desenvolvido pela MULTICERT e promovido pelo EPC, que tem como objectivo a definição de um modelo de operação e implementação para um serviço de autorizações de débitos directos a funcionar no ambiente SEPA. A MULTICERT, contratada para assessoria especializada pela SIBS, teve a seu cargo a especificação do modelo de funcionamento e os requisitos de implementação a adoptar pelos Bancos europeus aderentes, credores, fornecedores de serviços de encaminhamento, fornecedores de serviços bancários de directoria e Entidades de Certificação. Foi dedicada especial atenção a aspectos como interoperabilidade, não-repúdio, autenticação, integridade e confidencialidade. O modelo proposto pela

MULTICERT foi objecto de um rigoroso processo de avaliação de risco de acordo com o conjunto de normas ISO/IEC 27000.

Feita esta contextualização estão agora criadas as condições para abordarmos este novo serviço TPC (Terceira Parte de Confiança), o projecto TSL desenvolvido pela MULTICERT e comercializado, inicialmente, ao EPC. De uma forma geral, as TSL`s são listas de CA`s (*Certification Authority*) consideradas confiáveis pelo EPC. No documento "*e-Mandates e-Operating Model: High Level Definition*" podemos ver o propósito/necessidade da existência das TSL`s aplicadas a este serviço: "A mútua autenticação entre o *Routing Service* e o *Validation Service* é conseguida através da utilização de certificados emitidos pelas Entidades de Certificação Aprovadas pelo EPC" (EUROPEAN PAYMENTS COUNCIL, 2009). Tendo esta descrição em consideração podemos, sucintamente, concluir que a finalidade das TSL`s é a de prover uma lista de CA`s consideradas confiáveis pelo EPC, através das quais se podem adquirir certificados que serão utilizados para fazer a autenticação entre o *Routing Service* (organizações prestadoras de actividades auxiliares de serviços financeiros) e o *Validation Service* (Bancos), de forma segura.

4.2.Descrição e Objectivos

O valor dos recursos associados à informação de uma organização é incalculável, e portanto as organizações sentem cada vez mais a necessidade de protegerem e gerirem adequadamente estes recursos, de forma a controlarem e minimizarem o risco de esta ser violada no que concerne à sua confidencialidade, autenticidade, integridade, não-repúdio e disponibilidade. Este projecto tem como objectivo a implementação dos requisitos exigidos pelas normas internacionais com vista à implementação de um ISMS eficaz num projecto Europeu onde a informação é tratada com rigor. Devido à dimensão do trabalho em causa, os objectivos para esta dissertação culminam na fase de implementação do Plano de Tratamento do Risco.

O projecto de planeamento e implementação do ISMS na MULTICERT é um projecto transversal a toda a organização, no entanto é desenvolvido pelo Grupo de Gestão da Segurança da Informação, pertencente ao Departamento de Produção e Sistemas.

O âmbito do ISMS será a implementação e operação de TSL`s, promovido pelo EPC, com o objectivo de, num ambiente lógico e físico, seguro, fazer a gestão das CA`s confiáveis do EPC para utilização do serviço SEPA *e-Mandates*, que por sua vez consiste na definição de um modelo de operação e implementação para um serviço de autorização de débitos directos no ambiente SEPA.

Pretende-se assim neste contexto atingir os seguintes objectivos:

- Investigar as normas de segurança aplicáveis à Segurança da Informação, nomeadamente a ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27005 e BS 25999;
- Identificar os objectivos de controlo e os controlos necessários, em funcionamento e a implementar;
- Definir e elaborar a documentação necessária à implementação do ISMS para o âmbito definido;
- Realizar a Análise do Risco e preparar o Plano de Tratamento do Risco.

4.3. Actividades e Cronograma

Este projecto organizou-se em duas fases. A primeira fase foi desenvolvida desde Outubro até Dezembro e consistiu na pesquisa bibliográfica sobre a temática a ser explorada e na elaboração do respectivo Estado da Arte aqui exposto no capítulo 3. Tanto a pesquisa bibliográfica como o Estado da Arte foram desenvolvidos sobre o grande chapéu da Segurança da Informação, afunilando posteriormente a visão para a questão da Gestão da Segurança da Informação e do ISMS, tendo sempre como corte da realidade e como orientação para a visão e abordagem a Ciência da Informação.

A segunda fase foi desenvolvida de Janeiro a Junho e consistiu no planeamento e implementação práticos do ISMS em contexto organizacional, e consistiu nas seguintes actividades:

1ª Compromisso da Gestão de Topo;
2ª Definição do Âmbito de Protecção;
3ª Inventário de Recursos de Informação;
4ª Definir Metodologia para a Gestão do Risco;
5ª Realizar uma Análise do Risco;

6ª Preparar o "SoA[8] – *Statement of Applicability*";

7ª Preparar o Plano de Tratamento do Risco.

	Task Name	Duration	Start	Finish
1	Pesquisa Bibliográfica	21 days	Fri 01-10-10	Fri 29-10-10
2	Estado da Arte	35 days	Mon 01-11-10	Fri 17-12-10
3	Compromisso da Gestão de Topo	34 days	Tue 04-01-11	Fri 18-02-11
4	Definição do Âmbito de Protecção	40 days	Mon 21-02-11	Fri 15-04-11
5	Inventário de Recursos	6 days	Mon 18-04-11	Mon 25-04-11
6	Metodologia de Gestão do Risco	4 days	Tue 26-04-11	Fri 29-04-11
7	Análise do Risco	25 days	Mon 02-05-11	Fri 03-06-11
8	Declaração de Aplicabilidade	10 days	Mon 06-06-11	Fri 17-06-11
9	Plano de Tratamento do Risco	9 days	Mon 20-06-11	Thu 30-06-11

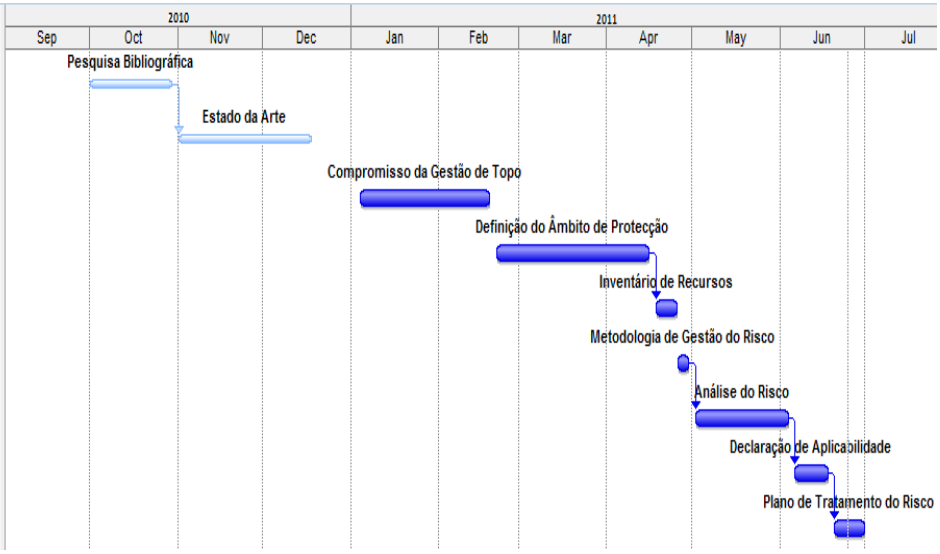

Figura 10 - Cronograma de Actividades

A primeira actividade – Compromisso da Gestão de Topo – consistiu num conjunto de etapas que se materializaram no seguinte:

1. Reunião do Director Geral com a Gestão de Topo (Conselho de Administração) para definição de linhas orientadoras para o âmbito de protecção, o projecto estratégico da empresa e a estrutura orgânica de segurança;
2. Acta formal da empresa identificando o projecto estratégico e nomeando a orgânica de segurança;
3. Definição da Política de Segurança da Informação (de topo), proposta pelo *Sponsor* e CISO (*Chief Information Security Office*);
4. Reunião formal do *Security Forum* para aprovação dos primeiros documentos que constituem o ISMS.

Por sua vez, a segunda actividade – Definição do Âmbito de Protecção – consistiu na definição do âmbito, limites e fronteiras dos processos, actividades e recursos que fazem parte do ISMS, bem como os processos, actividades e recursos que fazem parte dos processos de gestão para suporte ao ISMS.

A terceira actividade, já de certa forma facilitada pela actividade anterior, consistiu na elaboração de um inventário dos recursos de informação necessários à realização dos processos que fazem parte do âmbito de protecção.

[8] Em português, Declaração de Aplicabilidade.

Na quarta actividade foi definida a metodologia a utilizar para a gestão do risco. A quinta actividade está em muito relacionada com a anterior, visto que é neste momento que se procede à Análise do Risco, que de forma muito sucinta consiste na identificação de riscos associados aos recursos de informação.

Em penúltimo, foi preparado o documento SoA (*Statment of Applicability*) onde constam os objectivos de controlo e os controlos aplicados e/ou a aplicar, com respectiva justificação para os objectivos de controlo e/ou controlos excluídos.

Por último, foi preparado o Plano de Tratamento do Risco, onde constam as acções de tratamento do risco e onde são tomadas decisões sobre evitar, transferir, mitigar ou aceitar o risco.

4.4.Método e Normas utilizadas

Cabe neste subcapítulo descrever as técnicas de recolha de informação e normas utilizadas no decorrer desta dissertação. Neste sentido, são, na primeira secção, descritas as estratégias de pesquisa utilizadas essencialmente para obter a informação necessária à realização da primeira fase desta dissertação, que consiste na pesquisa bibliográfica e elaboração do estado da arte. Ainda nesta secção são descritas as técnicas de recolha de informação, utilizadas fundamentalmente para a realização da segunda fase desta dissertação, a decorrer em ambiente empresarial.

Na segunda secção deste subcapítulo são abordadas as normas utilizadas para a realização desta dissertação, que consistiram nas seguintes: ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27005, e BS 25999.

4.4.1. Recolha de Informação

Nesta secção pretende-se explanar, por um lado as estratégias de pesquisa delineadas para a elaboração desta dissertação, e por outro lado as técnicas de recolha de informação, dados e evidências utilizadas neste âmbito. Antes de avançarmos, impõe-se situarmo-nos no método científico anteriormente referido – o método quadripolar. Neste momento estamos situados no pólo técnico, onde são definidas as

estratégias de pesquisa e técnicas de recolha de informação. Segundo (MARTINS ; THEÓPHILO, 2007), este pólo é abordado sob duas perspectivas: as estratégias de pesquisa e as técnicas de recolha de informação, dados e evidências.

Entende-se por estratégias de pesquisa as diferentes maneiras de recolher e analisar dados empíricos no contexto das ciências sociais aplicadas, ou seja, são estratégias (delineamentos, planeamentos) que permitem conduzir as pesquisas científicas cujos objectos de estudo e objectivos de estudo se adequam a estas. Assim sendo, neste contexto foram utilizadas as seguintes estratégias de pesquisa (MARTINS ; THEÓPHILO, 2007):

- Pesquisa bibliográfica – pesquisa que procura explicar e discutir um assunto, tema ou problema com base em referências publicadas em livros, periódicos, revistas, enciclopédias, dicionários, jornais, *sites*, artigos de congressos, etc. Este tipo de pesquisa permite obter uma análise teórica sobre a problemática a estudar. Neste sentido foram elaboradas inúmeras expressões de pesquisa essencialmente nas bases de dados e nos livros existentes na biblioteca da FEUP;
- Pesquisa documental – pesquisa de documentos dos mais variados tipos, escritos ou não, tais como diários, documentos arquivados em organizações, etc. A diferença fundamental entre a pesquisa bibliográfica e a pesquisa documental é que a pesquisa documental baseia-se em documentos que não foram publicados, neste caso, baseou-se na pesquisa de documentos arquivados na organização onde foi desenvolvida esta dissertação;
- Estudo de caso – este tipo de pesquisa é orientado para a vertente qualitativa, uma vez que o seu objectivo é o estudo de uma unidade social que se analisa profunda e intrinsecamente. Trata-se de uma investigação empírica que pesquisa fenómenos dentro do seu contexto real (pesquisa naturalística), onde o investigador não tem controlo sobre eventos e variáveis, procurando apreender a totalidade de uma situação e, criativamente, descrever, compreender e interpretar a complexidade de um caso concreto. Neste contexto, o estudo de caso desencadeou-se tendo como pano de fundo a organização MULTICERT e a implementação prática do ISMS neste contexto organizacional.

As estratégias de pesquisa aqui referidas foram utilizadas concomitantemente, de forma a possibilitar a obtenção dos resultados mais completos e abrangentes da problemática proposta no âmbito desta dissertação.

Por sua vez, as técnicas de recolha de informação, dados e evidências relacionam-se a escolhas de técnicas para a recolha necessária ao desenvolvimento e conclusões da pesquisa. Reforçando a distinção entre as duas perspectivas aqui abordadas, as estratégias de pesquisa consistem em delineamentos (planeamentos) para uma pesquisa, enquanto as opções de técnicas de recolha de informação, dados e evidências podem ser avaliadas aquando da condução de uma pesquisa científica.

Relativamente às técnicas de recolha de informação, dados e evidências utilizadas, importa antes de mais referir a distinção entre dados primários e secundários. Entende-se por dados primários aqueles que são recolhidos directamente da fonte, neste caso os recolhidos da organização MULTICERT, por outro lado os dados secundários consistem em dados já recolhidos por outrem e organizados em arquivos e/ou bases de dados, relatórios, etc. Feita esta achega, foram utilizadas as seguintes técnicas de pesquisa (MARTINS ; THEÓPHILO, 2007):

- Observação participante – o pesquisador/observador torna-se parte integrante de uma estrutura social, e na relação face a face com os sujeitos da pesquisa realiza a recolha de informação. Neste sentido, o observador não olha apenas a realidade como um mero sujeito passivo, antes pelo contrário este é parte integrante/participante da realidade que pretende observar/estudar;
- Pesquisa documental – como já foi referido, assemelha-se à pesquisa bibliográfica, todavia utiliza informação que não é publicada, normalmente consiste em pesquisa sobre documentos de uma determinada entidade.

4.4.2. Normas ISO/IEC 27001, 27003, 27005 e BS 25999

Um dos objectivos propostos no âmbito desta dissertação era a análise de algumas normas internacionais de Segurança da Informação, que seriam aplicadas no ISMS da MULTICERT, nomeadamente a ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27005 e BS 25999.

Conforme se descreve de forma detalhada no capítulo “3. Estado da Arte” a ISO/IEC 27001 é a norma que permite obter a credenciação, ou seja, é nesta norma que estão definidos os requisitos para implementar o ISMS. Esta norma consiste assim num conjunto de especificações para estabelecer, implementar, monitorizar e rever, manter e melhorar o sistema de gestão da segurança da informação. Desta forma, a base de orientação para a implementação do ISMS na MULTICERT é esta norma.

No entanto, a ISO/IEC 27001 é uma norma bastante complexa, e por conseguinte necessita de ser complementada para que a sua aplicação seja mais eficaz. Neste sentido, a ISO/IEC 27003 desempenha um papel crucial na medida em que fornece um guia mais detalhado sobre a implementação do ISMS. Assim, a ISO/IEC 27003 descreve o processo de especificação e desenho do ISMS desde a concepção até à produção de planos de implementação do projecto, abrangendo as actividades de preparação e planeamento antes da verdadeira implementação. Esta norma detalha ainda aspectos chave que estão pouco detalhados na ISO/IEC 27001.

O grande foco na abordagem do ISMS é o risco inerente à informação e aos seus recursos. Por isso, foi elaborada a ISO/IEC 27005 que dá especial relevância ao risco, fornecendo um conjunto de linhas orientadoras para a gestão do risco da segurança da informação. Esta norma é baseada nos conceitos especificados na ISO/IEC 27001 e foi concebida para auxiliar uma implementação satisfatória da segurança da informação baseada numa abordagem de gestão do risco.

Por último, e embora não tendo sido aplicada na prática, foi também analisada a norma BS 25999, que consiste na etapa final e complementar ao ISMS – a Gestão da Continuidade de Negócio. A análise desta última norma teve duas etapas: a primeira consistiu na análise da BS 25999 – Parte 1, que consiste num código de boas práticas, fornecendo linhas orientadoras para estabelecer processos, princípios e terminologia sobre a Gestão da Continuidade de Negócio; a segunda etapa consistiu na análise da BS 25999 – Parte 2, que especifica os requisitos para a implementação, operação e melhoria de um Sistema de Gestão da Continuidade de Negócio bem documentado, onde são descritos requisitos que podem ser objectiva e independentemente auditados.

4.5.O Sistema de Gestão da Segurança da Informação

Neste subcapítulo abordaram-se de forma teórica as fases de implementação do ISMS que foram estudadas durante o decorrer desta dissertação. Assim sendo, será desde logo apresentado o método PDCA e as fases do ISMS pertencentes a cada uma das etapas do método, sendo de seguida apresentados os aspectos de cariz teórico que foram implementados: compromisso da gestão de topo; âmbito de protecção, com respectivos processos, actividades e recursos; políticas do ISMS; a abordagem BPM estendida aos processos do ISMS; processos de gestão para suporte; gestão da documentação, englobando a classificação da informação; declaração de aplicabilidade; análise e tratamento do risco; e por último a gestão de incidentes.

4.5.1. Modelo PDCA

Todo o processo de planeamento e implementação do ISMS é desenvolvido tendo como orientação o cumprimento dos requisitos estipulados na norma ISO/IEC 27001, que por sua vez aplica o método cíclico PDCA (*Plan-Do-Check-Act*) em todos os seus processos, como método que permite conseguir uma melhoria e aperfeiçoamento contínuo do sistema, garantindo assim que este se adequa e responde à constante mudança das necessidades organizacionais. Este método permite ainda que o ISMS respeite os nove princípios estabelecidos pela OECD: sensibilização, responsabilidade, resposta, ética, democracia, avaliação do risco, desenho e implementação da segurança, gestão da segurança e por último revisão/reavaliação(OECD, 2002).

O [*Plan*] (estabelecimento do ISMS) consiste, não só na primeira fase do método PDCA, mas também na primeira fase do ISMS proposto pela ISO/IEC 27001. Nesta primeira fase é estabelecida a política do ISMS, objectivos, processos e procedimentos relevantes para gerir o risco e melhorar a segurança da informação. Assim sendo, nesta fase procede-se, desde logo à obtenção do compromisso da gestão de topo para com o ISMS, seguindo-se a definição do âmbito de protecção do ISMS, a política de segurança da informação, a metodologia de avaliação do risco, identificação dos riscos, análise e avaliação dos riscos, identificação e avaliação de opções para o tratamento do risco, selecção dos objectivos de controlo e controlos para o tratamento do risco, obtenção da

aprovação da gestão de topo para os riscos residuais propostos, e culmina com a elaboração do SoA (*Statment of Applicability*).

O [*Do*] (implementação e operação do ISMS) consiste na implementação e operação da política de segurança da informação, controlos, processos, e procedimentos. Nesta fase procede-se à formulação do Plano de Tratamento do Risco, seguindo-se a implementação do mesmo, implementação dos controlos anteriormente seleccionados, definição do método de avaliação da eficácia dos controlos seleccionados, implementação de programas de treino e sensibilização, gestão da operação do ISMS, gestão dos recursos do sistema, e por último implementação de procedimentos e outros controlos capazes de detectar de forma imediata eventos de segurança e fornecer respostas a incidentes de segurança.

Relativamente à fase [*Check*] (monitorização e avaliação do ISMS), a organização deverá executar procedimentos de monitorização e avaliação, realizar avaliações regulares sobre a eficácia do ISMS, medir a eficácia dos controlos para verificar se os requisitos de segurança estão a ser cumpridos, rever as avaliações do risco em determinados intervalos assim como os riscos residuais e os níveis aceitáveis de risco, realizar auditorias internas regulares ao ISMS, realizar revisões regulares de gestão ao ISMS de forma a assegurar que o âmbito de protecção continua adequado e de forma a poderem-se identificar possíveis melhorias aos processos do ISMS, actualizar os planos de segurança de acordo com os resultados obtidos na monitorização e avaliação das actividades, registar acções e eventos que possam ter impacto na eficácia ou desempenho do ISMS.

Por último terminamos o método PDCA com a fase [*Act*], cuja aplicação no ISMS resulta nas seguintes actividades: implementação das melhorias identificadas, realização de acções apropriadas de prevenção e correcção, comunicação das acções e melhorias às partes interessadas, e por último assegurar que as melhorias realizadas atingem os objectivos inicialmente propostos. Finalizada esta fase, o ciclo retoma-se iniciando novamente a fase [*Plan*] e percorrendo novamente todas as fases.

4.5.1.1. Compromisso da Gestão de Topo

A implementação de um ISMS numa organização requer um compromisso da gestão de topo inequívoco, sendo este um requisito imprescindível para que se arranque com a implementação formal do sistema na organização. Este compromisso constitui a primeira etapa do ISMS e um factor crítico de sucesso para uma implementação eficaz do ISMS. É crucial que a gestão de topo assuma esse compromisso, mas é igualmente importante que se gerem evidências do mesmo.

A norma ISO/IEC 27001 aborda a questão do compromisso da gestão de topo no seu capítulo 5, no entanto esta etapa é esmiuçada com maior pormenor na norma ISO/IEC 27003. No que respeita à ISO/IEC 27001, é desde logo referido a importância de existir um compromisso da gestão de topo relativamente ao estabelecimento, implementação, operação, monitorização, avaliação, manutenção e melhoria do ISMS através de:

- Estabelecimento da Política de Gestão da Segurança da Informação;
- Assegurar que os objectivos e planos do ISMS são estabelecidos;
- Estabelecimento de papéis e responsabilidades para a segurança da informação;
- Comunicação à organização da importância de atingir os objectivos de segurança da informação e de conformidade com a Política de Gestão da Segurança da Informação, garantindo uma melhoria contínua do sistema;
- Fornecer recursos suficientes para estabelecer, implementar, operar, monitorar, avaliar, manter e melhorar o ISMS;
- Decidir o critério para aceitar os riscos e o nível aceitável de risco;
- Assegurar que as auditorias internas são realizadas;
- Conduzir revisões de gestão do ISMS.

A gestão de topo da organização com este compromisso assume ainda a responsabilidade de disponibilizar os recursos necessários ao ISMS, bem como as acções de formação e sensibilização de segurança da informação. Relativamente aos recursos, a gestão de topo deve comprometer-se a fornecer os recursos necessários para:

- Estabelecer, implementar, operar, monitorar, avaliar, manter e melhorar o ISMS;
- Assegurar que os procedimentos de segurança da informação suportam os requisitos de negócio;

- Identificar requisitos legais e regulamentares e obrigações contratuais de segurança;
- Manter uma segurança adequada através da aplicação adequada de todos os controlos implementados;
- Realizar avaliações quando necessário, e reagir de acordo com os resultados dessas avaliações;
- Melhorar a eficácia do ISMS, quando necessário.

No que respeita à formação e sensibilização, a gestão de topo deve garantir que, por um lado as pessoas com papéis e responsabilidades no ISMS têm as competências necessárias para cumprirem as suas funções, e por outro lado as restantes pessoas que incorporam a organização têm formação e estão sensibilizadas para as questões de segurança da informação.

Esta etapa onde se consegue o compromisso da gestão de topo com o ISMS é crucial ao seu sucesso e eficácia, pois se não houver esse compromisso "*dificilmente se conseguirá que os restantes elementos da organização levem a sério o ISMS*"(ABU-ZINEH, 2006) e o ponham em prática.

4.5.1.2. Âmbito de Protecção

A definição e fronteiras do âmbito de protecção constituem, a par do compromisso da gestão de topo, as etapas cruciais ao sucesso do ISMS. O âmbito de protecção consiste na "*protecção da informação oral, imprimida e registada automaticamente, na custódia de, ou usada por indivíduos e organizações. O âmbito também inclui todos os recursos que são o meio para a criação, processamento, transmissão, armazenamento, uso, disponibilização ou controlo (…) instalações, redes de comunicação, profissionais da informação, equipamento periférico, media de gravação e armazenamento de registos*"(ABU-ZINEH, 2006).

O âmbito de protecção pode abranger toda a organização, ou pode englobar uma parte da organização, por exemplo um *site* ou serviço. No entanto, todo o âmbito é constituído por processos, actividades, recursos e respectivos responsáveis (*owners*) pelos mesmos. Neste sentido, para que seja definido o âmbito de protecção é ainda necessário identificar:

- Âmbito e fronteiras organizacionais – onde deve constar a descrição das fronteiras organizacionais para o ISMS, funções e estrutura das partes da organização incluídas no âmbito, identificação da informação transmitida dentro do âmbito e da informação que transita de dentro para fora do âmbito, identificação de processos organizacionais e responsáveis alocados aos recursos de informação pertencentes ao âmbito incluindo fronteiras desses recursos com o exterior (ao âmbito), processo de hierarquia da tomada de decisão assim como a estrutura englobada no âmbito de protecção;
- Âmbito e fronteiras de TIC – identificação de recursos TIC abrangidos pelo âmbito, incluindo as suas fronteiras com processos e actividades externas ao âmbito. Devem ser descritas as infra-estruturas de comunicação, software, hardware, e respectivos papéis e responsabilidades;
- Âmbito e fronteiras físicas – onde devem ser identificadas localidades e instalações abrangidas pelo âmbito;
- Integração dos âmbitos e fronteiras acima definidos para obter o âmbito e fronteiras do ISMS – neste último ponto são integrados todos os âmbitos e fronteiras acima descritos, incluindo ainda os processos e actividades abrangidos pelo âmbito de protecção do ISMS.

No âmbito de protecção devem ainda ser referidos outros aspectos, como a conformidade legal, regulamentar e normativa, e a integração dos sistemas. Sobre este último aspecto, importa que referir que, tendo uma organização vários sistemas (ISMS, Sistema de Gestão da Qualidade, etc) implementados, é necessário garantir que esses sistemas mantêm a sua eficácia e não entram em conflito por funcionarem em conjunto.

Neste sentido, a BSI (*British Standards Institution*) desenvolveu o PAS 99 (*Publicly Available Specification*) que consiste no primeiro sistema integrado de gestão da especificação de requisitos. Este sistema é baseado em 6 requisitos da ISO *guide* 72 (norma para a escrita de normas de sistemas de gestão) (CHARTERED QUALITY INSTITUTE).

O PAS 99, à semelhança do ISMS, é estruturado segundo o método PDCA, e permite integrar dois ou mais sistemas de gestão de determinada organização num só sistema coeso, com um conjunto holístico de documentação (políticas, processos, procedimentos) (VASCONCELOS ; MELO, 2007).

Feita esta achega, e em jeito de conclusão, pode-se afirmar que o âmbito de protecção deve incluir as partes da organização abrangidas pelo ISMS, os recursos TIC, localidades e instalações físicas, e por último os processos, actividades e recursos que estão dentro do âmbito, devendo ainda existir um conjunto de processos de gestão para suporte aos processos incluídos no âmbito.

4.5.1.3. Políticas do ISMS

Segundo Zúquete (2006), as políticas de segurança definem o foco da segurança e o que deve ser garantido com a sua utilização. No fundo consistem num conjunto de boas práticas que definem o comportamento da organização: como esta gere, protege e atribui os recursos de forma a atingir os seus objectivos de segurança. As políticas são colocadas em prática através da implementação de um conjunto de mecanismos utilizados para o efeito. Neste sentido, a segurança da informação pode assim ser entendida como um conjunto de medidas compactadas e reflectidas na política de gestão da segurança da informação.

No que concerne às políticas, o ISMS é constituído, logo à cabeça, pela Política de Gestão da Segurança da Informação, considerada a política de topo e a mais importante de todas, sobre a qual se regerão os comportamentos e decisões tomadas na organização. Deve ser assumido um compromisso da gestão de topo relativamente a esta política, pois só assim se consegue fazer com os restantes elementos da organização a respeitem e pratiquem.

A Política de Gestão da Segurança da Informação deve ser um documento conciso, onde devem estar especificados aspectos cruciais como: a importância da gestão da informação e da gestão da segurança da informação para a organização; os compromissos assumidos pela organização, onde podem constar os pilares da segurança da informação (confidencialidade, integridade e disponibilidade) bem como outros considerados pertinentes para o contexto organizacional a que será aplicada a política; a descrição da orgânica de segurança do ISMS (CISO, Sponsor, *Security Forum*[9], *Process Owners*[10], *Resource Owners*[11]), onde devem ser descritos sucintamente os papéis e

[9] Grupo constituído com a finalidade de tomar decisões no âmbito do ISMS.
[10] Responsável por determinado(s) processo(s).
[11] Responsável por determinado(s) recurso(s).

respectivas responsabilidades no contexto do ISMS; o compromisso da organização pela continuidade de negócio, onde deve ser referenciada a consciência da organização de que nenhum sistema, por mais eficaz que seja, é 100% seguro e portanto é necessário que existam planos de continuidade de negócio e gestão de incidentes e crises que possam surgir; compromisso da organização pelo cumprimento das obrigações legais, regulamentares, normativas e contratuais a que é obrigada, garantindo assim a conformidade com os requisitos; garantia de condições para a auditoria, manutenção e melhoria contínua do ISMS, através da geração de evidências relativamente ao PDCA; e por último, compromisso da organização em divulgar a sua Política de Gestão da Segurança da Informação, tanto a nível interno como externo.

Mas as políticas do ISMS não se esgotam com a Política de Gestão da Segurança da Informação, embora esta seja considerada a política máxima de topo, é ainda necessário proceder ao desenvolvimento de um conjunto de políticas temáticas que sirvam de suporte à Política de Gestão da Segurança da Informação. São muitas as possibilidades de políticas temáticas que podem ser criadas, dependendo a selecção das mesmas do contexto organizacional e dos compromissos assumidos na Política de Gestão da Segurança da Informação. Assim sendo, a título de exemplo podemos ter as seguintes políticas temáticas: Política de Classificação da Informação, Política de Controlo de Acessos, Política de Gestão de Incidentes, Política de Segurança Física, Política de Gestão de Recursos Humanos, Política de Gestão da Continuidade de Negócio, Política de Avaliação do Risco, etc.

Assim sendo, a Política de Gestão da Segurança da Informação, considerada a "política de topo", deve antes de mais ser aprovada pela gestão de topo, gerando-se assim um compromisso pelo seu cumprimento. No entanto, esse compromisso não se restringe apenas à gestão, tendo todos os colaboradores da organização que se comprometer em cumprir e fazer cumprir a respectiva política. Posteriormente, esta deve também ser publicada demonstrando assim o compromisso da organização relativamente ao disposto na mesma.

4.5.1.4. BPM (*Business Process Management*)

O BPM (*Business Process Management*) é uma metodologia cujo objectivo é modelar o fluxo de processos organizacionais, através da sua análise, definição, execução, monitorização e gestão, relacionando o processo com a interacção de pessoas e aplicações informáticas, definindo metas a alcançar e levantando os requisitos de negócio. Esta metodologia pode ser vista de diferentes perspectivas e por conseguinte representar significados diferentes: pode ser vista como um processo para gerir os processos de negócio; uma disciplina de gestão; uma tecnologia ou conjunto de tecnologias; uma aplicação de desenvolvimento de *frameworks* (TREAT, 2006). Neste contexto, a BPM é vista como uma disciplina que permite estudar, identificar, mudar e monitorar os processos de negócio; é portanto uma forma de gerir processos.

A conceptualização de Processo consiste numa série ou uma rede de actividades de valor acrescentado, desempenhadas por pessoas (colaboradores) e/ou sistemas automáticos (informáticos ou não) com um objectivo identificado e que, embora tenha um início e fim definidos, repete-se ao longo do tempo. Um processo necessita de um ou mais *inputs* que são transformados ao longo das actividades que constituem o processo, acabando os mesmos por dar origem a novos *outputs*.

O processo de gestão de processos é composto por quatro actividades cíclicas (MULTICERT, 2011d):

- Levantamento e Definição – onde é feita a análise, desenho e documentação do processo e actividades, são definidas as métricas, os actores envolvidos (*process owner* e *process actor*[12]), os *inputs* necessários à realização do processo e actividades, e os *outputs* daí resultantes;
- Implementação – implica que todos os *outputs* que exijam modelos estejam disponíveis e definidos, e que o processo se encontre documentado e cada actor interveniente tenha recebido a respectiva formação para desempenhar as suas funções;
- Monitorização e controlo – esta fase é da responsabilidade do *process owner* do processo em questão, sendo este responsável por assegurar a sua correcta execução e os níveis de qualidade exigidos aquando a sua definição. Todas as alterações identificadas na monitorização e controlo (devidamente registadas no

[12] Colaborador que desempenha um papel activo em uma ou mais actividades do processo.

relatório de monitorização e controlo) ao processo deverão ser registadas e deverão ser incluídas na fase de reengenharia e melhoria contínua;

- Reengenharia e melhoria contínua – esta constitui a última fase do ciclo de gestão de processos, sendo aqui que, através dos *outputs* obtidos na fase de monitorização e controlo, se analisam os resultados e se propõem alterações ao processo (se necessário).

4.5.1.5. Gestão da Documentação

Como já foi referido anteriormente, o ISMS é constituído por um conjunto de documentos de diversas tipologias: políticas, processos, procedimentos, etc., consistindo assim numa grande fonte de produção documental. Como tal, a gestão da documentação produzida neste âmbito torna-se num factor crucial para o sucesso do mesmo. As normas ISO/IEC 27001 e BS 25999-2 fazem exactamente ênfase a esta questão, ressaltando a necessidade da organização elaborar um procedimento para a gestão de documentos, não constituindo este um mero procedimento acessório, mas antes um requisito crucial sem o qual a organização corre o risco de não conseguir obter a certificação (KOSUTIC, 2011a).

Mas porque é que a gestão da documentação do ISMS tem um papel tão importante na óptica da ISO/IEC e da BS? Em primeiro lugar porque o ISMS exige a produção de um grande volume de documentos, e por conseguinte, é fundamental a gestão destes para que se possam localizar fácil e rapidamente no momento pretendido e assim possam ser acedidos. Em segundo lugar porque uma gestão eficaz permite ter um maior controlo, quer sobre o histórico de versões do documento, quer sobre o acesso à versão mais actual do mesmo. Estas questões não se restringem "só" ao funcionamento interno da organização, têm também grande utilidade nos momentos de auditoria, pois o auditor não se limitará a verificar se existe um processo e/ou procedimento de gestão da documentação, este irá mais longe verificando se existe uma gestão efectiva da informação.

Passemos então a uma breve explanação dos requisitos estipulados nas normas acima citadas no que concerne a esta questão. A norma BS 25999-2 começa por indicar quais os documentos que devem ser produzidos no âmbito da continuidade de negócio,

indicando de seguida os factores que justificam a implementação de um controlo sobre os registos do BCMS (*Business Continuity Management System*) (BS 25999-2, 2007):

- O controlo de registos assegura que os documentos se mantêm legíveis, prontamente identificáveis e recuperáveis;
- Potencia a identificação dos documentos, o seu armazenamento, protecção e recuperação.

No item seguinte, a norma explica a relevância do controlo sobre a própria documentação referente ao BCMS, indicando que devem existir controlos sobre a mesma de forma a assegurar que os documentos (BS 25999-2, 2007):

- São aprovados de acordo com a sua prioridade;
- São revistos, actualizados e re-aprovados sempre que necessário;
- São identificadas as mudanças nos documentos, bem como o estado actual de revisão dos mesmos;
- Estão disponíveis as versões relevantes dos documentos aplicados;
- São identificados os documentos provenientes do exterior e a sua distribuição é controlada;
- É prevenida a utilização inadequada de documentos obsoletos.

A abordagem da norma ISO/IEC 27001 vai de encontro com a visão disposta na norma BS 25999-2, sendo indicados alguns documentos mandatórios no âmbito do ISMS. De seguida é indicada a necessidade de elaborar um procedimento que permita gerir a informação produzida, no sentido de indicar as acções de gestão necessárias para:

- Aprovar os documentos de acordo com a sua prioridade;
- Rever, actualizar e re-aprovar os documentos sempre que necessário;
- Assegurar que são identificadas as mudanças feitas nos documentos, bem como o estado actual de revisão dos mesmos;
- Assegurar que as versões relevantes dos documentos aplicados estão disponíveis para utilização no momento pretendido;
- Assegurar que os documentos se mantêm legíveis e prontamente identificáveis;

- Assegurar que os documentos estão disponíveis para quem precise de os usar, e que são transferidos, armazenados e finalmente eliminados de acordo com os procedimentos aplicáveis à sua classificação;
- Assegurar que os documentos provenientes do exterior são identificados;
- Assegurar que a distribuição dos documentos é controlada;
- Prevenir a utilização inadequada de documentos obsoletos;
- Associar um identificador adequado aos documentos, caso estes sejam mantidos.

Por último, esta norma refere ainda a importância de se gerarem registos que demonstrem evidências da conformidade com os requisitos estipulados na mesma, bem como a conformidade com os requisitos legais e regulamentares a que a organização está sujeita.

Quando se inicia a implementação do ISMS começa-se desde logo a percepcionar não só a importância de registar a informação, mas também de gerir esses registos antes que seja instaurado o caos e se perca o controlo sobre a organização da informação. "*Os documentos são na verdade o sangue do seu sistema de gestão – cuide bem deles se quiser que o seu sistema se mantenha saudável*" (KOSUTIC, 2011a).

4.5.1.5.1. Classificação da Informação

Como já foi referido, uma parte crucial do ISMS é exactamente a informação e os recursos de informação. Embora anteriormente se tenha referido a importância da gestão da documentação, a ênfase que se pretende atribuir é efectivamente à informação contida nesses documentos e é exactamente sobre a informação que recai a classificação.

A classificação da informação é atribuída de acordo com a importância e relevância que essa informação tem para a organização que a detém, ou seja, "*a informação que iremos classificar é fruto da interpretação e de um contexto próprio que determina, na maioria dos casos, o seu valor*" (CANÁRIO, 2010). Por outro lado, é através da classificação que determinada informação tem que ganhamos a percepção do seu valor, e por conseguinte, é através dessa que se definem os mecanismos que aquela informação terá para que se possa garantir a sua segurança.

A norma ISO/IEC 27002 aborda a questão da classificação da informação indicando desde logo que a informação deve ser classificada de acordo com o seu valor, requisitos legais a que está sujeita, sensibilidade e criticidade para a organização (ISO/IEC 27002, 2005).

Mas como pode ser determinado se a informação tem ou não valor para a organização? Antes de mais, para que determinada informação tenha valor para a organização é necessário que a mesma respeite certos atributos de qualidade, designadamente (CANÁRIO, 2010):

- Adequada – deve obedecer aos objectivos a que se propõe;
- Completa – deve conter todos os conteúdos, meta-informação e elementos gráficos necessários à sua compreensão;
- Correcta – deve conter informação sem erros;
- Verdadeira – deve conter informação verídica;
- Significativa/Compreensível – deve espelhar a sua importância para a organização e suportar de forma compreensível os seus conteúdos;
- Actualizada – deve ser actualizada e espelhar a realidade para a qual foi criada. Todas as versões devem ser armazenadas e passíveis de consulta;
- Íntegra – deve ser mantida de forma íntegra, devendo portanto estar salvaguardada de alterações não autorizadas;
- Disponível – deve estar disponível para o acesso no momento pretendido por quem estiver devidamente autorizado para tal;
- Protegida – deve ser mantida de forma segura e encontrar-se sempre disponível para utilização por elementos devidamente autorizados para tal.

Assim sendo, os factores que determinam o valor da informação são (CANÁRIO, 2010):

- A confirmação e manutenção dos atributos de qualidade;
- O valor do impacto na confirmação do compromisso da sua confidencialidade, integridade e disponibilidade;
- A disponibilidade do decisor/utilizador para aceitar essa informação.

Porém, a classificação e controlos de segurança associados à informação devem ainda ter em consideração as necessidades de negócio da organização relacionadas com

a partilha ou restrição do acesso à informação, e os impactos no negócio associados a tais necessidades (ISO/IEC 27002, 2005).

São muitas as razões que levam à preocupação pela classificação e segurança da informação, podendo-se desde logo incluir (GOVERNMENT OF ALBERTA (CANADA), 2005):

- Protecção da informação pessoal;
- Protecção de informação confidencial de acessos não autorizados;
- Protecção da propriedade intelectual;
- Apoiar a disseminação da informação;

Em jeito de conclusão podemos aferir que a informação deve ser classificada de acordo com o seu valor, tendo sempre em consideração os interesses da organização e os requisitos legais, regulamentares e normativos em vigor. A classificação da informação deve ser posta em prática tendo sempre em consideração (GOVERNMENT OF ALBERTA (CANADA), 2005):

- Classificação dos recursos de informação;
- Armazenamento da informação;
- Transmissão da informação;
- Eliminação da informação desnecessária;
- Protecção da integridade da informação;
- Permitir o acesso e divulgação apropriados;
- Estabelecer responsabilidades.

4.5.1.6. Análise do Risco

O ISMS baseia-se numa abordagem de risco, sendo este elemento "*a chave para a gestão da organização e para a protecção dos seus recursos de informação. Se a organização não conhece os riscos a que está sujeita, não será capaz de implementar uma protecção eficaz*" (HUMPHREYS, 2008).

A norma ISO/IEC 27005 é uma norma complementar à ISO/IEC 27001, cujo foco é exactamente a gestão do risco. São então definidas um conjunto de acções que

constituem o processo de gestão do risco de segurança da informação, seguindo o método PDCA (ISO/IEC 27005, 2008):

- [*PLAN*] – é estabelecido o contexto, avaliado o risco, desenvolvido o Plano de Tratamento do Risco, e a aceitação do risco;
- [*DO*] – é implementado o Plano de Tratamento do Risco;
- [*CHECK*] – é feita a monitorização e revisão contínua dos riscos;
- [*ACT*] – é mantido e melhorado o processo de gestão do risco de segurança da informação.

Relativamente à análise e avaliação do risco, a norma ISO/IEC 27005 começa por abordar a necessidade de se identificar o risco. Uma vez que a esta altura já está elaborado o inventário dos recursos de informação necessários à operacionalização dos processos considerados dentro do âmbito de protecção, já é possível começar a identificar as vulnerabilidades, e por conseguinte as ameaças a que estes recursos estão sujeitos.

Feito isto, há que verificar quais os controlos já introduzidos na organização e a forma como estão implementados, e que podem gerir o risco a que os recursos estão sujeitos.

Uma vez identificados os riscos associados aos recursos pertencentes ao âmbito de protecção do ISMS, torna-se necessário estimar o risco. Para tal é necessário adoptar uma ou mais metodologias de estimativa do risco, podendo o risco ser estimado através da atribuição de uma escala a nível qualitativo (risco baixo, médio, alto, …), através da atribuição de uma escala a nível quantitativo, ou uma combinação das duas (dependendo dos casos).

Antes de passarmos às acções seguintes, impõe-se abordar, pela sua pertinência e relevância, a metodologia PSR (Probabilidade x Severidade x Relevância) (ESPINHA ; S.), que consiste numa metodologia quantitativa que permite calcular o risco:

- Probabilidade – possibilidade de determinada vulnerabilidade ser explorada pelas ameaças associadas;
- Severidade – consequências na segurança da informação caso as ameaças explorem a vulnerabilidade com sucesso e ponham em causa os aspectos de confidencialidade, integridade e disponibilidade;

- Relevância – grau de importância do recurso para a continuidade do negócio da organização.

Esta metodologia consiste num cálculo, cuja composição da fórmula é a seguinte:

Valor do risco = Probabilidade x Severidade x Relevância

O resultado do cálculo cabe numa determinada escala numérica que pode ter associada uma determinada escala qualitativa (muito baixo, baixo, médio, alto, muito alto).

Em face desta informação, em seguida são identificados e ponderados os cenários de incidentes relevantes que possam suceder, incluindo a identificação de vulnerabilidades e ameaças associadas aos recursos de informação, bem como possíveis consequências aos recursos e aos processos de negócio, advenientes desses mesmos incidentes que possam ocorrer. Associado aos cenários de incidentes deve estar também a probabilidade de ocorrência do(s) mesmo(s).

4.5.1.7. Declaração de Aplicabilidade

A fase [*PLAN*] do ciclo PDCA termina com a elaboração deste documento – a Declaração de Aplicabilidade. A norma ISO/IEC 27001 contém um conjunto de objectivos de controlo e controlos que devem ser implementados para que seja garantida a segurança da informação. É através dos resultados obtidos pela análise do risco que se reúnem as condições para seleccionar os objectivos de controlo e controlos necessários a implementar na organização em questão.

A Declaração de Aplicabilidade é o documento onde são descritos os objectivos de controlo e controlos a implementar na organização, sendo que deve ser devidamente justificada a exclusão de qualquer controlo e/ou objectivo de controlo. A selecção dos controlos é direccionada de acordo com os requisitos identificados nos processos de avaliação do risco e tratamento do risco.

Mas se a avaliação do risco já nos fornece indicações sobre quais os controlos e objectivos de controlo necessários a implementar na organização, qual a utilidade de

elaborar uma Declaração de Aplicabilidade? Eis algumas razões para a necessidade de elaborar tal documento (KOSUTIC, 2011b):

- Durante o tratamento do risco são identificados os controlos necessários relacionados com os riscos identificados, no entanto na Declaração de Aplicabilidade são também identificados controlos necessários por outros motivos (requisitos legais, contratuais, etc);
- O documento resultante da avaliação do risco é de natureza algo extensa pelo que pode ser difícil a sua consulta para o uso operacional. A Declaração de Aplicabilidade é um documento bastante sucinto, muitas vezes consiste numa tabela onde são listados os controlos, e portanto a sua consulta é muito mais fácil;
- A Declaração de Aplicabilidade contém ainda informação sobre os controlos já aplicados na organização, e mais importante, dá indicação sobre como o controlo está implementado, fazendo referência a políticas, procedimentos, equipamentos, etc.

Para além das vantagens já referenciadas para a elaboração deste documento, um outro aspecto positivo que pode ser destacado é a facilidade que a Declaração de Aplicabilidade trará no momento de auditoria, pois fornecerá um guia de fácil verificação da operacionalização dos controlos.

Em suma, a Declaração de Aplicabilidade permite à organização reunir num documento os controlos e objectivos de controlo a implementar na organização, os controlos e objectivos de controlo já implementados demonstrando as evidências de tal, e permite ainda excluir e justificar a exclusão de alguns controlos e objectivos de controlo.

4.5.1.8. Plano de Tratamento do Risco

O tratamento do risco surge na sequência da análise e avaliação do risco. Embora o tratamento do risco faça ainda parte da fase [*PLAN*] do método PDCA, a formulação e implementação do Plano de Tratamento do Risco fazem já parte da fase [*DO*] do método.

No momento de proceder ao tratamento do risco torna-se necessário tomar decisões relativamente ao mesmo, com base nos resultados obtidos na avaliação do risco. Importa ainda referir que a organização deve definir um critério para determinar o nível aceitável para o risco, devendo este critério ser aprovado pela gestão de topo da organização.

Assim sendo, as opções de tratamento do risco são as seguintes (ISO/IEC 27005, 2008):

- Redução do risco – neste caso o nível do risco deve ser reduzido através da selecção de controlos, de forma a que o nível passe para o determinado como aceitável pela organização;
- Retenção do risco – dependendo da avaliação do risco, a organização pode aceitar o nível de risco tal e qual o resultado apresentado pela avaliação do risco, sem tomar qualquer acção para o reduzir;
- Evitar o risco – devem ser evitadas acções que possam aumentar o risco;
- Transferência do risco – neste caso, o risco é transferido para uma terceira parte que o possa gerir de forma mais eficaz.

Uma vez realizada a análise e avaliação do risco, identificados os tratamentos do risco, bem como elaborada a Declaração de Aplicabilidade, estão criadas as condições para se proceder à elaboração do Plano de Tratamento do Risco.

Este documento tem como objectivo definir exactamente como os controlos definidos na Declaração de Aplicabilidade serão implementados: Quem irá implementar os controlos? Quando? Como? Com que orçamento? etc. No fundo, o Plano de Tratamento do Risco consiste num plano de implementação focado nos controlos descritos na norma ISO/IEC 27001, fundamentado nos resultados obtidos na análise e avaliação do risco, e tendo ainda em linha de conta os critérios de aceitação do risco estabelecidos pela gestão de topo da organização.

5. O Sistema de Gestão da Segurança da Informação da MULTICERT

Neste capítulo são apresentados os resultados práticos obtidos durante a implementação das fases do ISMS na MULTICERT.

Por motivos de confidencialidade, este capítulo da dissertação foi suprimido do corpo de texto, passando a constituir um anexo desta dissertação.

6. Conclusões e Perspectivas Futuras

Cada vez mais as organizações dependem dos seus sistemas de informação, e cada vez mais a informação é vista, não só como representante da memória organizacional, mas também como factor de competitividade estratégica. A crescente utilização da internet e das ligações em rede proporcionam novas dinâmicas de trabalho, porém abrem também portas a novas ameaças à informação, que consigo acarretam riscos acrescidos.

Um incidente pode causar grandes danos numa organização, que podem ir desde custos financeiros e/ou informacionais até pôr em risco a própria continuidade do negócio. Assim, a segurança da informação desempenha cada vez mais um papel crucial para as organizações, deixando de ser vista como um custo e passando a ser encarada como um investimento.

Porém, engane-se quem encara a segurança da informação como uma solução que passa por bases tecnológicas, esta vai mais além significando uma mudança cultural interna à organização, que trespassa para o exterior. A segurança da informação passa sim por uma gestão contínua e eficaz de inúmeros factores nesta dissertação abordados, e que de certa forma podem ser compactados numa visão que recai sobre a gestão dos riscos associados à informação e aos recursos informacionais.

O ISMS permite gerir a segurança da informação através de um método que proporciona uma eficácia garantida, pela sua abordagem que possibilita atingir uma melhoria contínua deste sistema. No entanto, a organização tem que estar preparada e receptiva às mudanças na sua cultura e na sua abordagem à segurança da informação, o que por vezes não constitui tarefa facilitada.

Fazer ver aos colaboradores da organização as vantagens do ISMS pode ser um meio eficaz para que estes aceitem as mudanças que este sistema acarreta. De forma sucinta, podem ser enumeradas algumas vantagens do ISMS:

- Identificar os recursos críticos para o negócio;
- Prover uma *framework* que permite a melhoria contínua;
- Proporcionar uma confiança acrescida, quer dos colaboradores, quer das partes externas (clientes, parceiros, *etc*) que interagem com a organização;

- Proporcionar à organização uma capacidade de resposta aos incidentes mais eficaz e eficiente;
- *Etc*.

A implementação de um ISMS numa organização requer um grande esforço para cada indivíduo da organização e para a organização como um todo, não só de adaptação ao novo comportamento que toda a organização deve ter, como também de gestão contínua do sistema. Fundamentalmente, é necessária a alteração da cultura da organização para que se possa alcançar melhorias na segurança da informação da mesma.

No âmbito desta dissertação foram propostos os seguintes objectivos:

- Investigar as normas de segurança aplicáveis à Segurança da Informação, nomeadamente a ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27005 e BS 25999;
- Identificar os objectivos de controlo e os controlos necessários, em funcionamento e a implementar;
- Definir e elaborar a documentação necessária à implementação do ISMS para o âmbito definido;
- Realizar a Análise do Risco e preparar o Plano de Tratamento do Risco.

Como já pudemos constatar pelo conteúdo apresentado ao longo desta dissertação, os objectivos propostos foram totalmente alcançados com sucesso, sendo em alguns casos até mesmo ultrapassados. O desenvolvimento do ISMS feito até agora na MULTICERT requereu um enorme trabalho, uma vez que a fase de planeamento do ISMS constitui a fase mais crítica para o sucesso do sistema, e talvez por isso também a mais exigente, pois é nesta fase que se tomam decisões que irão condicionar/encaminhar o desenvolvimento das fases seguintes do projecto de implementação do sistema.

Como trabalho futuro perspectiva-se explorar as problemáticas que surgirão aquando da operacionalização das etapas [*DO*], [*CHECK*] e [*ACT*], para além da implementação do Plano de Continuidade de Negócio.

Em jeito de conclusão, poder-se-á ainda referir a experiência enriquecedora que esta dissertação proporcionou, bem como o conhecimento aprofundado sobre uma área

que cada vez mais ganha maior dimensão. Implementar um ISMS requer, como já foi referido, um grande esforço de toda a organização, pois implica a implementação de grandes mudanças. No entanto, as vantagens resultantes da implementação deste sistema recompensam todo o esforço que a organização, como um todo, tem que ter para que o ISMS seja implementado.

Referências Bibliográficas

– ABU-ZINEH, Sami - *Sucess Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies*. 2006.

– BS 25999-1 - *Business continuity management - Code of practice*. 2006.

– BS 25999-2 - *Business continuity management - Part 2: Specification*. 2007.

– CANÁRIO, Sofia Neto - Implementação de um Sistema de Classificação da Informação. *Páginas a&b: arquivos & bibliotecas*. 2.5:(2010). p. 111-130.

– CASSIDY, Anita - *A pratical guide to information systems strategic planning*. 1998.

– CHARTERED QUALITY INSTITUTE - *PAS 99: Integrated Management Framework*.

– CHOO, Chun Wei - *A Gestão de Informação para a organização inteligente: A arte de explorar o meio ambiente*. 2003.

– CHOO, Chun Wei - *Information Management for the Intelligent Organization*. 1998.

– CLINCH, Jim - ITIL V3 and Information Security. (2009). p.

– DEY, Manik - *Information Security Management: A Pratical Approach*. 2007.

– DOLYA, Alexey - *Internal IT Threats in Europe 2006*. 2007.

– ESPINHA, Rafael; S., João - Melhorando Processos Através da Análise de Risco. *Engenharia de Software*.

– EUROPEAN PAYMENTS COUNCIL - *e-Mandates e-Operating Model: High Level Definition*. 2009.

– GABINETE NACIONAL DE SEGURANÇA - *Norma Técnica D02: Requisitos Mínimos de Segurança Física de Instalações de Entdades Certificadoras*. 2008.

– GOVERNMENT OF ALBERTA (CANADA) - Information Security Classification. (2005).

– HUMPHREYS, Edward - Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*. 13:4 (2008).

– ISO/IEC 27001 - *Information security management systems - Requirements*. 2005.

– ISO/IEC 27002 - *Information Technology - Security Techniques: Code of practice for information security management*. 2005.

– ISO/IEC 27003 - *Information security management system implementation guidance*. 2010.

– ISO/IEC 27005 - *Information security risk management*. 2008.

– JOSANG, Audun; ALZOMAI, Mohammed - *Security Usability Principles for Vulnerability Analysis and Risk Assessment*. Miami: 2007.
– KOSUTIC, Dejan - *Document management in ISO 27001 & BS 25999-2*. 2011a.
– KOSUTIC, Dejan - *The Importance of Statement of Applicability for ISO 27001*. 2011b.
– MA, Qingxiong - *A Study on Information Security Objectives and Practices*. Southern Illinois University at Carbondale, 2004.
– MAMEDE, Henrique São - *Segurança Informática nas Organizações*. 2006.
– MARTINS, Gilberto de Andrade; THEÓPHILO, Carlos Renato - *Metodologia da Investigação Científica para Ciências Sociais Aplicadas*. 2007.
– MIRELA, Gheorghe; MARIA, Boldeanu Dana - Information Security Management System. (2008).
– MULTICERT - *Declaração de Aplicabilidade*. 2011a.
– MULTICERT - *Definição do Âmbito de Protecção*. 2011b.
– MULTICERT - *Diagrama de Arquitectura do Âmbito de Protecção*. 2011c.
– MULTICERT - *Estratégia BPM*. 2011d.
– MULTICERT - *Guia de Classificação de Segurança*. 2008a.
– MULTICERT - *Manual de Acolhimento*. 2010a.
MULTICERT - *Política de Gestão de Processos*. 2010b.
– MULTICERT - *Empresa*. 2010c.
– MULTICERT - *Projectos*. 2010d.
– MULTICERT - *Metodologia de Análise do Risco*. 2011e.
– MULTICERT - *Política de Gestão da Segurança da Informação*. 2011f.
– MULTICERT - *Processo de Gestão do Ambiente de Informação*. 2011g.
– MULTICERT - *Processo de Gestão do Risco*. 2011h.
– MULTICERT - *Regras de Ambientes*. 2008b.
– NNOLIM, Anene L. - *A Framework and Methodology for Information Security Management*. Michigan: Lawrence Technological University, 2007.
– OECD - *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. 2002.
– OLIVEIRA, Wilson - *Segurança da Informação: Técnicas e Soluções*. 2001.
– PARK, Cheol-Soon; JANG, Sang-Soo; PARK, Young-Tae - A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. *Computer Science and Network Security*. 10:3 (2010). p.

– PINTO, Manuela Azevedo - *Slides das aulas de Gestão de Serviços de Informação*. 2009.

– RIBEIRO, Joaquim - Método Quadripolar. 2006.

– SILVA, Armando Malheiro da - A Gestão da Informação abordada no campo da Ciência da Informação. *Páginas a&b: arquivos & bibliotecas*. 16:(2005). p. 89-113.

– SILVA, Armando Malheiro da - *A Gestão da Informação Arquivística e suas Repercussões na Produção do Conhecimento Científico*. Rio de Janeiro: 2000.

– SILVA, Armando Malheiro da - *A Informação: Da compreensão do fenómeno e construção do objecto científico*. 2006.

– SILVA, Armando Malheiro da; RIBEIRO, Fernanda - *Das "ciências" documentais à ciência da informação: Ensaio epistemológico para um novo modelo curricular*. 2002.

– SILVA, Claudete Aurora da - *Gestão da Segurança da Informação: Um olhar a partir da Ciência da Informação*. Universidade Católica de Campinas, 2009.

– SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho - *Segurança dos Sistemas de Informação: Gestão Estratégica da Segurança Empresarial*. 2003.

– SIPONEN, Mikko; WILLISON, Robert - Information Security Management Standards: Problems and Solutions. *Information and Management*. 46:5 (2009). p. 267-270.

– SOARES, António Lucas - *Slides das aulas de Planeamento Estratégico de Sistemas de Informação*. Faculdade de Engenharia da Universidade do Porto, 2009.

– TINTAMUSIK, Yanarong - *Examining the Relationship between Organization Systems and Information Security Awareness*. Northcentral University, 2010.

– TREAT, Mark - *What Is BPM Anyway?* 2006.

– VAN BON, Jan; VERHEIJEN, Tieneke - *Framework for IT Management*. itSMF-NL, 2006.

– VASCONCELOS, Diogo Sérgio César de; MELO, Maria Bernadete Fernandes Vieira de - *Aplicabilidade da Especificação PAS 99:2006 como Modelo Integrado de Gestão: Um Caso de Estudo*. 2007.

– ZÚQUETE, André - *Segurança em Redes Informáticas*. 2008.