Universidade do Minho
Escola de Engenharia

Pedro Manuel Gomes Silva

A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências

Tese de Mestrado submetida à Universidade do Minho para a obtenção do grau de Mestre em Tecnologias e Sistemas de Informação, na área de conhecimento em Gestão de Sistemas de Informação.

Trabalho efectuado sob a orientação do
Professor Doutor José Carlos Nascimento

Setembro de 2007

Agradecimentos

Ao Professor Doutor José Carlos Nascimento
pela orientação e disponibilidade para este trabalho de investigação.

Ao Doutor Alberto Carneiro, ao Dr. Rui Gomes e ao Dr. Paulo Gomes
pela colaboração e participação na aplicação prática de resultados deste trabalho.

Resumo

O título deste trabalho "A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências" reflecte o seu principal objectivo que é propor um modelo com os vários processos de gestão da função Auditoria de SI e com as competências que complementarmente são exigíveis ao Auditor de SI. Este modelo poderá constituir as bases para a elaboração futura de uma Metodologia de Auditoria de SI e de uma Política de Auditoria de SI. A função Auditoria tem evoluído no seu paradigma, preocupando-se actualmente com os processos de negócio e com os SI que os suportam, baseando-se numa abordagem ao risco. Como consequência desta evolução no Modelo Funcional da Auditoria, dever-se-á verificar também uma indissociável evolução no Modelo de Competências dos profissionais de Auditoria. Este trabalho começa por efectuar a definição dos conceitos associados à Auditoria de SI, um resumo da evolução da função e do seu papel e uma exploração dos principais factores caracterizadores do paradigma actual da função. É proposto um Modelo Funcional, ou seja, um conjunto de ideias estruturadas e sequenciadas sobre a função que, em conjunto, formam o modelo: os objectivos, a organização, o âmbito, os referenciais metodológicos e os processos de Auditoria de SI. Trata-se de um exercício pouco frequente na literatura académica de Auditoria de SI pelo tipo de contributos recolhidos (originais do autor, autores independentes, organizações profissionais de Auditoria e entidades que estudam os processos de SI) e pela sistematização dos conceitos efectuada (apoiada em representações gráficas). São igualmente lançadas novas ideias, entre as quais se destacam três: o posicionamento conceptual da função; a identificação de actividades específicas de Auditoria de SI previstas em três referenciais de SI (CobiT, ITIL e ISO 17799); e a utilização dos conceitos de Gestão de Projectos aplicados na Gestão das Auditorias de SI. O trabalho complementa-se com a proposta dum Modelo de Competências, designado de "MICASI - Modelo de Identificação de Competências do Auditor de SI", para o qual se desenvolveu uma ferramenta informática de suporte. O modelo resulta da combinação e adaptação de dois referenciais distintos que correspondem aos dois principais tipos de competências do Auditor de SI: as Competências de Gestão (baseado num modelo de competências de Gestão de Projectos) e as Competências Técnicas (baseado no Modelo Curricular da ISACA). Por fim, apresentam-se os resultados da aplicação prática do modelo MICASI através da realização de entrevistas semi-estruturadas a profissionais de Auditoria de SI. O propósito foi a classificação das competências que estes profissionais consideram como mais importantes para a actividade de Auditor de SI.

Abstract

This work's title "The Information Systems Audit Function: Functional and Competence Model" reflects its main objective: to propose a model with several management processes of the IS Audit function and, complementary, to present the skills that are required to the IS Auditor. This model could set the basis for a future development of an IS Audit Methodology and an IS Audit Politics. The Audit function has evolved in its paradigm, being nowadays concerned with the business processes and the IS that support them, adopting a risk-based approach. As an outcome of this evolution in the Audit Functional Model, there should also be a binding evolution in the Competence Model of the Audit professionals. This work begins with the definition of IS Audit related concepts, a summary of the evolution of the function and its role, and the exploration of the main factors that characterize the current paradigm of the function. A Functional Model is proposed, that is to say, a set of structured and sequential ideas about the function that altogether shape the model: the purpose, the organization, the scope, the methodological frameworks and the processes of IS Audit. This constitutes an unusual exercise in IS Audit academic literature due to the type of collected contributions (author originals, independent authors, Audit professional associations, and entities that study IS processes) and due to the concept systematization that is done (supported by graphical representations). New ideas are also presented and these three are highlighted: the conceptual positioning of the function; the identification of IS Audit specific activities considered in three IS frameworks (CobiT, ITIL and ISO 17799); and the use of Project Management concepts applied to IS Audit Management. The work is complemented with the proposal of a Competence Model for the IS Auditor, named "MICASI - Information Systems Auditor Competence Identification Model", for which a supporting tool was developed. This model results from the combination and adaptation of two distinct frameworks that correspond to the two main types of IS Audit competences: Management Skills (based on a Project Management competence model) and Technical Skills (based on the ISACA Model Curriculum). Lastly, a presentation is made of the results of a practical application of the MICASI model by doing semi-structured interviews to IS Audit professionals. The aim was to classify the skills that these professionals considered to be the most important for the activity of IS Auditor.

Índice

Lista de Figuras

Lista de Tabelas

1 INTRODUÇÃO

1.1 MOTIVAÇÃO E ENQUADRAMENTO

A evolução, complexidade e predominância dos Sistemas de Informação (SI) nas organizações actuais fazem com que a Informação e os Sistemas que a suportam devam ser cada vez mais controlados.

Os SI e as Tecnologias da Informação e Comunicação (TIC) têm afectado as organizações em diversas vertentes, alterando não só os processos de negócio mas também os papéis/missões das diversas funções da organização, entre as quais se encontra a função Auditoria. No domínio dos SI e das TIC, em que a mudança é uma constante, é importante conhecer esses efeitos transformadores, nomeadamente nas competências exigidas para o desempenho de uma função particular relacionada com os SI: a Auditoria de SI.

O exigente nível de conhecimento e de competências necessárias ao controlo dos SI implicam uma crescente necessidade das organizações possuírem profissionais de SI que assegurem e se dediquem a funções de suporte tais como a segurança, a auditoria e a gestão dos riscos associados aos SI.

A função Auditoria nas organizações, onde se inclui a Auditoria de SI, tem evoluído no seu estatuto, devendo ser encarada como uma actividade de suporte ao negócio (por oposição a uma actividade de inspecção) e como tendo um carácter pró-activo ou preventivo (por oposição a um carácter reactivo). Segundo este novo paradigma, a Auditoria deve ter a sua preocupação centrada nos processos de negócio e nos SI que os suportam, baseando-se numa abordagem ao risco.

Como consequência desta evolução no modelo funcional da Auditoria, dever-se-á verificar também uma evolução do modelo de competências dos profissionais de Auditoria de SI. Estes

tenderão a ser de um modo geral menos técnicos e especializados, passando a deter mais competências de gestão e conhecimento do negócio, complementando as competências técnicas base sempre necessárias.

O tema desta Dissertação – "A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências" – insere-se no âmbito da área disciplinar da Gestão dos SI, nomeadamente:

- Na área do Planeamento e Organização dos SI, no que diz respeito à vertente "função"
- Na área de Recursos Humanos de SI, no que diz respeito à vertente "competências".

A abordagem a este tema será também uma oportunidade para o autor da tese reflectir sobre uma área relacionada com a sua actividade profissional actual – Auditoria e Gestão de Risco – esperando que este trabalho de investigação possa contribuir para a "excelência profissional" nesta área.

1.2 QUESTÕES DE INVESTIGAÇÃO E OBJECTIVOS

Perante o contexto atrás apresentado, a tese será orientada, essencialmente, pelo estudo da seguinte questão de investigação:

→ Qual o papel/missão actual para a função Auditoria de SI nas organizações?

E, complementarmente, pelo impacto que aquela tem na questão:

→ Quais as competências/capacidades actualmente exigidas aos profissionais de Auditoria de SI?

Tendo por base estas questões de investigação, esta tese pretende atingir o seguinte objectivo:

→ Identificar um modelo funcional para a Auditoria de SI, compreendendo e situando o papel/missão desta função no contexto das organizações.

Possui, também, como objectivo complementar:

→ Identificar/apontar pistas para um modelo de competências para os profissionais de Auditoria de SI (competências de gestão, técnicas, etc.).

Considerando o risco das duas questões de investigação aqui formuladas constituírem talvez um âmbito de investigação demasiado vasto para uma Tese de Mestrado, às quais se juntam ainda os objectivos enunciados, torna-se importante esclarecer que:

- A resposta à segunda questão de investigação constitui-se como um complemento às ideias sistematizadas na resposta à primeira.
- A adopção das duas questões em conjunto faz sentido, tornando-se necessária e justificada pois o papel/missão da função Auditoria, em particular a Auditoria dos SI, é indissociável das competências/capacidades que um profissional de Auditoria de SI deve possuir.

1.3 METODOLOGIA DE INVESTIGAÇÃO

1.3.1 VÉRTICES DA METODOLOGIA UTILIZADA

Esta investigação tem como ponto de partida o previsto no documento de Proposta de Dissertação, nomeadamente nos seguintes pontos deste documento: Enquadramento, Objectivos, Metodologias e Referências Bibliográficas. Com o decorrer do processo de investigação, o âmbito e os objectivos foram reajustados de modo a serem compatíveis com uma abrangência realística de uma Tese de Mestrado, tendo-se optado por manter o título da tese pois este continua a suportar o reajuste.

A Figura 1.1. esquematiza os três vértices de investigação (revisão bibliográfica, análise qualitativa e experiência profissional) que foram utilizados nas três principais componentes da tese:

- A Auditoria de SI → Baseia-se fundamentalmente na revisão bibliográfica para a apresentação dos conceitos associados à Auditoria de SI e à sua evolução. Baseia-se também, em menor proporção, na experiência profissional do autor, na área da Auditoria e Gestão de Risco, para a identificação dos principais elementos caracterizadores do paradigma actual da função, bem como para a adaptação de abordagens sistémicas para entender o papel da Auditoria nas organizações.

- O Modelo Funcional → Baseia-se na revisão bibliográfica e na incorporação da experiência profissional do autor. Note-se que sendo a componente Modelo Funcional uma das bases da tese, após esta componente estar fundamentada de um modo adequado à realidade das organizações, estaremos em condições de analisar a componente Modelo de Competências.

- O Modelo de Competências → Baseia-se na revisão bibliográfica e na análise qualitativa dos resultados das entrevistas semi-estruturadas efectuadas a profissionais responsáveis por Auditoria de SI, com uma experiência muito significativa na área. Nesta tese, entende-se por análise qualitativa o binómio recolha e tratamento dos dados das entrevistas semi-estruturadas. O objectivo destas breves entrevistas é identificar, sob um ponto de vista prático, quais são as competências mais importantes que os Auditores de SI deverão possuir, de entre as identificadas na revisão bibliográfica. Refira-se que, embora a experiência profissional do autor da tese não seja directamente considerada como fundamento para a componente Modelo de Competências, o factor experiência profissional foi considerado indirectamente através da análise qualitativa aos resultados das entrevistas semi-estruturadas que traduzem a experiência dos profissionais responsáveis por Auditoria de SI.

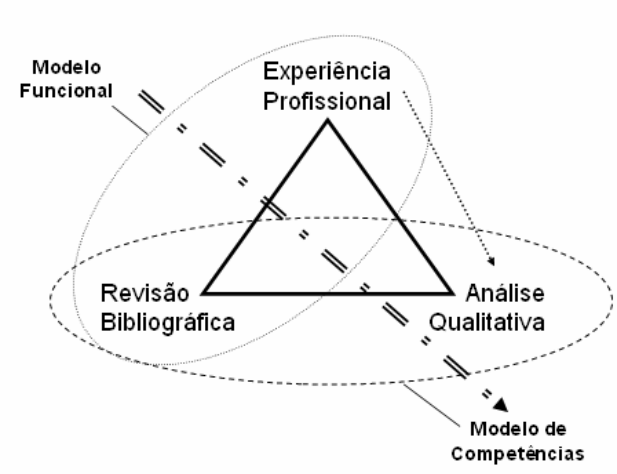


Figura 1.1 - Vértices da Investigação de Tese

Fonte: Elaborado pelo autor

1.3.2 VANTAGENS E LIMITAÇÕES

No que diz respeito ao primeiro dos vértices da tese, a revisão bibliográfica, entende-se que a utilização desta abordagem metodológica é, quando comparada com os outros dois vértices, pacífica e de aceitação generalizada (e até mesmo obrigatória) em trabalhos desta natureza, pelo que não serão exploradas as vantagens e limitações. É, no entanto, importante esclarecer que a revisão bibliográfica foi delimitada com uma perspectiva muito prática e direccionada para o contexto das organizações, recorrendo apenas em poucos casos a "descrições históricas" da evolução da função Auditoria de SI. Foram também incorporados nesta tese alguns resultados de trabalhos que se relacionam com o tema, efectuados pelo autor no âmbito das disciplinas do curso de Mestrado.

Relativamente ao segundo dos vértices, a análise qualitativa, a sua utilização no estudo da componente Modelo de Competências constitui valor acrescentado, na medida em que se recorre a uma pequena amostra de três entrevistas semi-estruturadas para complementar o estudo. A adequação da análise qualitativa enquanto ferramenta metodológica será, de seguida, debatida com maior detalhe.

O facto da análise ser qualitativa, implica fundamentalmente que é uma análise que lida com conceitos (neste caso, competências de um Auditor de SI) e não essencialmente com números. No entanto, uma análise qualitativa não é necessariamente especulativa (com enviesamentos, intencionalmente positivos ou negativos), podendo ser meramente interpretativa (isenta de enviesamentos intencionais, tanto quanto possível).

A propósito de visões diferentes no processo de investigação em SI, (Nascimento, 2002) faz referência aos "princípios da lógica indutiva, segundo a qual a teoria emerge a partir dos contributos dos participantes, considerando estes contributos como importantes para a própria construção do processo de investigação e aceitando a intervenção do investigador como integrante activa do próprio processo, sendo que aquele o influencia e é por este influenciado." Ainda segundo este autor, "face ao peso da tradição positivista e do suporte quantitativo na investigação em SI, a falta de qualidade é um argumento que trava frequentemente a aceitação pela comunidade científica de trabalhos de investigação de natureza qualitativa e interpretativista".

No domínio da investigação em SI, esta problemática está particularmente bem desenvolvida num estudo de (Kaplan and Duchon, 1998) sobre novos SI que considera que as entrevistas incluem-se nos métodos qualitativos. Segundo estes autores, na abordagem qualitativa, teorias são desenvolvidas indutivamente a partir dos dados recolhidos, generalizações são construídas de base e são tentados vários esquemas interpretativos. O estudo observa ainda, em abordagens qualitativas tais como as entrevistas, a importância de se manterem registos sistematizados para serem usados na análise da informação recolhida. A utilização de entrevistas semi-estruturadas é também apontada por (Nascimento, 2002) como um "instrumento de recolha de informação adequado quando o período de disponibilidade dos participantes da investigação se afirma limitado". O estudo de caso (*case study*) de (Kaplan and Duchon, 1998) contém aquela que poderá ser uma possível resposta para a questão: será que as entrevistas semi-estruturadas se adequam aos objectivos desta investigação? O referido estudo indica, entre outras conclusões: "*the need for context-specific measures of job characteristics*". Neste sentido, a utilização de entrevistas a profissionais de Auditoria de SI para validar as características que um Auditor de SI deve possuir parece ser uma opção aceitável.

Quanto ao terceiro dos vértices, a experiência profissional, este deverá ser entendido aqui como uma mais-valia em cima dos dois vértices anteriores, ganhando formalização através da passagem de conhecimento implícito (que foi adquirido pelos intervenientes na investigação ao longo das suas práticas profissionais) para conhecimento explícito (que ficará registado e moldará a forma dos conteúdos da tese).

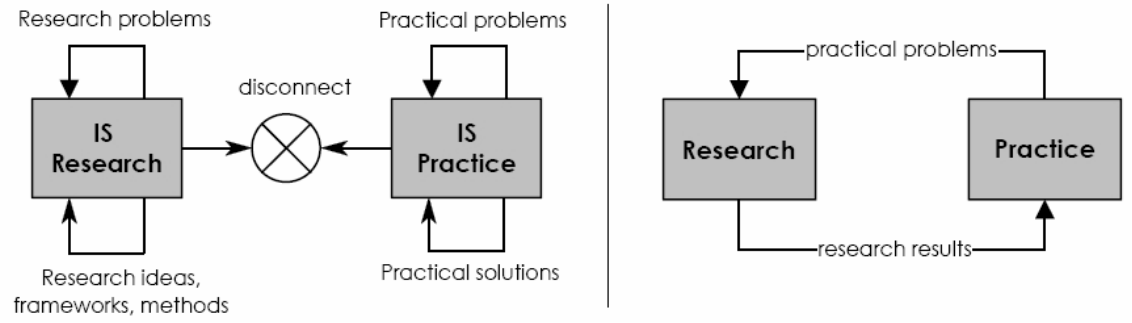


Figura 1.2 - Falta de ligação entre a Investigação académica e a Prática profissional em SI

Fonte: Versão original extraída de (Moody, 2000): "*The Current Situation vs. What Should Happen*"

Tal como a figura anterior pretende esquematizar, verifica-se por vezes que a investigação académica em SI está desligada da prática profissional, existindo pouca intersecção e transferência de conhecimento entre estes dois domínios. Este facto é reconhecido por (Moody, 2000) que considera que a disciplina de SI aproxima-se mais de uma ciência "aplicada" do que uma ciência "pura". Isto é, deve-se focar mais na aplicação prática dos SI, ou seja, contribuição para as profissões de SI e, em última instância, para a satisfação de necessidades da sociedade, do que apenas nos SI por si só, caso em que estaríamos perante uma falta de responsabilidade social ("*social accountability*"). Defende que os SI, enquanto ciência aplicada, não alcançarão mais legitimidade pelo rigor dos seus métodos ou pela sua base teórica, mas sim pela sua utilidade prática. Compara ainda a disciplina dos SI à Medicina em que, nesta última, existe forte ligação entre a investigação académica e a prática profissional.

Embora esta seja uma temática de grande abrangência e nem sempre consensual, a da natureza da disciplina de SI (aplicada vs. pura), o importante é reconhecer que diferentes métodos de investigação são adequados dependendo das questões de investigação (*research questions*) em causa. Aliás estas questões, ou seja, "o que investigar?", ficam por vezes subordinadas à questão do "como investigar?". No caso da presente investigação, dada a dificuldade de testar o tema num contexto formal ("de laboratório"), afigura-se ser adequada a utilização de contextos organizacionais (empresariais), usando a experiência de profissionais de Auditoria de SI para a identificar e validar ideias sobre as competências que um Auditor de SI deve possuir.

Em jeito de encerramento do ponto das vantagens e limitações, pode concluir-se que é legítima uma metodologia de investigação académica que, para além da tradicional revisão bibliográfica, inclui também uma análise qualitativa baseada em casos e complementa com o conhecimento provindo de experiência de profissionais. Esta afirmação parece ser compatível com o já referido estudo de (Kaplan and Duchon, 1998) quando este conclui que uma mistura de métodos pode levar a novas perspectivas e formas de análise que são pouco prováveis de ocorrer quando apenas um dos métodos é usado isoladamente.

1.3.3 MODELOS ESTRUTURADOS, NORMAS E FERRAMENTAS UTILIZADAS

Entendeu-se também considerar a utilização de outros instrumentos de suporte à investigação e à produção do trabalho, nomeadamente de modelos estruturados (*frameworks*) e normas (*standards*), no sentido de referências metodológicas, e também de ferramentas, no sentido de aplicativos informáticos.

Quanto ao propósito da utilização destes instrumentos, eles possuem diferentes graus de adequabilidade e de aproveitamento consoante o objectivo e o capítulo do texto em que se enquadram, tal como a tabela seguinte pretende sistematizar.

CAPÍTULO	MODELOS / NORMAS / FERRAMENTAS	OBJECTIVOS
2.3	*Framework* - COSO	Compreender a base do paradigma actual da Função Auditoria, nomeadamente a visão holística e as diversas dimensões da Auditoria de SI.
2.3	*Framework - IT Risk Management Life Cycle*	Identificar conceitos e actividades que poderão/deverão ser consideradas e aplicadas numa Auditoria de SI baseada no risco.
3.2	*Framework - Process Classification*	Enquadrar as funções de Gestão de SI e de Auditoria dos SI como Processos de Negócio no modelo organizativo.
3.4	*Framework / Standard* - COBIT	Descrever 3 referenciais metodológicos que podem ser utilizados nas Auditorias de SI, tanto como delimitadores do universo/âmbito dos processos de SI a auditar, ou como metodologias de Auditoria de SI para adaptar.
	Framework / Standard - ITIL	
	Framework / Standard - ISO 17799	
3.5	*Framework / Standard* - PMBOK	Equiparar uma Auditoria de SI a um Projecto, entendendo a gestão das fases e das actividades de uma Auditoria de SI como processos de Gestão de Projectos.
4.2	*Framework - SSQ Soft Skills Quantification*	Identificar, caracterizar e classificar quantitativamente as competências de gestão (SSQ) e as competências técnicas (*Model Curriculum*) que os Auditores de SI devem possuir, servindo de base para as entrevistas semi-estruturadas.
4.2	*Framework - ISACA Model Curriculum for IS Audit and Control*	
4.3	Ferramenta – *MS Excel*	Estruturar, calcular e apresentar sob a forma de gráficos os resultados das entrevistas semi-estruturadas relativos à avaliação quantitativa (pontuação) e qualitativa (destaques) das competências dos Auditores de SI.

4.3	Ferramenta - *Mind Manager*	Estruturar, mapear e apresentar graficamente as ideias identificadas e debatidas nas entrevistas semi-estruturadas relativas à avaliação qualitativa das competências dos Auditores de SI.

Tabela 1.1 - Objectivos dos Modelos, Normas e Ferramentas utilizadas

Fonte: Elaborado pelo autor.

Antes de concluir esta secção relativa à metodologia de investigação utilizada, é relevante informar sobre as seguintes opções de escrita deste texto:

- As citações de autores e obras, quando transcritas na íntegra, foram mantidas na respectiva língua original (por exemplo, em inglês). Esta opção pretende favorecer a manutenção do sentido das citações, ou seja, manter o espírito da letra original que por vezes é difícil de conservar nas traduções.
- Nos casos em que os termos/expressões em língua estrangeira possuem um significado mais rico do que em português, optou-se por mantê-los, traduzindo-os e colocando-os da seguinte forma: [termo traduzido para português (*termo na língua original*)].
- A revisão bibliográfica vai intercalar e coexistir, ao longo dos diversos capítulos do trabalho, com os contributos do próprio autor (exemplos: esquemas conceptuais originais e/ou adaptações de trabalhos sobre o tema efectuados anteriormente pelo autor). Com esta opção de não existir um capítulo específico e autónomo para revisão bibliográfica, pretende-se enriquecer os diversos capítulos com pontos de vista obtidos na bibliografia e com os defendidos pelo autor.

§ § §

No capítulo seguinte, a aplicação das metodologias de investigação ao tema da tese inicia-se com a revisão dos conceitos associados à Auditoria, aos SI e, consequentemente, à Auditoria de SI.

2 A AUDITORIA E OS SISTEMAS DE INFORMAÇÃO

Neste capítulo pretende-se efectuar uma abordagem global à primeira parte do título da tese ("A Auditoria de Sistemas de Informação"), para posteriormente nos Capítulos 3 e 4 se explorar os dois conceitos mais específicos relacionados com a segunda parte do título ("Modelo Funcional e Modelo de Competências").

2.1 DEFINIÇÕES

Esta secção tem por objectivo efectuar uma selecção de definições que contribuam para o esclarecimento de alguns conceitos fundamentais associados à Auditoria de SI. Estes conceitos, compilados sob a forma de tabelas, são apresentados em sequência lógica e relacionada.

Para alguns dos conceitos, designados com um só termo (como por exemplo, Informação, Controlo, Risco, etc.), será apresentada uma definição geral, ou seja, não contextualizada (extraída do dicionário da língua portuguesa). Para os conceitos compostos por vários termos (como por exemplo, Auditoria de SI, Controlos de SI, etc.), assim como para os conceitos de um só termo, será apresentada sempre uma ou mais definições contextualizadas (no domínio da Auditoria, dos Sistemas de Informação e das Organizações).

2.1.1 DEFINIÇÕES BASE

As designadas definições base efectuam a decomposição da expressão "Auditoria de Sistemas de Informação", apresentando sequencialmente a definição para cada um dos termos, para um sub-conjunto de termos e para a totalidade da expressão.

Conceito	Definição
Informação	Acto ou efeito de informar ou informar-se. Comunicação. Conjunto de dados, em princípio imprevisíveis, recebidos do exterior, ou por um ser vivo (especialmente o homem) por intermédio dos seus sentidos, ou por uma máquina electrónica. Elemento ou sistema que pode ser transmitido por um sinal ou uma combinação de sinais. O que é transmitido. (Porto Editora, 2007)
	Essentially, anything that can be digitized – encoded as a stream of bits – is information. (Shapiro and Varian, 1999)
	Information is understood as symbolic objects (opposed to material and energetic objects) deliberately built in order to enable communication and the formation of knowledge. As symbolic objects are used to represent other things they can also be called representations. (Carvalho, 2000)
	Informação é aquele conjunto de dados que, quando fornecido de forma e a tempo adequado, melhora o conhecimento da pessoa que o recebe, ficando ela mais habilitada a desenvolver determinada actividade ou a tomar determinada decisão. (Amaral e Varajão, 2000 citando Galliers, 1987)
	A Informação é tudo aquilo que, diminuindo o nosso grau de incerteza, ou indefinição, nos potencializa a racionalidade do processo de decisão, isto é, de administração e gestão. Daí que não possa haver Gestão sem Informação – a Informação e a Gestão são, afinal, os dois lados da mesma moeda. (Olivera, 1998/9)
	Information is a tool that adds value, builds competitive advantage and should be used to support management – it is not simply an overhead or functional system. (Marchand, 2000)
Sistema	Conjunto de partes dependentes umas das outras. Conjunto de leis ou princípios que regulam certa ordem de fenómenos. Em Informática, tudo o que é indispensável à execução de uma tarefa completa com a utilização de um computador: hardware, software e pessoas responsáveis pelo funcionamento correcto dos aparelhos. (Porto Editora, 2007)
	A system is a set of interdependent, goal-oriented and driven processes and related resources. *Virtually anything and everything in our real or conceptual world can be perceived as a system or at least as a part of one.* (Karapetrovic and Willborn, 2001)

	A system (in general or in abstract) can be defined as an active (does something), stable (has a structure) and evolutionary (that changes over time) thing or object that operates in an environment (it interacts with other things) with some purpose (from the point of the view of the modeller, there is a reason for the system to do what it does). *System is a concept that is useful to study active objects, especially when they are complex. A system is the result of viewing the active world from a certain point of view. Any thing (and specially an active thing) can be viewed as being a system.* (Carvalho, 2000)
Sistema de Informação	*Information system is either: (i) an active object that deals with (processes) information; or (ii) an active object whose purpose is to inform.* *The first interpretation focuses the nature of the processed objects. Information systems are systems that process only information, i.e., symbolic objects or representations.* *The second interpretation focuses on the purpose of the system. Information system is a system whose purpose is to inform, i.e., to contribute to someone's acquisition of knowledge. This knowledge is necessary to the execution of some action in some context.* (Carvalho, 2000)
	Sistema de Informação é um sistema que reúne, guarda, processa e faculta informação relevante para a organização de modo que a informação é acessível e útil para aqueles que a querem utilizar, incluindo gestores, funcionários, clientes, etc. Um Sistema de Informação é um sistema de actividade humana (social) que pode envolver ou não a utilização de equipamentos. (Amaral e Varajão, 2000 citando Buckingham, 1987)
	Conjunto de meios físicos e lógicos, humanos, financeiros, organizacionais e consumíveis diversos, que de uma forma racional interagem entre eles, se integram e se combinam com vista à produção, memorização e distribuição/consulta de Informação, com vista a satisfazer determinadas necessidades de gestão. (Oliveira, 1998/9)
Auditoria	Cargo de auditor. Tribunal ou repartição onde se exercem as funções de auditor. Em Economia, fiscalização da contabilidade e da gestão de uma empresa ou de um organismo; diagnóstico que visa analisar a gestão e a situação financeira de uma empresa ou organismo. (Porto Editora, 2007)
	Tem o objectivo de analisar o funcionamento parcelar ou global das organizações, para avaliar as deficiências de desempenho e sugerir vias de correcção e melhoramento. A auditoria não é um actividade meramente técnica que implique apenas a aplicação de certos procedimentos cujos resultados apresentam um indubitável rigor. (Carneiro, 2004)
Auditoria de Sistemas de Informação	A Auditoria de Sistemas não tem por objectivo apenas a função informática, focalizando-se em todos os SI, informatizados ou não, que existem na organização. A auditoria tem de concentrar os seus esforços na análise e avaliação, quer envolvendo-se em processos de planeamento, desenvolvimento, testes e aplicação de sistemas, quer examinando a estrutura lógica, física, ambiental, organizacional de controlo, segurança e protecção de dados. (Carneiro, 2004)

The IS audit activity should assist the organisation by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. (ISACA, 2005)
Information Systems Audit is the process of collecting and evaluating evidence to determine whether a computer system (Information System) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently. *Information Systems Audit is a part of the overall audit process, which is one of the facilitators for good corporate governance.* (Sayana, 2002)

Tabela 2.1 - Definições Base associadas à Auditoria de SI

Fonte: Citações compiladas pelo autor a partir das várias fontes indicadas

2.1.2 Definições Adicionais

As designadas definições adicionais complementam as definições base e esclarecem-nos sobre alguns dos conceitos relevantes que estão associados à Auditoria de SI, apresentando a definição para cada um dos termos e para alguns sub-conjuntos de termos.

Conceito	Definição
Controlo	Acção de controlar ou de dominar; domínio. Acto ou efeito de se dominar; autodomínio. Inspecção; fiscalização. Verificação de documentos ou serviços. Verificação do bom funcionamento (de uma máquina ou sistema). Teste escrito ou oral para verificação de conhecimentos. Vigilância exercida sobre o comportamento de alguém. (Porto Editora, 2007)
	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. *The policies, procedures, practices and organizational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.* (IIA, 2004 & 2007c)

	Um mecanismo de controlo ajuda a atingir o objectivo de um processo sem ser necessariamente parte do processo. Estes mecanismos são recursos que têm por objectivo, quando utilizados pelos processos, eliminar ou minimizar os riscos. É comum designar por sistema de controlo interno o conjunto de regras, políticas e procedimentos (mecanismos de controlo), envolvidos na gestão do risco empresarial. Um controlo é designado interno quando é um mecanismo interno de uma entidade. O controlo interno pode ser uma excelente ferramenta para que os objectivos de uma organização sejam atingidos. Contudo, a sua implementação necessita de uma *framework* coerente. (Santos, Vasconcelos e Tribolet, 2004)
Controlo de SI	*Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must establish an adequate system of internal control.* (ISACA, 2005)
	IT Controls are those controls that provide reasonable assurance of the secure, reliable and resilient performance of hardware, software, processes and personnel, as well as the reliability of the organization's information. (IIA, 2005a)
Risco	Possibilidade de um acontecimento futuro e incerto; perigo. (Porto Editora, 2007)
	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. (IIA, 2004)
	The possibility of an act or event occurring that would have an adverse effect on the organization and its information systems. (ISACA, 2007)
	Risk is a concept used to express uncertainty about events and/or their outcomes that could have a material effect on the goals of the organization. (McNamee and Selim, 1998)
Gestão de Risco	*Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.* *Risk Management processes identify, assess, manage, and control potential events or situations, to provide reasonable assurance regarding the achievement of the organisation's objectives.* (IIA, 2004)
Auditoria Interna	*Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.* (IIA, 2000)

	A Auditoria Interna tem um vasto âmbito de actuação, pretendendo-se que auxilie a equipa de gestão no seu desempenho de atribuições e responsabilidades, com base nas suas avaliações e recomendações. A Auditoria Interna é realizada com recursos materiais e pessoal da própria empresa auditada. Entende-se que a Auditoria Interna deva constituir uma função de avaliação independente, embora pertença à própria organização. (Carneiro, 2004)
	The internal audit department's mission is twofold: To provide independent assurance to the audit committee (and senior management) that internal controls are in place at the company and are functioning effectively; To improve the state of internal controls at the company by promoting internal controls and by helping the company to identify control weaknesses and develop cost-effective solutions for addressing those weaknesses. (Davis, Schillerand and Wheeler, 2007)
Auditoria Externa	A Auditoria Externa é realizada por entidades que não pertencem à empresa auditada, pretendendo-se, assim, uma maior objectividade relativamente à Auditoria Interna, devido ao maior distanciamento entre auditores e auditados. É, por vezes, designada como auditoria financeira, pois integra a análise das contas e das demonstrações financeiras. (Carneiro, 2004)
Auditoria Tecnológica	Tem por objectivo analisar as tecnologias mais importantes da cadeia de valor da organização, isto é, as tecnologias que mais influenciam a formulação das estratégias e a respectiva competitividade. As tecnologias são analisadas quanto ao seu grau de adequação aos objectivos da organização, à sua gama de produtos e aos mercados onde a mesma opera. (Carneiro, 2004)
Tecnologias de Informação	Numa perspectiva estritamente tecnológica, são o conjunto de equipamentos e suportes lógicos (hardware e software) que permitem executar tarefas como aquisição, transmissão, armazenamento, recuperação e exposição de dados. (Amaral e Varajão, 2000)
	Information Technology (IT) is the infrastructure that makes it possible to store, search, retrieve, copy, filter, manipulate, view, transmit and receive information. (Shapiro and Varian, 1999)
	Information Technology (IT) is all the computer hardware and software used to process information and provide communications, the process for administering and maintaining the technology and the human resources associated with the use of technology. (IIA, 2005a)
	In Information Technology (IT) the management focus is on infrastructure policies, standards and practices; the key issues include reliability, responsiveness, flexibility, ease of use and price/performance ratio. (Marchand, 2000)
Gestão da Informação	A Informação, como qualquer outro dos recursos vitais, deve ser gerida, pelo que deve constituir o cerne de um aérea funcional da gestão da organização a que comummente se chama de gestão da Informação. (Amaral e Varajão, 2000)

	A gestão da informação é entendida como a gestão eficaz de todos os recursos de informação relevantes para a organização, tanto de recursos gerados internamente como os produzidos externamente e fazendo apelo, sempre que necessário, à tecnologia de informação. (Braga, 2000)
	Information Management is business- and process-driven, and focuses on the use, quality and integrity of information. (Marchand, 2000)
Gestão de Sistemas de Informação	Gestão de Sistemas de Informação é a gestão do recurso Informação e de todos os recursos envolvidos no planeamento, desenvolvimento, exploração e manutenção do Sistema de Informação. (Amaral e Varajão, 2000)
Governo das Sociedades *(Corporate Governance)*	*Corporate Governance is the structure through which the objectives of an organization are set, and the means of attaining those objectives, and determines monitoring performance guidelines. Good corporate governance should provide proper incentives for board and management to pursue objectives that are in the interests of the company and stakeholders and should facilitate effective monitoring, thereby encouraging firms to use resources more efficiently.* (ISACA, 2007)
Governo dos SI (*IT Governance*)	*IT Governance is a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.* (ISACA, 2007)

Tabela 2.2 - Definições Adicionais associadas à Auditoria de SI

Fonte: Citações compiladas pelo autor a partir das várias fontes indicadas

2.1.3 Considerações sobre as Definições

Tal como é reconhecido por (Amaral e Varajão, 2000), "Informação, Tecnologias de Informação e Sistemas de Informação, apesar de serem termos banalizados na linguagem comum, são conceitos sem um entendimento universal", pelo que se sentiu a necessidade de efectuar a distinção e a clarificação destes e outros termos que lhes estão associados.

Desde logo, no que diz respeito à Informação, destacam-se as definições que a tomam como um activo que a organização possui, com a inerente propriedade de ter utilidade e valor, e que deve ser tratado como qualquer um dos outros bens.

Alerta-se também para a distinção do termo Sistema que possui um significado próprio e independente de SI (um SI é um Sistema, mas nem todos os Sistemas são de Informação).

Muitas vezes utiliza-se erradamente, como atalho, o termo Sistema para designar SI. Por outro lado, as definições apresentadas para SI reforçam o seu carácter sistémico que, não obstante a redundância, é muitas vezes ignorado quando se tomam os SI como Tecnologias de Informação, dado que estas últimas não possuem todas as características identificadoras de um Sistema.

Esta confusão entre as expressões SI e TI (Tecnologias de Informação) é agravada pela correntemente aceite e generalizada (mas incorrecta!) utilização na língua inglesa da expressão *IT (Information Technology)* para designar os *IS (Information Systems)*. Cientes desta limitação, no presente texto, sempre que apareça em designações ou citações em língua inglesa, interpretaremos a expressão *IT* como sendo SI em português.

Para finalizar a argumentação sobre a correcta utilização da expressão SI, recorreu-se a um texto de (Oliveira, 1997) onde este afirma que "qualquer sistema informático está contido num SI". O conceito de sistema informático, entenda-se Tecnologias de Informação, "apenas cobre uma parte da problemática inerente ao SI". Sempre existiram SI, mesmo quando não existiam Tecnologias de Informação. Aliás, (Oliveira, 1998/9) observa que "o primeiro tratado sobre SI tem mais de cinco séculos" (é um tratado sobre um sistema matemático, datado de 1494).

Agregando então os conceitos de Informação e de Sistema, bem como a utilidade da sua existência nas organizações, temos a chamada abordagem de SI ("*information system approach"),* referida por (Oliveira, 1998/9) como sendo uma "exigência arquitectural que priviligie o fluxo de Informação ao longo da pirâmide organizacional ou ao longo do processo produtivo". Daqui também se deriva a necessidade de se efectuar a Gestão da Informação.

As definições apresentadas de Auditoria e de Gestão de Risco, com os seus indissociáveis conceitos de Risco e de Controlo, deixam transparecer que são considerados como instrumentos de Governo das Sociedades e, como iremos ver mais à frente, cada vez mais também como instrumentos de Governo dos SI.

No que se refere às definições de Auditoria apresentadas, importa perceber a existência de diversos tipos de Auditoria (Interna, Externa, Tecnológica, entre outros aqui não referenciados). O

presente texto centra-se fundamentalmente na Auditoria de SI enquanto parte integrante da Auditoria Interna. Não obstante, os princípios fundamentais da Auditoria Interna são os mesmos da Auditoria Externa, pelo que também são aplicáveis aos casos em que a função Auditoria de SI é da responsabilidade da Auditoria Externa (casos menos frequentes nas grandes organizações). Num contexto em que as organizações baseiam cada vez mais os seus processos produtivos em SI e em Tecnologias, é legítimo afirmar que a Auditoria de SI também pode integrar os objectivos da Auditoria Tecnológica.

2.2 REFERÊNCIAS À EVOLUÇÃO DA FUNÇÃO AUDITORIA

Nesta secção são efectuadas breves referências à evolução da função Auditoria. Espera-se que contribua para a percepção do modo como a Auditoria de SI surgiu e se desenvolveu a partir de uma Auditoria mais generalista, como por exemplo a Auditoria Interna, e tornar evidente que a Auditoria de SI continua a fazer parte integrante e a basear-se nos principais fundamentos daquela.

2.2.1 A EVOLUÇÃO DA FUNÇÃO AUDITORIA

O termo Auditoria remonta aos tempos medievais, altura em que, em algumas fazendas privadas e nos estados feudais, os registos contabilísticos do governo eram aprovados em audiência pública, sendo as contas lidas e ouvidas em voz alta. Neste contexto, encontrámos o significado original da palavra Auditor que provém do vocábulo "*audire*" e que significa ouvir. Segundo (Geada, 2005), existem registos de actividades de Auditoria datados de 3000 AC e também da designada China antiga, Grécia e Roma. Nesta última, os auditores ouviam os contribuintes e elaboravam registos públicos tendo em conta os negócios e as taxas devidas.

De acordo com o levantamento histórico efectuado por (Díaz y Vera, 2006), por volta dos séculos XIII e XIV, existem evidências de que em Inglaterra se auditava a gestão dos funcionários públicos responsáveis pelos fundos estatais, bem como as operações de algumas actividades privadas (este foco na Auditoria às operações só iria reaparecer por volta de 1950!). Nos

princípios do século XIX, o desenvolvimento empresarial provocado pela Revolução Industrial potencia a actividade da Auditoria. Até finais do século XIX, esta actividade tinha como principais objectivos a detecção de fraudes e os aspectos contabilísticos. Na primeira metade do século XX, os objectivos da Auditoria reposicionam-se para determinar e opinar sobre se os relatos financeiros das organizações representam correctamente a sua situação financeira e os resultados operacionais. A partir das décadas de 1940 e 1950, o conceito de Auditoria Interna começa a afirmar-se, passando o Controlo Interno a ter um papel chave na Auditoria das grandes organizações. A função Auditoria inicia então uma evolução em paralelo com os objectivos das modernas organizações empresariais. A gestão destas organizações sentia uma necessidade cada vez maior de possuir mecanismos que lhe permitissem confiar nas demonstrações financeiras publicadas, recorrendo a inspecções efectuadas por funcionários da própria organização (Auditoria Interna), como complemento às inspecções efectuadas externamente (Auditoria Externa). A partir da década de 1980, a função da Auditoria vê o seu âmbito alargar-se progressivamente, passando a incluir análises de controlos administrativos e também análises à eficiência e eficácia das operações e da utilização dos recursos. Passa a existir uma maior cooperação entre Auditoria Interna e a Externa. Por último, na década de 1990, a função Auditoria atinge um último patamar, mais abrangente e sistemático, em que a sua actividade se baseia na identificação e gestão dos riscos das organizações.

Em termos de marcos institucionais ou metodológicos relevantes para a actividade da Auditoria, (Cangemi, 2003) identifica a primeira Auditoria Externa efectuada por um funcionário público em 1720 em Inglaterra e o facto do no *British Companies Act* de 1844 constar a obrigatoriedade de se efectuarem Auditorias Financeiras às empresas financiadas por accionistas. O primeiro documento formal com princípios geralmente aceites e standards aplicados à Auditoria, "*Approved Methods for the Preparation of Balance-Sheet Statements"*, foi elaborado em 1918 na América. Em 1941, publica-se o primeiro grande compêndio sobre Auditoria, "*Internal Auditing* " do autor Victor Z. Brink, e ocorre a fundação da maior associação mundial de Auditores, o IIA - *The Institute of Internal Auditors*. O jornal/revista desta Associação, o *Internal Auditor*, publica em 1948 o artigo "*Audits of Operations*" onde pela primeira vez é explicitamente descrito este âmbito mais alargado da Auditoria, relacionado com os processos das operações das organizações. Em 1957, numa revisão do "*Statement of Responsabilities of Internal Auditing*", o

IIA refere neste documento formal que o Auditor dever-se-á preocupar com toda e qualquer fase da actividade da organização. Está aberto o caminho para que os futuros Sistemas de Informação possam também caber no âmbito das Auditorias.

Como fenómeno paralelo à evolução geral da Auditoria, desde a década de 1950 até aos nossos dias, assiste-se a um surgimento progressivo de segmentos de Auditoria, ou seja, tipos de Auditoria focados em determinadas funções ou áreas da organização. Para além da divisão entre a Auditoria Interna e a Externa, e das mais generalizadas Auditoria Financeira e Auditoria de Fraude, surgem a Auditoria da Qualidade, a Auditoria do Ambiente, a Auditoria de Processos de Negócio, etc. Começam a surgir também Auditorias associadas a activos intangíveis ou imateriais, como seja a Auditoria da Informação.

2.2.2 A Evolução da Função Auditoria de SI

O desenvolvimento da Auditoria de SI está em primeiro lugar relacionado com a necessidade de, em determinado momento, se passarem a efectuar Auditorias à própria Informação. O já referido estudo de (Díaz y Vera, 2006), situa as origens da Auditoria da Informação na década de 1970 e inícios de 1980, acompanhando o desenvolvimento nas áreas das ciências da informação, das ciências económicas e das tecnologias de informação e comunicação. A primeira referência explícita ao termo Auditoria da Informação encontra-se datada de 1982. Com o prosseguir das décadas de 1980 e 1990, devido à proliferação dos estudos de mercado, dos consumidores e das suas necessidades, no âmbito das ciências económico-sociais, as práticas de Auditoria da Informação consolidam-se em algumas grandes organizações. Com a aplicação destas práticas, começa a surgir também o conceito de Gestão da Informação que foi alavancado, entre outros factores, pelo ênfase que as grandes organizações colocavam nos SI associados às áreas financeiras e de contabilidade e, por outro lado, pela crescente necessidade que sentiam em valorizar, ou seja, atribuir valor aos seus recursos de Informação. Neste contexto, a Auditoria da Informação passou a incluir no seu âmbito não só a identificação das fontes, dos serviços e dos sistemas, mas também a avaliação de como estes são utilizados, a sua relação com as actividades críticas do negócio e o seu alinhamento com os objectivos estratégicos da organização.

No fundo, podemos dizer que a Auditoria da Informação deixou de estar centrada em si própria, (ou seja, estritamente na Informação), passando a estabelecer elos de ligação com as necessidades da organização e com os Sistemas de Informação que as suportam.

No compêndio de (Cangemi, 2003) sobre a função de Auditoria numa grande empresa, no capítulo relativo à história da Auditoria de SI ("*History of Information Systems Auditing*"), podemos encontrar uma afirmação que posiciona o estado de desenvolvimento da função Auditoria com as respectivas competências do Auditor:
"*It was possible for an auditor to retire in the 1950s having used similar audit programs throughout one's career. That will never happen again! The effects of IT on auditing have culminated in a set of knowledge skills and standards necessary to conduct the contemporary audit that were nonexistent...*"

Ainda segundo (Cangemi, 2003), no período aproximado entre 1955 a 1965, constatava-se que as tecnologias de informação das organizações eram baseadas apenas em computadores centralizados (*mainframes*), com os seus inerentes e proprietários mecanismos de segurança. Apenas um conjunto de pessoas muito restrito tinha conhecimentos para poder violar o sistema, pelo que os próprios auditores também não tinham as competências adequadas para os auditar, nem reconheciam a necessidade de fazê-lo. Com a crescente computorização nas grandes organizações, os Auditores ficaram também cada vez mais dependentes das capacidades (*skills*) de terceiros, dos técnicos especializados em processamento electrónico de dados (*EDP - Electronic Data Processing*), pelo que o acesso à informação estava a escapar-lhes. Paradoxalmente nesse mesmo período começavam a surgir artigos em que os Auditores reconheciam as potencialidades que as tecnologias de informação poderiam ter para serem usadas, elas próprias, como um meio de auditar a informação financeira, levando assim ao desenvolvimento de software para Auditoria (designado como *GAS - Generalized Audit Software* ou como *CATT - Computer Aided Audit Tools*). A ferramenta *AUDITAPE* foi a pioneira em 1967. A partir de 1980 até aos nossos dias, com a massificação do uso dos computadores pessoais em contexto empresarial, existem várias ferramentas do tipo *CAAT* que se generalizaram a nível

mundial, entre as quais as duas mais conhecidas actualmente no meio profissional da Auditoria: *IDEA* (*Interactive Data Extraction and Analysis*) e *ACL* (*Audit Control Language*).

No que diz respeito a marcos institucionais ou metodológicos relevantes para a actividade da Auditoria de SI, (Asthon, 2001) identifica a primeira norma (*standard*) geralmente aceite, publicada nos EUA em 1983 pelo *Department of Defense*, vulgarmente conhecida como *The Orange Book* e intitulada de "*DOD STD - Trusted Computer System Evaluation Criteria (TCSEC)*". Dado que a Segurança dos SI foi o primeiro dos domínios da Auditoria de SI a ser explorado, esta norma tratava de medidas de salvaguarda dos computadores com vista à protecção de informação classificada, existente em ambientes com acesso remoto e sistemas com partilha de recursos. Outros marcos importantes são também referidos por (Cangemi, 2003): a fundação em 1969 nos EUA da *EDPAA - Electronic Data Processing Auditors Association* ; a publicação em 1977, por esta Associação, da primeira edição dos *Control Objectives* ("*compilation of guidelines, procedures, best practices and standards for EDP Audits"*); várias revisões deste documento, entre as quais a de 1996 em que foi renomeado para *CobiT - Control Objectives for Information and related Technology* ; e a introdução em 1978 de um programa de certificações para Auditores de SI, iniciado com a certificação *CISA - Certified Information Systems Auditor*.

2.2.3 A Evolução do Papel do Auditor

A tabela apresentada de seguida pretende sistematizar a evolução da Auditoria ao longo de 4 Eras relacionando-as com algumas das características que compõem o papel a desempenhar pelo Auditor. Foi construída partindo desta ideia base apresentada por (Fretwell, 2004):
"*Auditing has always been comparing 'what is' to 'what should be'. But 'how' and 'what' has changed over time.*"

De facto, como poderemos perceber pelos papéis do Auditor detalhados na tabela, o modo de exercer a Auditoria ("como?") e os objectos alvo da Auditoria ("o quê?") foram evoluindo ao longo das 4 Eras, desde a Era da Inspecção, passando pela Era do Controlo, pela presente Era do Risco e pela próxima Era da Auditoria Contínua.

A ERA DA AUDITORIA:	**O PAPEL DO AUDITOR:**
A Auditoria baseada na **Inspecção**	▪ Auditores focados na inspecção e na recontagem. ▪ Auditores focados nos testes substantivos (provas suficientes e convincentes sobre as transacções).
A Auditoria baseada no **Controlo**	▪ Auditores focados na adequação aos controlos e às políticas definidas. ▪ Auditores começam a executar auditorias operacionais. ▪ Auditores começam a encarar a Auditoria de uma forma mais abrangente, como estando ao serviço da Gestão da organização.
A Auditoria baseada no **Risco**	▪ Auditores focados na mitigação dos riscos verificando a definição e a execução dos controlos ao nível das entidades e dos processos de negócio. ▪ Auditores não assumem à partida que os controlos implementados são os mais adequados. ▪ Auditores encaram o risco de forma holística, muito para além dos riscos associados aos financeiros (passam a incluir, por exemplo, os riscos associados aos Sistemas e Tecnologias de Informação.)
Factores que potenciam a evolução:	▪ Auditores perante legislações com *reportings* exigentes e abrangentes (ex: Sabarnes-Oxley). ▪ Auditores perante elevado ritmo de mudança do negócio e Tecnologias cada vez mais complexas. ▪ Auditores efectuam mais Auditorias aos Sistemas e Tecnologias que resultam em *findings* muito técnicos, dificultando a sua compreensão e necessária acção por parte da Gestão da organização. ▪ Auditores lidam com activos intangíveis que representam maior proporção do valor da empresa.
A Auditoria **Contínua** (no futuro próximo)	▪ Auditores obrigados a providenciarem relatórios de conformidade de forma independente mas cada vez mais rápida e contínua. ▪ Auditores obrigados a desenvolverem e implementarem sistemas de monitorização que permitam um contínuo *risk assessment* e consequente actualização do plano e das prioritizações das Auditorias. ▪ Auditores obrigados a detectarem e a reportarem aos Comités de Auditoria e aos Accionistas de forma quase imediata as violações ou quebras nos controlos. ▪ Auditores obrigados a acompanharem o elevado ritmo de mudança nos negócios, que tornam os *risk assessments* com periodicidade apenas anual inadequados no tempo e rapidamente obsoletos. ▪ Auditores necessitam de compreender os crescentes riscos associados à Informação e aos Sistemas e Tecnologias de Informação e Comunicação. ▪ Auditores recorrem à contratação de especialistas externos em Tecnologias. ▪ Auditores intensificam o uso das *IT audit tools and techniques*. ▪ Auditores necessitam de adaptar os *risk assessments* para incorporar os riscos associados aos Sistemas que gerem activos intangíveis: *Customer Relationship, Human Capital, Brand Management, Knowledge Capital,* etc. ▪ Auditores necessitam de compreender e consolidar os *inputs* de várias iniciativas na organização que efectuam *risk assessments*:: *Internal Audit, Internal Control & Compliance, Enterprise-Wide Risk Management, Business Continuity Management, Sabarnes-Oxley, Corporate Social Responsability, etc.*
Competências necessárias à evolução:	▪ Auditores melhorarem competências de comunicação e de facilitação do processo de Auditoria. ▪ Auditores com maior formação base, incluindo mais MBA's e graduações em Sistemas. ▪ Auditores com maior formação específica, incluindo certificações e especializações tecnológicas. ▪ Auditores com conhecimento operacional e de negócio para potenciar a melhoria contínua. ▪ Auditores adquirirem competências de Sabarnes-Oxley *compliance* e de detecção de Fraude. ▪ Auditores terem liberdade de responder directamente aos Comités de Auditoria independentes, reduzindo a influência da Gestão da organização nos processos de Auditoria.

Tabela 2.3 - As Eras da Auditoria vs. o Papel do Auditor

Fonte: Elaborado e compilado pelo autor a partir de vários conceitos apresentados por (Fretwell, 2004): "*The Changing Role of the Internal Auditor*"

Não dispensando uma leitura mais atenta dos conteúdos da tabela anterior, poderemos identificar, desde já, uma ideia chave: o papel do Auditor tem evoluído e de forma positiva. Partindo de um Auditor preocupado com "o passado" (Era da Inspecção), passou-se para um Auditor preocupado com "o presente" (Era do Controlo), agora preocupado com "o futuro" (Era do Risco) e, cada vez mais, preocupado de "forma permanente" (Era da Auditoria Contínua).

Sem situar cronologicamente as diferentes Eras, é relativamente consensual nos meios profissionais da Auditoria, admitir que esta se encontra actualmente na Era do Risco. Existem, contudo, já algumas práticas que a posicionam na entrada da Era da Auditoria Contínua.

Destacam-se alguns factores que têm potenciado a evolução para esta Era, como sejam o crescente ritmo de mudança dos negócios, das Tecnologias e dos SI, com uma consequente maior proporção dos activos intangíveis nas organizações (incluindo a Informação e o conhecimento Humano). Paralelamente, são cada vez mais abrangentes as exigências de Informação pública, favorecidas por fenómenos como o *Sarbanes-Oxley Act*, publicado em 2002 pela entidade reguladora do mercado financeiro dos EUA. Esta legislação para empresas cotadas, tem impacto nas Auditoria Financeiras, mas também nas Auditorias Operacionais e de SI pois regula os registos financeiros, define tipos de Informação que têm de ser guardados e por quanto tempo, tem implicações no planeamento e na capacidade de armazenamento de dados, etc. Por outro lado, esta legislação surgiu na sequência de uma série de incidentes com a Informação financeira de algumas grandes empresas nos EUA, o que levou inclusivamente à extinção/separação das empresas de Consultoria das empresas de Auditoria (como por exemplo a *Arthur Andersen*), no sentido de garantir maior independência para a função Auditoria.

Estas evoluções da Auditoria requerem um acompanhamento das competências dos Auditores, com conhecimentos técnicos e especializados mais aprofundados (formações, certificações, etc.) mas cada vez mais, também, com conhecimentos abrangentes (gestão, comunicação, etc.).

Na secção seguinte, relativa ao paradigma actual da função Auditoria, são desenvolvidos alguns dos aspectos da actual Era (Auditoria com visão holística e baseada no risco) e também da Era que se está a iniciar (Auditoria com soluções de melhoria contínua).

2.3 O PARADIGMA ACTUAL DA FUNÇÃO AUDITORIA

Nesta secção é efectuada uma exploração de três dos principais factores caracterizadores do paradigma actual da função.

2.3.1 VISÃO HOLÍSTICA

Nos EUA, em 1987, uma comissão patrocinada por 5 grandes organizações relacionadas com a contabilidade e a Auditoria, conhecida como COSO - *Commmittee of Sponsoring Organizations,* elaborou o chamado *Treadway Comission Report* que concluiu que uma função de Auditoria Interna deveria existir em todas as empresas públicas e que deveria existir um Comité de Auditoria Corporativo, constituído por administradores/directores com funções não executivas (para garantir independência). Este relatório foi considerado um marco e contribuiu decisivamente para:

- A consolidação/desenvolvimento da missão e do papel da função de Auditoria Interna, tornando-a necessária e, por vezes, obrigatória.
- A introdução de uma visão holística da Auditoria, ao definir um carácter multi-dimensional quanto ao âmbito.
- A introdução de uma abordagem baseada no risco para a Auditoria, ao definir práticas de avaliação de risco (*risk assessment*).

Dos três pontos atrás indicados, destacamos, por agora, o segundo relativo à visão holística da Auditoria. O terceiro ponto, relativo à abordagem ao risco, está também muito relacionado com o segundo, pelo que mais à frente será devidamente desenvolvido.

A figura seguinte é habitualmente conhecida como o Cubo COSO (*COSO's framework*), sendo apresentada a sua versão mais recente (IIA, 2007b). A versão original (*Internal Control Framework*) possuía 5x3x4 dimensões mas a versão actual (*Risk Management Framework*) possui 8x4x4. Verificou-se uma expansão com a introdução de mais linhas e mais colunas nas faces frontal e superior do cubo, sendo que a face lateral manteve-se mas passou a ser menos

genérica, concretizando agora 4 níveis organizacionais. Estes factos são sintomáticos da evolução de uma visão de Controlo Interno para uma visão de Gestão de Risco e também do carácter multi-dimensional da Auditoria, pois cada vez se vai identificando mais dimensões para o seu âmbito.

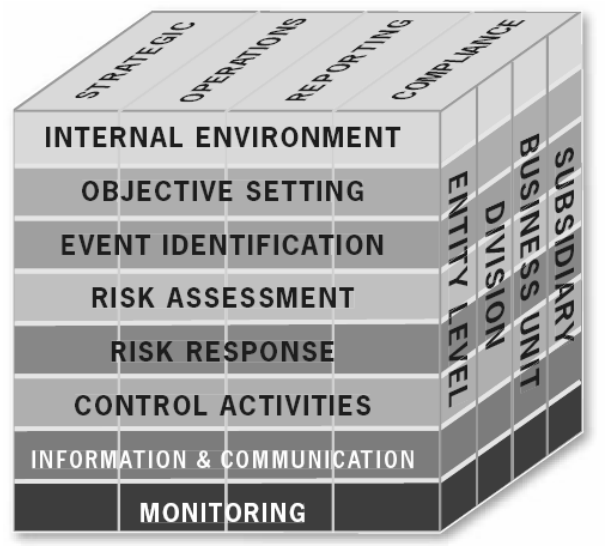


Figura 2.1 - Visão Holística da Auditoria: as Dimensões do Risco

Fonte: Versão original extraída de (IIA, 2007b): "*COSO's Framework*"

Embora este modelo estruturado (*framework*) tenha sido pensado genericamente para actividades de Gestão de Risco, devido ao facto da Auditoria ter adoptado uma abordagem baseada no risco, possui conceitos essenciais a ser considerados pelas actividades de Auditoria.

De acordo com este modelo (IIA, 2007b), na face do topo do cubo, encontrámos as 4 categorias de objectivos que a gestão da organização define e que a Auditoria deve abordar: os Estratégicos (alto nível, alinhados com a missão e a visão); os Operacionais (uso eficaz e eficiente dos recursos); os de Relato (fiabilidade dos relatórios); e os de Conformidade (com as leis e regulamentos).

A Auditoria deverá verificar que os objectivos atrás enunciados estão integrados em todos os processos de gestão da organização. Na face frontal do cubo, estão indicados 8 componentes que se interrelacionam e que a Auditoria deve considerar: a Envolvente Interna (estabelecimento

de uma cultura e nível de risco desejado); a Definição de Objectivos (considerar o nível de risco nos objectivos); a Identificação de Ocorrências (internas ou externas que representem um risco ou uma oportunidade para a organização); a Avaliação do Risco (qualificação e quantificação da probabilidade e do impacto dos riscos); a Resposta ao Risco (escolher a forma de mitigar o risco e definir acções de resposta); as Actividades de Controlo (controlar a execução e eficácia das acções de reposta ao risco); a Informação e Comunicação (atempada e abrangente, para garantir que os papeis e responsabilidades de gestão dos riscos são executados eficazmente); e a Monitorização (monitorização contínua dos riscos face às mudanças).

Por fim, a Auditoria pode trabalhar em diferentes níveis organizacionais, tal como é visível na face lateral do cubo: nível da Entidade (por ex. empresa/ *holding*); nível da Divisão (por ex. departamentos); nível da Unidade de Negócio (por ex. tipos de negócio); e nível da Subsidiária (por ex. empresas/ *sub-holdings*).

A visão holística anteriormente apresentada para a Auditoria em geral pode ser transposta para as especificidades da Auditoria de SI. O *Global Technology Audit Guide – IT Controls* do (IIA, 2005a) apresenta uma aplicação do modelo COSO (versão *Internal Controls*) para os SI.

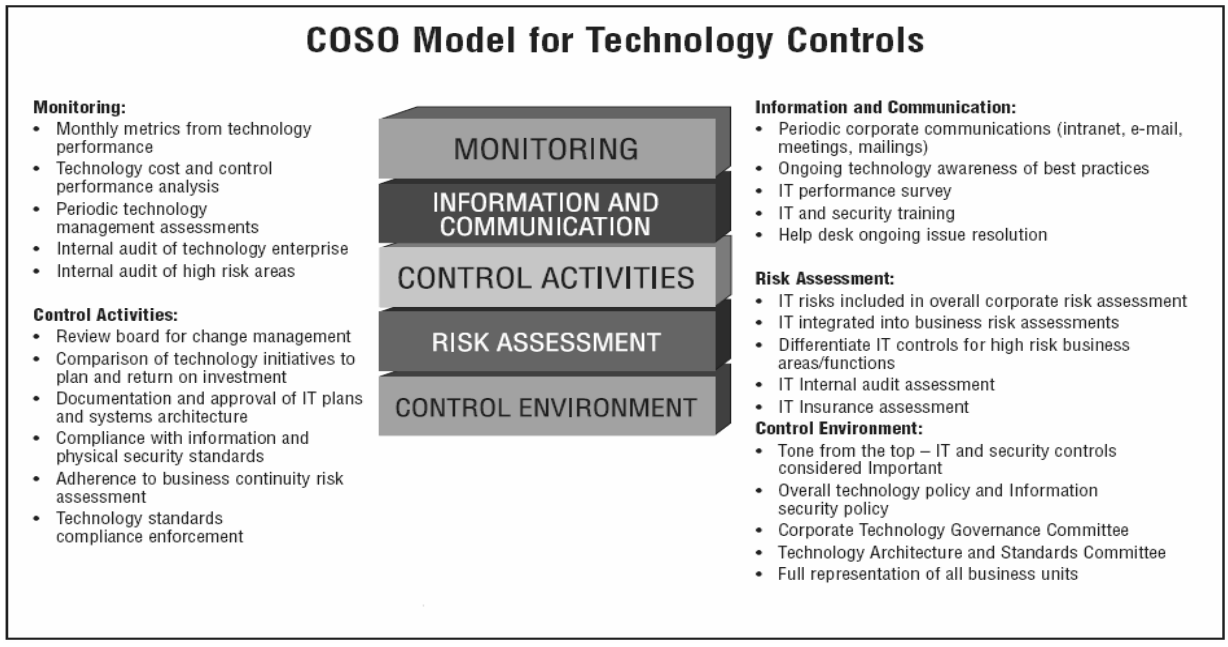


Figura 2.2 - Visão Holística da Auditoria: os Controlos de SI

Fonte: Versão original extraída de (IIA, 2005a): "*COSO Model for Technology Controls*"

Apesar de no Capítulo 3 se descreverem com maior pormenor os objectivos, o âmbito e os referenciais metodológicos, este modelo estruturado permite-nos reforçar a visão holística da Auditoria de SI. De facto, a actividade desta pode ser bastante abrangente, se considerarmos auditar os diversos domínios de Controlo Interno que o modelo prevê em 5 grandes componentes: o Ambiente de Controlo (organização, políticas e níveis dos controlos a aplicar às tecnologias e aos SI); a Avaliação do Risco (riscos e controlos que são específicos dos SI); as Actividades de Controlo (aplicação dos controlos de SI pela organização utilizando metodologias de análise, normas e boas práticas de SI); a Informação e Comunicação (cultura e divulgação dos controlos de SI da organização) e a Monitorização (medições, análises e avaliações do desempenho dos SI face aos seus controlos).

2.3.2 Auditoria baseada no Risco

Um estudo efectuado por (McNamee and Selim, 1998), intitulado *Risk Management: Changing the Internal Auditor's Paradigm*, identificou uma mudança significativa no paradigma da Auditoria: de passiva, reactiva e baseada em controlos, passou para activa, proactiva e baseada em riscos. Este estudo, patrocinado pelo *The Institute of Internal Auditors*, chegou àquela conclusão através da análise aos processos de Auditoria de 29 organizações de alto desempenho (*top performers*) de diversos países e diversos sectores de actividade públicos e privados. Este novo paradigma reconhece que o risco é um dos motores da actividade das organizações e que os processos de Governo das Sociedades (*Corporate Governance*) são a resposta estratégica das organizações ao risco.

Embora as respostas das organizações aos riscos sejam específicas ao sector em que actuam, podemos dizer que elas devem passar, hoje em dia, por usar e relacionar conjuntamente dois instrumentos de Governo das Sociedades (*Corporate Governance*): a Auditoria e a Gestão de Risco.

Ainda segundo (McNamee and Selim, 1998), estes dois instrumentos atrás mencionados têm evoluído em conjunto, beneficiado da crescente importância que o tema dos riscos globais de

negócio tem assumido no domínio do Governo das Sociedades (*Corporate Governance*). Neste contexto, a natureza do conceito de risco têm-se tornado mais alargada, ao ponto do planeamento anual das Auditorias estar cada vez mais relacionado com o planeamento anual dos negócios, sendo os factores de ligação entre aqueles dois planos os riscos que são considerados estratégicos para o negócio. Ao garantirmos a ligação entre aqueles dois planos anuais, estamos a garantir que os riscos presentes (não os passados) são analisados e, por consequência, que se está a obter valor acrescentado dos processos de Auditoria, alterando o seu foco do passado em direcção ao presente e ao futuro. Contrariamente ao que acontecia quando o Auditor se confinava à verificação dos detalhes dos controlos das transacções passadas, neste novo paradigma quando o Auditor se foca nos riscos das transacções presentes e futuras, ele está a trabalhar a um nível superior ao detalhe e a identificar obstáculos que impedem a organização de atingir os objectivos.

Não poderíamos terminar as referências a este estudo sem alertar para o facto da evolução de paradigma implicar também uma evolução ao nível das competências que o Auditor deve possuir. O Auditor especializado na verificação de controlos pode não ter a experiência necessária à identificação de todos os riscos relevantes. Um Auditor compatível com o novo paradigma necessita de competências com cariz mais estratégico, como sejam, por exemplo, a visão, o planeamento e a comunicação. Por outro lado, o Auditor deve afastar-se duma perspectiva meramente financeira para uma perspectiva mais abrangente e de gestão. Esta posição está alinhada com a seguinte afirmação de (Cangemi, 2003):
"*The main objective of the Internal Audit function has moved from that of fraud detection to assisting management in making decisions beginning with a risk assessment.*"

A avaliação dos riscos (*risk assessment*) é precisamente uma das primeiras etapas que se aconselha no contexto deste paradigma de Auditoria ou pode, também, ser uma das fases dos chamados Ciclos de Gestão de Risco. Na figura seguinte, apresenta-se uma possível abordagem para um Ciclo de Gestão de Risco aplicado aos SI. As 5 fases, sequenciais e cíclicas, estão representadas no gráfico circular na parte inferior da figura. Cada uma destas fases é constituída por um conjunto de actividades que estão decompostas e mapeadas na figura.

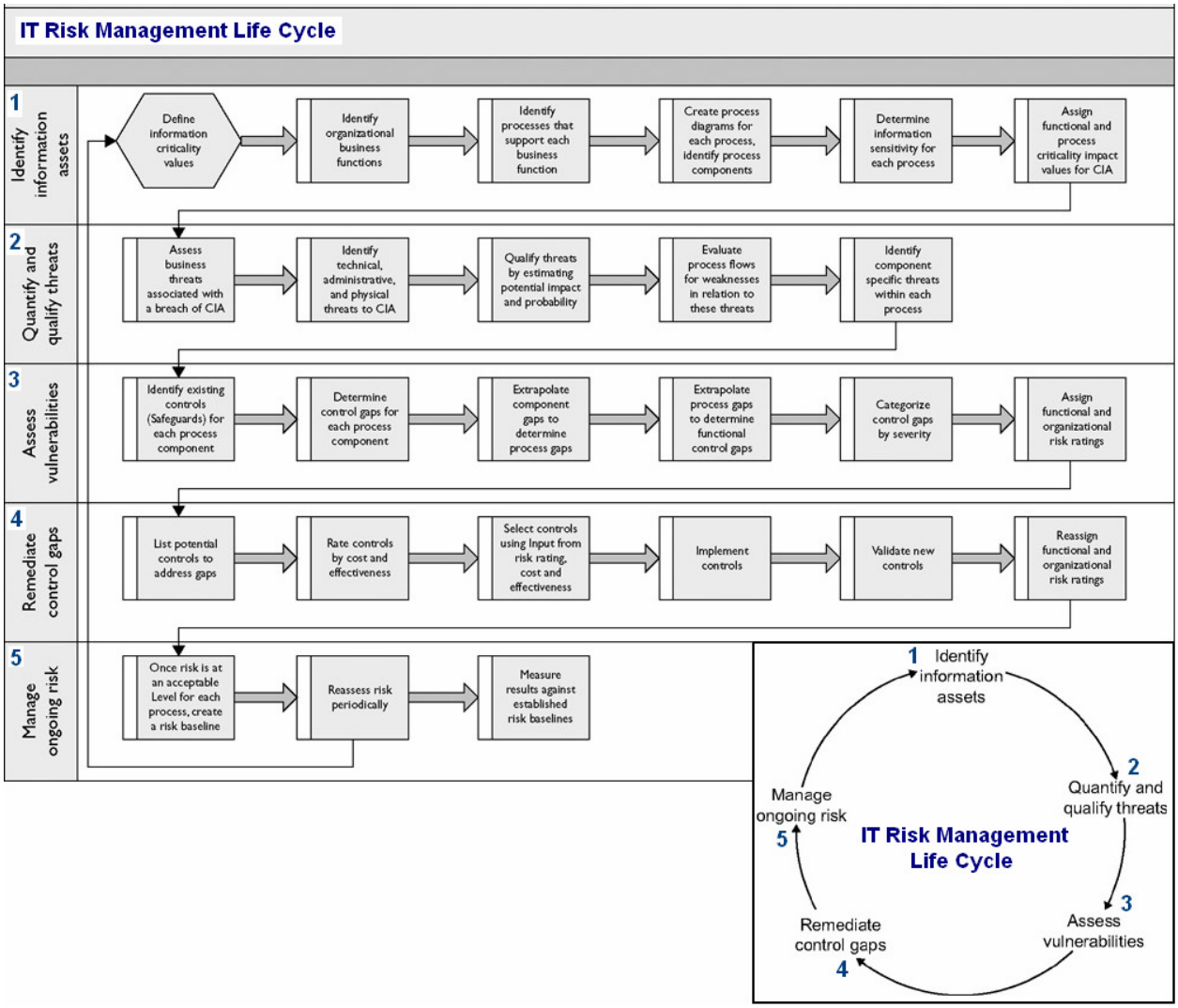


Figura 2.3 - *Framework* de Gestão de Risco de SI

Fonte: Adaptado das versões originais de (Davis, Schillerand and Wheeler, 2007):

"*IT Risk Management Lifecycle" & "Risk-management process*"

Nesta metodologia apresentada por (Davis, Schillerand and Wheeler, 2007) a avaliação dos riscos inicia-se com as duas fases em que se identificam os activos de Informação (Fase 1) e se quantificam e qualificam as ameaças (Fase 2) e completa-se com a análise de vulnerabilidades (Fase 3). Após a avaliação, há que focar na mitigação dos riscos associados às falhas com maior vulnerabilidade, através de actividades do controlo à correcção das falhas (Fase 4) e da gestão contínua do risco (Fase 5).

Para cada uma das fases deste Ciclo de Gestão de Risco, iremos destacar algumas das actividades e respectivos conceitos que poderão/deverão ser considerados e aplicados numa Auditoria de SI baseada no risco.

Na identificação dos activos de Informação (Fase1), a abordagem aconselhável para efectuar essa identificação é do topo para a base (*top-down*): Funções de negócio → Fluxos de Informação dos processos → Componentes do processo. Começa-se por identificar as funções de negócio da organização, seguem-se os processos que suportam essas funções e, por fim, desce-se ao nível (*drill-down*) dos activos de Informação que são processados. É necessário definir valores de criticidade para a Informação (por exemplo, Alto, Médio, Baixo), devendo estes corresponder a uma escala que represente a criticidade da falha de um desses activos. Uma vez que, por natureza, os SI processam Informação, a identificação dos riscos de SI possui uma complexidade agravada pois devemos considerar todos os potenciais activos de Informação que atravessam um determinado processo. Note-se que, neste ponto, não devemos estar ainda preocupados com a tecnologia utilizada para processar a Informação, mas apenas com o processo. Só posteriormente deveremos identificar os passos manuais ou as tecnologias que são utilizadas no processo.

Na quantificação e qualificação das ameaças (Fase 2), devem-se identificar os riscos e quantificar os respectivos impactos. Devem ser considerados todos os tipos de riscos associados directa e indirectamente à Informação e aos SI que a suportam, como por exemplo: financeiros (perda de Informação proprietária, perda de produtividade, etc.); legais (perda de informação confidencial, etc.); administrativos (*social engineering*, eliminação acidental de dados, etc.); técnicos (intrusão em sistemas, vírus, etc.); físicos (fogo, interrupção de energia, etc.). A quantificação das ameaças deve ser o resultado do produto de dois factores: a probabilidade (da ameaça se concretizar) e o impacto (que a concretização provoca). A probabilidade deve ser quantificada através de uma taxa anual de ocorrência (*Annual Rate of Occurrence*) e o impacto através de um factor de exposição (*Exposure Factor*).

Na análise de vulnerabilidades (Fase 3), o foco são processos de Informação, ao contrário da fase anterior, relativa às ameaças, em que o foco são activos de Informação. Para analisar as

vulnerabilidades, deveremos adoptar uma abordagem da base para o topo (*bottom-up*): Vulnerabilidades das componentes do processo → Vulnerabilidades do processo → Vulnerabilidades da função de negócio. Esta abordagem inicia-se com a revisão das ameaças identificadas anteriormente (incluindo a inventariação dos controlos existentes) e segue-se a determinação das falhas aos controlos (incluindo uma avaliação da eficácia de cada controlo). Agregando sucessivamente as diversas falhas de controlo ao nível das componentes, dos processos de Informação, das funções de negócio e da organização como um todo, podemos determinar uma classificação de risco (*rating*) para cada um destes níveis, no que diz respeito à Informação e aos SI que a suportam.

No controlo à correcção das falhas (Fase 4), procede-se à escolha dos controlos (decisão de negócio baseada numa relação custo/benefício), à sua implementação (nos processos de Informação e nos SI), à sua validação (por exemplo, através de Auditorias periódicas aos SI) e, por fim, recalculam-se as classificações de risco (*ratings*) tendo em conta o risco residual (ou seja, o risco que resta após a sua mitigação com a implementação dos controlos).

A gestão contínua do risco (Fase 5) traduz-se pela criação de um referencial de risco (*risk baseline*), a partir do qual se poderão efectuar comparações quando ocorrem mudanças na organização e nos SI, de modo a determinar alterações no nível de risco (*risk rating*). Dada a natureza dinâmica dos SI, o ciclo deverá ser realizado periodicamente ou despoletado sempre que exista alguma mudança profunda (novas arquitecturas de sistemas, alterações em funções chave de negócio, regulamentações que imponham novos controlos, etc.).

Como resumo, poderemos dizer que a Gestão dos Riscos deverá, no mínimo, passar por 3 etapas fundamentais: a avaliação dos riscos (*risk assessment*) que agrega as Fase 1, 2 e 3; o controlo dos riscos (*risk controlling*) que corresponde à Fase 4; e a monitorização dos riscos (*risk monitoring*) que corresponde à Fase 5.

Nesta última fase, numa perspectiva de gestão contínua dos riscos, inclui-se ainda o despoletar da repetição periódica de todo o ciclo, o que equivale a dizer que estamos perante uma solução de melhoria contínua.

2.3.3 SOLUÇÕES DE MELHORIA CONTÍNUA

Nos meios profissionais relacionados com os SI defende-se a crescente adopção de normas (exemplos: CobiT, ITIL, ISO, SGQ, etc.) para os processos de SI das organizações, podendo também algumas destas normas serem utilizadas como modelo de referência para a execução dos trabalhos de Auditoria de SI (as normas serão explorados mais à frente no capítulo relativo ao Modelo Funcional). Como resultado da aplicação das normas, é expectável verificar-se um crescimento na implementação de soluções de melhoria contínua (no sentido de melhorias preventivas e não apenas soluções correctivas). Neste contexto, a melhoria contínua é entendida como aplicável, em particular, ao processo de Auditoria e aos respectivos Auditores, mas também, no geral, a toda a restante organização que beneficia das soluções de melhoria contínua que lhe são apontadas em resultado dos trabalhos de Auditoria.

Para formalizar esta ideia através de um referencial teórico e, com base neste, aplicarmos um exemplo relativo a uma Auditoria de SI, recorreu-se à seguinte representação da autoria de (Karapetrovic and Willborn, 2001). Em resumo, esta demonstra-nos como uma série de Auditorias que sejam interdependentes potenciam a implementação de acções preventivas que, por sua vez, podem acelerar a melhoria, tornando-a também num processo contínuo.

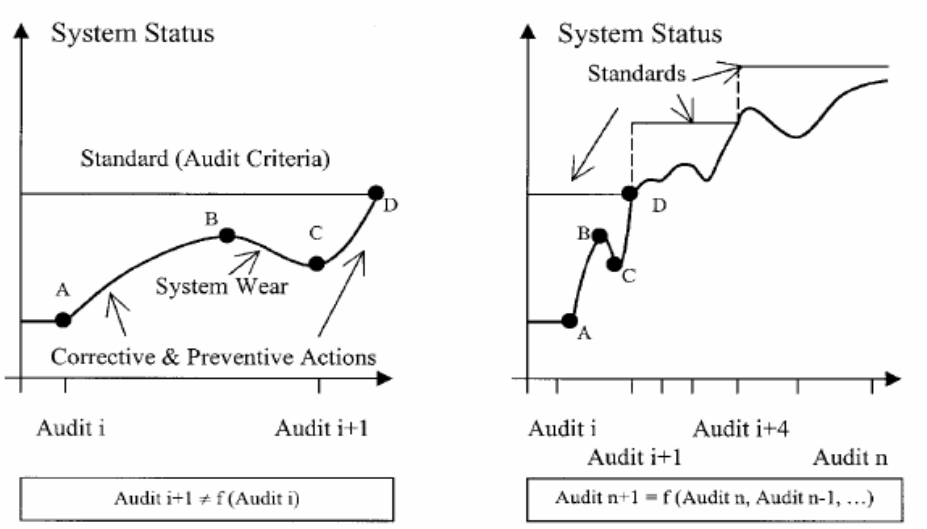


Figura 2.4 - Melhoria Contínua na Auditoria

Fonte: Versão original extraída de (Karapetrovic and Willborn, 2001): "*Independent versus Interdependent series of audits*"

Imaginemos que uma determinada Auditoria a um Sistema deve ser executada com uma periodicidade definida e realizada por referência a uma norma fixa (*standard*), ou seja, um critério de Auditoria fixo (*Audit Criteria*). No momento da primeira Auditoria (*Audit* i), o Sistema auditado tem um nível de conformidade com a norma representado pelo ponto A (gráfico do lado esquerdo da Figura). Após a Auditoria, através da implementação de medidas correctivas, o nível de conformidade sobre para B. Devido ao passar do tempo e com o uso, desce posteriormente para o nível C no momento em que se executa a segunda Auditoria (*Audit* i+1). Na sequência desta, através da implementação de medidas preventivas, o nível de conformidade sobe finalmente para D, atingindo o nível objectivo requerido pela norma. Imaginemos agora um exemplo similar mas em que as Auditorias não são independentes, nem de periodicidade fixa, sendo sim inter-dependentes e executadas de acordo com uma escala de prioridades, definida em função do desvio face ao nível de conformidade desejado (gráfico do lado direito da Figura). Neste caso, será expectável que o intervalo de tempo entre a primeira Auditoria (*Audit* i) e a segunda (*Audit* i+1) seja mais curto, pois a segunda Auditoria não é efectuada passado um período de tempo fixo e pré-definido (x meses), mas sim em função de uma prioritização de situações de maior risco e, consequentemente, com maiores necessidades de melhoria. Estas são identificadas através dum processo contínuo de monitorização do nível de implementação das acções correctivas recomendadas na primeira Auditoria. Quando se identifica que ainda não atingiram o nível de melhoria desejável, a segunda Auditoria (*Audit* i+1) acaba por ser despoletada mais cedo e, em resultado desta, o sistema atingirá o nível de conformidade desejado no ponto D também mais rapidamente. Por outro lado, em vez de usarmos a mesma norma fixa ao longo do tempo, devemos introduzir normas mais exigentes (ou novas partes destas) a partir do ponto D. Isto é, se definirmos novos critérios e objectivos de Auditoria sempre que tivermos atingido um objectivo de conformidade anterior, estaremos a potenciar a elaboração de novas recomendações de acções preventivas (não só reactivas) e a consequente implementação de soluções de melhoria contínua.

Conclui-se que cada auditoria seguinte (*Audit* n+1) deverá ser função das auditorias anteriores e tê-las em consideração. Uma postura dinâmica e adaptativa que promove continuamente a elevação dos referenciais (*Audit Criteria*) será certamente facilitada se entendermos cada Auditoria como fazendo parte de um Sistema de Auditorias.

2.4 ABORDAGENS SISTÉMICAS DA AUDITORIA

Nesta secção são apresentadas duas abordagens em que o Sistema é encarado não apenas como o objecto da Auditoria (Auditoria de Sistemas) mas essencialmente como o próprio sujeito (a Auditoria enquanto um Sistema).

2.4.1 A AUDITORIA ENQUANTO UM SISTEMA DA ORGANIZAÇÃO

Uma abordagem sistémica é utilizada por (Karapetrovic and Willborn, 2001) para explicar a existência de uma Hierarquia de Sistemas de Auditoria, com relações distribuídas por 3 níveis: 1° Sistema de Gestão; 2° Sistema de Auditoria; 3° Auditorias Individuais.

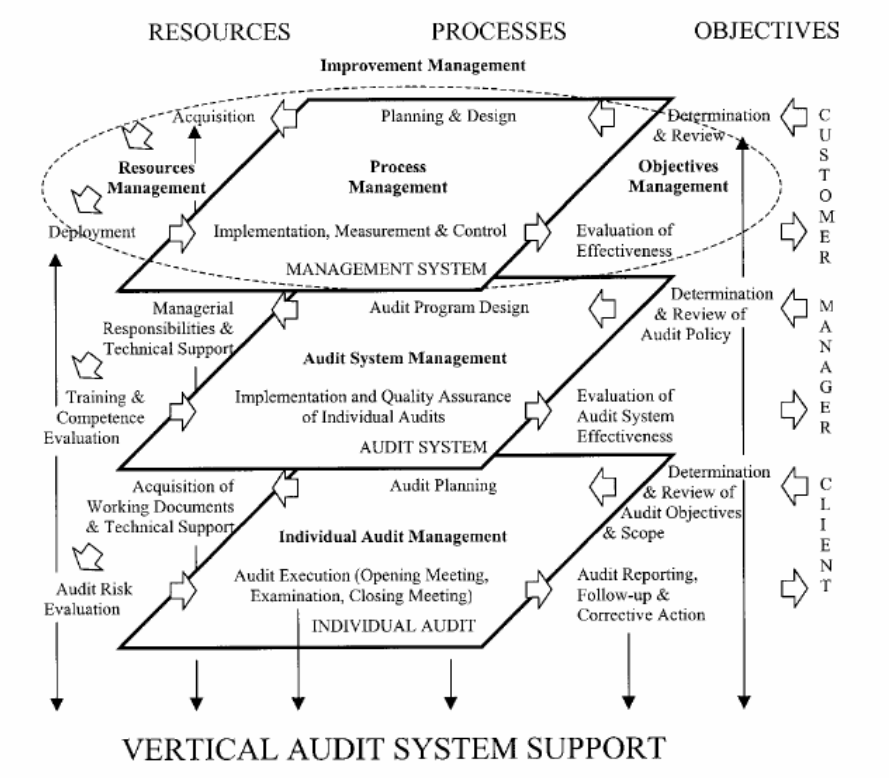


Figura 2.5 - Hierarquia de Sistemas de Auditoria

Fonte: Versão original extraída de (Karapetrovic and Willborn, 2001): "*Hierarchical view of audit-related systems.*"

Começando pelo topo, pelo primeiro nível, estes dois autores defendem que o Sistema de Gestão é um todo constituído por vários elementos que podem eles próprios também ser Sistemas. Estes constituem Sub-Sistemas que têm objectivos específicos relacionados com o objectivo global do Sistema de Gestão. Prosseguindo para o segundo nível, e efectuando um raciocínio semelhante, esta abordagem afirma que é ao Sistema de Auditoria que está atribuído o objectivo específico de avaliar e analisar o Sistema de Gestão no que diz respeito à sua capacidade de atingir os objectivos e ao seu cumprimento de regras (*compliance, benchmarks, standards*). Uma organização pode ter este Sistema de Auditoria focado em determinados tipos de Auditoria (por ex. Auditoria da Qualidade, Auditoria do Ambiente) ou ser mais abrangente (por ex. Auditoria de Processos de Negócio). Entrámos no terceiro nível, as Auditorias Individuais, quando nos referimos aos vários processos inter-relacionados que constituem uma Auditoria, como sejam planeamento da Auditoria, alocação de recursos, execução da Auditoria, relato de resultados, etc.

Reconhecer as diferentes inter-relações entre os processos de Auditoria que acabámos de exemplificar, bem como o seu lugar em relação aos restantes Sistemas de uma organização (ver também Figura 2.6), é fundamental para os Auditores poderem percepcionar a Auditoria como um Sistema e, consequentemente, desempenharem adequadamente a sua função.

O Auditor deve compreender que é necessária uma abordagem sistémica que relaciona todos os processos, actividades e decisões numa Auditoria. O processo de Auditoria é constituído por uma série de actividades inter-relacionadas. Só utilizando esta abordagem sistémica, o Auditor será capaz de focar com uma visão global ("*big picture*"). Assim, o Auditor contribuirá positivamente para um desempenho superior da Auditoria e para uma melhoria das suas próprias competências (este último aspecto será mais à frente explorado no capítulo referente ao Modelo Funcional).

De um modo similar, a organização como um todo também beneficiará se optar por um modelo sistémico de Auditoria, em que os diferentes tipos de Auditoria (da Qualidade, do Ambiente, de Processos de Negócio, de Sistemas, etc.) estão integrados e, de preferência, são simultâneos e executados sob orientação de uma mesma entidade interna (exemplo: Departamento de Auditoria Interna) ou externa (exemplo: empresas de consultoria especializada). Socorrendo-nos da lógica do modelo apresentado na figura anterior, deste modo consegue-se relacionar o Plano

do Sistema de Auditorias (2° nível) com cada uma das Auditorias Individuais (3° nível). Por outro lado, pode ser uma forma eficaz de integrar o número crescente e a diversidade de Auditorias obrigatórias (exemplo: *Sarbanes-Oxley*) a que as organizações estão sujeitas hoje em dia, especialmente as Auditorias aos Sistemas de Gestão (1° nível).

2.4.2 A AUDITORIA INSERIDA NUM MODELO DE SISTEMAS VIÁVEIS DA ORGANIZAÇÃO

Utilizar-se-á aqui a perspectiva do Modelo de Sistemas Viáveis de Stafford Beer para extrapolar o papel da Auditoria enquanto função de controlo e monitorização da eficiência de uma organização em que está inserida. De acordo com a interpretação deste modelo efectuada por (Carvalho, 1998), o modelo considera cinco funções essenciais para uma organização ser vista como um Sistema que é autónomo (existência independente) e é viável (capacidade de adaptação às alterações no ambiente). Na figura seguinte representam-se os cinco requisitos de viabilidade que se traduzem em cinco Sub-Sistemas:

1. Operações (unidades produtivas/operacionais que implementam produtos e serviços);
2. Coordenação (actividades de decisão sobre recursos e interacção com a Direcção/Gestão);
3. Controlo e Monitorização (análise dos Sub-Sistemas 1.Operações, internos à organização);
4. "*Intelligence*" (análise da envolvente da organização);
5. Política (actividades de decisão relacionadas com a política e a missão da organização).

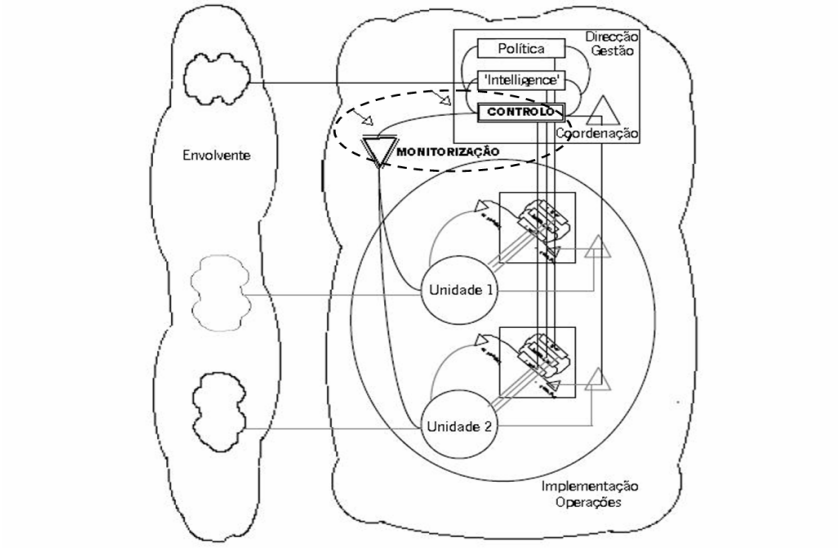


Figura 2.6 - Modelo de Sistemas Viáveis

Fonte: Adaptado e traduzido de (Carvalho, 1998): "*Simplified view of VSM*"

Segundo este modelo, um sistema viável tem uma estrutura recursiva, pois um sistema possui outros sistemas viáveis, que por sua vez possuem outros sistemas viáveis e assim sucessivamente. A viabilidade requer autonomia e capacidade de resolução de problemas e depende da estrutura do sistema. A estrutura deve ser entendida como uma rede de interacções entre unidades organizacionais. Esta estrutura possibilita a comunicação através da qual é obtido o conhecimento necessário para a acção. Todos estes conceitos referidos (autonomia, resolução de problemas, interacções, unidades, comunicação, conhecimento, acção, etc.) são habitualmente parte integrante de um processo de Auditoria que se caracteriza por ser independente, mas que também comunica e interage com as unidades organizacionais, produz conhecimento sobre os problemas dessas unidades organizacionais e culmina em planos de acções cujo objectivo é melhorar a eficiência da organização.

Neste contexto, interessa-nos centrar nos dois Sub-Sistemas que, segundo o referido autor, são: "*Sub-System 3 (and 3*) – Control (and Monitoring): capture and analysis of information about what is happening inside Sub-Systems 1*".

O conjunto destes dois Sub-Sistemas poderá ser comparável ao papel que a Auditoria desempenha neste tipo de modelo organizacional (Silva, 2004a), dado que:

- A Auditoria permite sistematizar a análise da informação sobre os Sub-Sistemas que são alvos de controlo e monitorização. Facilita não só a comunicação assíncrona entre os diversos Sub-Sistemas, mas constitui-se também como um mecanismo de memória organizacional, atenuando possíveis factores de entropia entre as unidades Operacionais.

- A Auditoria permite à Direcção/Gestão a obtenção de uma visão sistémica sobre os riscos e os processos do negócio. A Auditoria pode ser encarada como um sistema de reporte de excepções (*exception reporting system)* pois permite disponibilizar à Direcção/Gestão relatórios com as excepções (*findings*), reflectindo o status das Operações. Trata-se de um sistema de informação para a Direcção/Gestão que possui funcionalidades de classificação, filtragem e resumo sobre a situação interna das suas unidades produtivas. Adicionalmente, fornece à função de Direcção/Gestão uma ajuda na tarefa de monitorizar e compreender a organização sem necessidade de estar por dentro de todos os detalhes.

- A Auditoria poder-se-á consubstanciar numa infra-estrutura de Controlo interno, orientada para fomentar a viabilidade da organização, na medida em que as Operações (áreas auditadas) beneficiam do facto da Auditoria lhes disponibilizar recomendações de como operar de um modo mais eficiente.

§ § §

Encerra-se o presente capítulo com esta apresentação de duas abordagens sistémicas que ajudam a entender a Auditoria como um Sistema, inserida num modelo de Sistemas que constituem uma organização.

Após se ter igualmente efectuado uma definição dos conceitos associados à Auditoria de SI, um resumo da evolução da função e uma exploração de três dos principais factores caracterizadores do paradigma actual da função, no capítulo seguinte apresentar-se-á uma proposta de modelo para estruturar a função Auditoria de SI numa organização.

3 MODELO FUNCIONAL DE AUDITORIA DE SI

O capítulo que agora se inicia tem por objectivo propor um Modelo Funcional, ou seja, um conjunto de ideias estruturadas e sequenciadas sobre a função Auditoria de SI. Este modelo resulta do somatório de vários contributos, correspondendo às diversas dimensões que compõem a Auditoria de SI e que serão apresentadas ao longo deste capítulo.

Trata-se de um exercício pouco frequente na literatura académica existente sobre Auditoria de SI pelo tipo de informação obtida de diversas fontes (organizações profissionais de Auditoria, entidades que estudam os processos de SI e ainda autores independentes) e pela sistematização dos conceitos efectuada (sempre que possível apoiada em representações gráficas adaptadas ou originais). São igualmente lançadas novas ideias, entre as quais se destacam, desde já, três: o posicionamento conceptual da função Auditoria de SI; a identificação de actividades específicas de Auditoria de SI previstas em referenciais de SI (exemplo: CobiT, ITIL e ISO 17799); e a utilização dos conceitos de Gestão de Projectos aplicados na Gestão das Auditorias de SI.

Pretende-se que, percorrendo este capítulo até ao seu final, se vá construindo progressivamente uma boa percepção sobre o que é a Auditoria de SI. Foram já avançados alguns conceitos ao longo de todo o Capitulo 2 e, relembra-se, já foi também apresentada uma breve definição formal de Auditoria de SI (na secção 2.1.1 - Definições base). Tentar-se-á, a partir deste ponto, detalhar os objectivos, a organização, o âmbito, os referenciais metodológicos e os processos de Auditoria de SI que, em conjunto, formam o seu Modelo Funcional.

3.1 OS OBJECTIVOS DA FUNÇÃO

No domínio da Auditoria em geral, os objectivos da função de Auditor devem estar espelhados, sucintamente e a alto nível, na formulação da missão do departamento de Auditoria da organização. Associada também à identificação dos objectivos da função, habitualmente levanta-se a questão da independência da função, pois o grau de liberdade de actuação do Auditor de SI pode condicionar e determinar os seus objectivos. De seguida, serão desenvolvidas estas duas ideias, aplicadas no domínio da Auditoria de SI.

3.1.1 A MISSÃO DA AUDITORIA DE SI

A missão, enquanto conceito do domínio da gestão empresarial, é vulgarmente definida como um conjunto de objectivos de alto nível de uma organização, o principal propósito da sua existência e o modo como contribui para a visão da organização. O mesmo conceito aplica-se à missão de uma parte da organização (unidade de negócio ou departamento). Neste caso, deverá traduzir, a alto nível, o seu propósito e as responsabilidades específicas que lhe estão atribuídas no contexto global da organização.

Como se percebe, a missão deve ser uma descrição relativamente breve mas bastante clara no seu propósito. Contrariamente ao que acontece com outras temáticas relativas à Auditoria de SI, as referências bibliográficas específicas sobre a sua missão nem sempre são claras, sendo mais difíceis de identificar. No entanto, encontrou-se numa recente obra de (Davis, Schillerand and Wheeler, 2007) um conjunto expressivo de contributos sobre a missão da Auditoria de SI. Estes contributos formalizam as tendências mais actuais sobre o que deve ser a missão de um departamento de Auditoria, colocando em causa algumas das posições mais conservadoras sobre a independência da função (as questões da independência serão tratadas na próxima secção).

Aqueles três autores defendem que a atitude conservadora da Auditoria de reportar os problemas (*findings*) à Gestão de Topo e aos Comités de Auditoria é importante mas, por si só, é muito redutora da sua missão e não traz valor acrescentado para a organização. O verdadeiro contributo da função surge quando os problemas são resolvidos, sendo o relatório de Auditoria apenas um meio para atingir um fim que é a melhoria do estado dos controlos dos SI da organização. Na sua relação directa e privilegiada com aqueles órgãos de governo da organização, a Auditoria tem a oportunidade de apresentar relatórios que dão o devido ênfase aos problemas graves, conquistando assim a atenção dos responsáveis e facilitando a obtenção dos recursos necessários para a sua resolução.

Os referidos autores vão ainda mais longe quando advogam que a Auditoria só trará verdadeiro valor com a sua actividade se os problemas reportados não forem já do conhecimento dos responsáveis da organização e se a sua resolução não estiver já planeada anteriormente à Auditoria. Esta última posição é mais radical, mas o importante a reter é a capacidade da Auditoria de SI em identificar os problemas e potenciar a sua resolução.

Esta posição considera que, para a Auditoria de SI ser eficaz, não é sua missão ser uma função de policiamento, mas sim uma função de parceria com a restante organização. Idealmente, dever-se-á cultivar uma atitude de colaboração e de cooperação, tratando as áreas de SI, não como auditados, mas sim como clientes internos aos quais se deve apresentar um conjunto de preocupações (*findings*) de forma aberta e positiva e com os quais devem ser identificadas acções de melhoria.

Em síntese, a missão da Auditoria de SI é formalizada por (Davis, Schillerand and Wheeler, 2007) como tendo um duplo objectivo. Por um lado, providenciar à Gestão de Topo e aos Comités de Auditoria uma garantia independente de que os controlos de SI estão implementados e que funcionam eficazmente. Por outro lado, num patamar acima, melhorar o estado dos controlos de SI através da promoção destes e ajudar a organização a identificar vulnerabilidades nos controlos e a desenvolver soluções eficientes para gerir essas vulnerabilidades.

Na perspectiva da (ISACA, 2005), alinhada com a perspectiva anterior mas não tão desenvolvida, a Auditoria de SI é responsável por efectuar uma revisão e avaliação dos riscos do ambiente de trabalho dos SI que suportam os processos de negócio. A actividade da Auditoria de SI deverá ajudar a organização através da identificação e avaliação de exposições ao risco que sejam significativas, bem como contribuir para a melhoria dos mecanismos de gestão de risco e de controlo dos SI.

No ponto de vista do (IIA, 2005a), a Auditoria de SI deve avaliar a capacidade dos controlos de SI para protegerem a organização contra as ameaças mais importantes e deve fornecer evidência de que os riscos residuais são pouco prováveis de causar danos significativos à organização e às suas partes interessadas (*stakeholders*).

Como se vê, esta última preposição, para além de incorporar a ideia do risco, está muito dependente do conceito de controlo de SI. No entanto, o IIA esclarece a posição da Auditoria quanto aos controlos de SI:

"*It is not necessary to know 'everything' about IT controls*".

Esta afirmação é justificável na medida em que o IIA entende que devem existir dois tipos de garantias sobre os SI, com responsabilidades distintas. Em primeiro lugar, a garantia primária deve provir dos mecanismos de controlo interno, sendo responsabilidade dos Gestores de SI implementar esses controlos que devem ser contínuos e fornecer evidência rastreável. Em segundo lugar, vem a garantia secundária, fornecida pelos Auditores de SI, avaliando os controlos de forma independente e objectiva. Neste contexto, podemos detalhar a missão da Auditoria de SI como sendo uma garantia baseada no conhecimento, exame e avaliação dos controlos chave relacionados com os riscos que esses controlos pretendem gerir, bem como baseada na execução de testes suficientes para garantir que esses controlos estão apropriadamente desenhados e que funcionam de forma eficaz e continua.

Segundo esta visão, nem os controlos de SI, nem a Auditoria de SI funcionam por si só, complementam-se. O propósito da Auditoria de SI é atestar a validade dos controlos de SI e emitir opinião sobre o seu valor para a organização. Neste contexto, é necessária uma relação próxima da Auditoria de SI com a Gestão dos SI, a todos os níveis da organização. O modo como essa relação é mantida deve acautelar alguns princípios de independência que desenvolveremos de seguida.

3.1.2 A Independência da Auditoria de SI

A (ISACA, 2005) atribui grande relevo à independência dos Auditores de SI uma vez que nos seus "*IS Standards, Guidelines and Procedures for Auditing and Control Professionals*", a norma relativa à independência da função é a número 2 (*S2 – Independence*), logo a seguir à primeira

norma que define o propósito da função (*S1 - Audit Charter*). A norma caracteriza a independência do seguinte modo que integralmente se transcreve:
"*In all matters related to the audit, the IS auditor should be independent of the auditee in both attitude and appearance. The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.*"

Desta definição, destacam-se os conceitos de atitude, aparência e objectividade. Como veremos, a relação entre estes três conceitos é relevante pois pode acontecer que os objectivos da função não se limitem à própria auditoria. Por vezes, a Gestão das organizações e os Gestores dos SI têm a expectativa de poderem recorrer aos Auditores de SI para estes desempenharem papéis que não fazem parte dos objectivos primários da função de Auditor. Como exemplos, temos o apoio na definição de estratégias de SI, na avaliação e selecção de tecnologias ou de soluções de SI fornecidas por terceiros, na modificação e adaptação de aplicações para a organização, no desenho e implementação de controlos de segurança, no estabelecimento de políticas e procedimentos de SI, etc.

O desempenho destas actividades, às quais chamaremos objectivos secundários da função, são um importante contributo da Auditoria de SI para promover uma cultura de controlo na organização. Adicionalmente melhoram o conhecimento especializado e prático em SI por parte dos Auditores e, reciprocamente, colocam-no ao serviço da organização. A questão da independência levanta-se quando existe necessidade de efectuar uma Auditoria subsequente a algumas dessas actividades de SI em que o Auditor esteve envolvido. Neste caso, surge a relevância da aparência, dado que eventuais problemas (*findings*) levantados ou recomendações sugeridas podem ser apercebidas como não independentes. Por outro lado, podem também parecer não objectivas.

Segundo a ISACA, naquele tipo de actividades que nomeamos de objectivos secundários da função, embora a independência não seja mandatória, a objectividade continua a ser um objectivo obrigatório para a função do Auditor de SI que a deverá desempenhar de maneira racional e sem enviusamentos. De qualquer forma, a atitude a tomar nestes casos de Auditorias subsequentes também é relevante. O Auditor de SI deve colocar à consideração do Comité de

Auditoria a legitimidade de executar essa Auditoria, devendo esse órgão de governo da organização discutir e propor soluções que permitam que a Auditoria seja executada e com a necessária independência (por exemplo, obter pontualmente um Auditor ou equipa de Auditoria diferente).

A obra de (Carneiro, 2004) chama a atenção para as relações de semelhança da função Auditoria com a função de Controlo Interno, pelo que também é relevante distinguir estas duas funções quanto aos seus objectivos e trazê-las para a discussão sobre a independência. Segundo este autor, existem profissionais de controlo interno que possuem formação em segurança informática, sendo esta última também do domínio da formação em Auditoria. Por outro lado, encontram-se Auditores de SI que já passaram por funções de controlo interno de SI, dado que existem alguns objectivos partilhados entre as duas funções. Ambas são habitualmente desempenhadas por profissionais especialistas em SI e TIC que efectuam verificações ao cumprimento dos controlos. No entanto, a função de controlo interno de SI distingue-se por ser executada por profissionais internos à organização, que reportam à Gestão dos SI e que se dedicam à análise de um conjunto definido de controlos no "dia-a-dia". Diferentemente, a função de Auditoria de SI garante a sua independência através do reporte directo aos órgãos superiores de governo da organização, pode subcontratar externamente profissionais de Auditoria e tem liberdade para avaliar, em determinados momentos de tempo, todos os tipos de controlos de SI.

Com um raciocínio idêntico, o (IIA, 2005b) traça uma linha que define a independência da Auditoria de SI face à Gestão dos SI no que diz respeito à responsabilidade sobre os controlos. Os Auditores de SI devem limitar-se a efectuar uma avaliação para garantir a adequação dos mecanismos de controlo e de gestão do risco dos SI, sendo estes mecanismos da responsabilidade dos Gestores de SI. Não é objectivo da função Auditoria de SI fazer parte integrante, nem desenhar ou manter correntemente estes mecanismos, preservando assim a sua objectividade e independência.

Uma posição menos conservadora é defendida por (Davis, Schillerand and Wheeler, 2007), aliás de acordo com as suas ideias sobre a missão da Auditoria de SI. Como frequentemente existe um duplo reporte da função Auditoria, não só ao Comité de Auditoria, mas também à Gestão de

Topo, e dado que os Auditores são funcionários da organização, os referidos autores consideram que a função não é de facto independente. Assim, o sucesso da organização é também de todo o interesse dos Auditores de SI. Estes não se devem escudar na sua posição de independência absoluta para evitar a sugestão de recomendações úteis e encontrar soluções de melhoria em colaboração com os Gestores dos SI.

A Auditoria de SI pode também ter como objectivo actividades de consultoria interna destinadas à Gestão dos SI, dando contributos sobre o modo como os controlos de SI devem ser desenhados, mas não devendo executar esses controlos. Caso se venha a realizar uma Auditoria subsequente aos SI que foram alvo de consultoria, o Auditor de SI trará mais valia à organização pois detém um conhecimento único sobre aquilo que está a auditar. A sua independência não ficará comprometida se o trabalho de consultoria tiver sido executado com objectividade.

Os referidos autores consideram que para caracterizar um Auditor de SI, hoje em dia, independência não é a palavra mais acertada, mas sim objectividade! Em suma, o objectivo da função Auditoria de SI é a melhoria da qualidade dos controlos de SI da organização.

Conclui-se este espaço dedicado aos objectivos da função Auditoria de SI informando que os conceitos sobre a missão da função e as suas relações de (in)dependência com a restante organização ficarão mais perceptíveis e consolidados ao longo das próximas secções. Nestas, teremos oportunidade de compreender o modo como a função deve estar organizada, enquanto um processo de negócio com um propósito específico (3.2.1), e como se tenta posicionar de forma independente face à restante organização (3.2.2). Por outro lado, as visões apresentadas sobre os controlos de SI enquanto objectos da Auditoria ficarão mais perceptíveis com a identificação do âmbito da Auditoria de SI, nomeadamente com a definição do seu universo de actuação (3.3.1) e com a descrição dos níveis, dimensões e tipos de controlo de SI que podem estar sujeitos à Auditoria de SI (3.3.2).

3.2 A ORGANIZAÇÃO DA FUNÇÃO

Esta secção, relativa à organização da função Auditoria de SI, será fortemente baseada num conjunto de contributos do autor da presente investigação, em que se tentará responder às seguintes questões:

Onde situar a função de Auditoria de SI e como posicioná-la no contexto da organização? Mais especificamente, qual a sua relação com os processos de SI e com os restantes processos de negócio? Como deve estar organizada a função de Auditoria de SI no contexto de um departamento de Auditoria de uma organização? Qual as suas relações com os órgãos de governo da organização, de modo a garantir a necessária independência?

3.2.1 AS FUNÇÕES DE GESTÃO DE SI E AUDITORIA DE SI COMO PROCESSOS DE NEGÓCIO

Para entender de que modo a Gestão de SI e a Auditoria de SI podem ser encaradas como sendo processos de negócio, começaremos por analisar a seguinte representação gráfica.

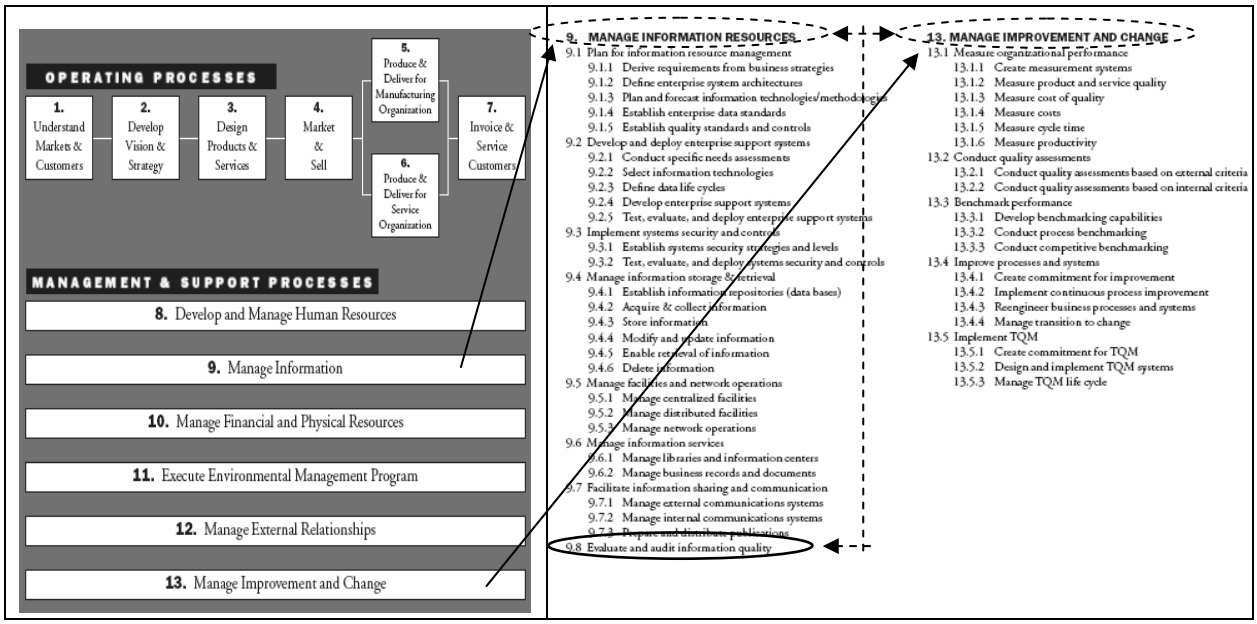


Figura 3.1 - *Framework* de Processos de Negócio

Fonte: Adaptado da versão original de (APQC and AA, 1996): "*Process Classification Framework*"

Utilizou-se este modelo de classificação de processos (*Process Classification Framework*), da autoria conjunta da *APQC - American Productivity & Quality Center* e da *AA - Arthur Andersen*, apenas para transmitir a visão de processos, bem como para situar e distinguir os processos operacionais dos de suporte. As relações estabelecidas entre os processos de Gestão dos SI e de Auditoria de SI são um contributo adicional, adaptado sobre a representação gráfica original.

De acordo com as entidades autoras (APQC and AA, 1996), este modelo estruturado tem os seguintes principais propósitos:
"*The Process Classification Framework seeks to represent major processes and subprocesses, not functions, through its structure and vocabulary*. (...) *The intent has been to create a high-level, generic enterprise model that will encourage businesses and other organizations to see their activities from a cross-industry process viewpoint instead of a narrow functional viewpoint*."

Uma das ideias base presentes nesta afirmação e que merece ser comentada é o facto do modelo representar processos de negócio e não funções de negócio (estas últimas no sentido de departamentos ou áreas de negócio). Esta visão foi relativamente inovadora na altura em que foi originalmente lançada, pois descola de uma visão de silos funcionais ou departamentais (visão redutora e limitada pelo organograma organizacional). A visão de processos torna-se importante na medida em que permite às organizações terem uma percepção das actividades ao longo da sua cadeia de valor de produção de produtos ou de disponibilização de serviços.

Este modelo estruturado prevê 13 macro-processos de negócio (representados do lado esquerdo da figura) que se desdobram em diversos processos e sub-processos (2 dos quais estão representados do lado direito da figura). Por sua vez, estes podem ainda ser desdobrados pela organização em actividades e tarefas. O referencial não lista todos os processos que são específicos de cada organização, nem todos os processos listados estão presentes em todas as organizações. Trata-se de um referencial que as organizações podem utilizar e adaptar em função da realidade do seu negócio, existindo liberdade para efectuar as alterações que sejam adequadas (acrescentar/retirar/mover processos). Aliás, os processos, sub-processos e actividades de SI podem ser alterados ou detalhados em função de outros modelos estruturados que sejam mais específicos da realidade dos SI, sendo o ITIL (*IT Infrastructure Library*) um bom

exemplo a adaptar (na secção 3.4 desenvolveremos os modelos estruturados que se adequam à Gestão dos SI e à Auditoria de SI).

Neste contexto, podemos encaixar os processos de Gestão dos SI como sendo processos dentro dos da Gestão da Informação (*9. Manage Information*) e os de Auditoria dentro dos da Gestão da Melhoria e da Mudança (*13. Manage Improvement and Change*).

O modelo originalmente proposto pelas (APQC and AA, 1996) prevê inclusivamente um processo que tem algumas semelhanças com os objectivos da Auditoria de SI mas que não é tão abrangente (*9.8. Evaluate and audit information quality*). No entanto, para além de redutor da missão da Auditoria de SI, consideramos não estar devidamente localizado pois está debaixo do domínio dos processos de Gestão da Informação, não garantindo a necessária independência enquanto processo de Auditoria. Deste modo, considera-se que a solução de os localizar debaixo dos processos de Gestão da Melhoria e da Mudança é mais adequada, tendo em conta os processos e sub-processos que o modelo estruturado aí prevê (exemplos: desempenho organizacional, avaliações de qualidade, melhoria de processos e sistemas, etc.).

Aproveitámos para analisar aqui a classificação dos processos como sendo "operacionais" ou de "gestão ou suporte". Utilizando conceitos geralmente aceites no domínio da gestão empresarial, podemos dizer simplificadamente que são processos operacionais os que contribuem directamente para a cadeia de valor de produção de produtos ou de disponibilização de serviços. Um outro critério para classificar como operacional pode ser a sua especificidade, no sentido de serem processos que criam valor e trazem vantagem competitiva à organização pois são processos distintivos face a outros tipos de negócios, habitualmente também designados por processos centrais (*core processes*). Os processos de suporte (também aqui designados de processos de gestão) são relativos a processos que não são diferenciadores da actividade da organização pois podem ser encontrados em muitas outras organizações (exemplos: processos de gestão de recursos financeiros, recursos físicos, recursos humanos, etc.). Parte destes processos podem até ser alvo de externalização (*outsourcing*), sintoma de que poderão não ser processos operacionais centrais para a organização. Tomando por base estes conceitos, é relativamente pacífico considerar a Auditoria de SI como um processo de suporte. Já no caso da Gestão dos SI essa classificação pode não ser tão consensual pois, hoje em dia, existem algumas organizações cujos seus processos operacionais de disponibilização de serviços estão

directamente e fortemente baseados na utilização intensiva de SI e de TIC. Estas são, muitas das vezes, tecnologias específicas ou proprietárias para determinados tipos de negócio (exemplos: sectores de telecomunicações, de integração de sistemas, da banca electrónica, etc.). Assim sendo, poder-se-ão classificar alguns tipos de processos de SI como sendo processos operacionais e não processos de suporte.

No fundo, a ideia fundamental que se pretende transmitir é que a gestão dos recursos associados à Informação, tais como os SI e as TIC, deve ser encarada como um processo de negócio. Em consequência, os processos de SI devem ser alvo de Auditoria, à semelhança dos restantes processos de negócio, sendo precisamente a Auditoria de SI o processo mais indicado para o fazer. Por seu lado, a Auditoria é também um processo de suporte ao negócio, devendo ela própria estar também sujeita a Auditorias periódicas, de preferência realizadas por entidades externas independentes. Como corolário adicional, daqui se deduz também a importância de, tanto a Gestão dos SI, como a Auditoria de SI, compreenderem bem os restantes processos de negócio e as suas necessidades. Na secção seguinte será apresentado o posicionamento da Auditoria de SI e as suas relações com a Gestão dos SI e os restantes processos de negócio.

3.2.2 O Posicionamento da Função Auditoria de SI

A próxima figura representa e sistematiza a visão do autor deste trabalho de investigação sobre o modo como a função Auditoria de SI se deve posicionar no contexto de um departamento de Auditoria e como deve reportar aos órgãos de governo da organização.

Comecemos por analisar este último ponto do reporte organizativo. A função de Auditoria de SI deve reportar ao responsável do departamento de Auditoria e Gestão de Risco. Por sua vez, este deverá reportar ao Comité de Auditoria e Gestão de Risco e, por via deste, ao responsável máximo da organização que é o CEO (*Chief Executive Officer*). Note-se que o modelo de reporte aqui defendido difere ligeiramente face à maior parte das organizações em que a Auditoria e Gestão de Risco reporta ao CFO (*Chief Financial Officer*) ou, nalguns casos, directamente ao CEO. No sentido de garantir maior coerência com a abrangência das funções de Auditoria e Gestão de Risco, defende-se um reporte ao CEO e não ao CIO. No sentido de garantir um maior

grau de independência, defende-se que o reporte ao CEO seja no âmbito das suas responsabilidades de supervisão no Comité de Auditoria e Gestão de Risco e não directamente no âmbito das suas funções executivas na Gestão de Topo da organização (Conselho de Administração / Comissão Executiva). Para além disso, o referido Comité pode ser entendido como uma última instância à qual o departamento de Auditoria e Gestão de Risco pode recorrer, em eventuais situações em que os gestores da organização não se mostram disponíveis para colaborar.

Diferentemente, os responsáveis pelo departamento de SI deverão reportar directamente à Gestão de Topo da organização, nomeadamente ao CIO (*Chief Information Officer*). Este papel (CIO) justifica-se com o facto de existir um processo de negócio responsável pela gestão dos recursos associados à Informação, incluindo os SI e as TIC (tal como vimos na secção anterior).

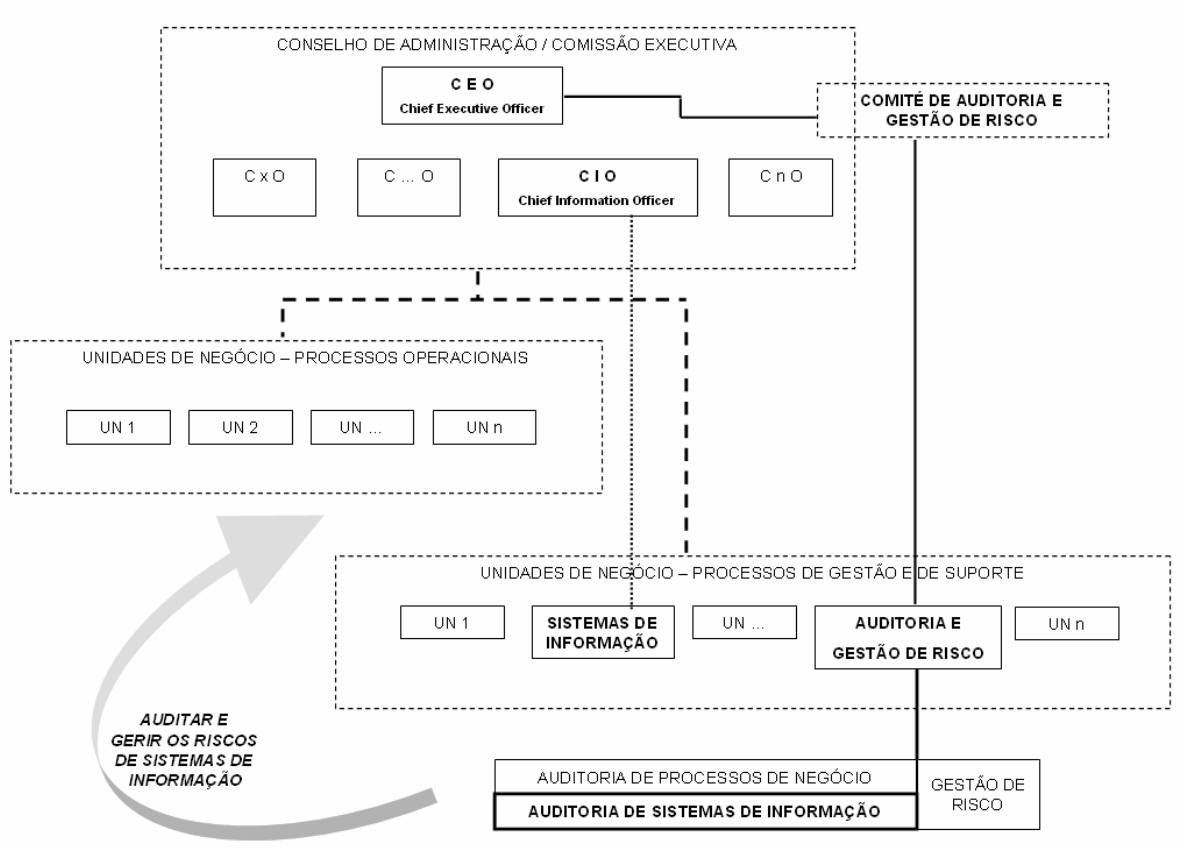


Figura 3.2 - Posicionamento e Reporte Organizativo da Função Auditoria de SI

Fonte: Proposta elaborada pelo autor

Apresenta-se agora para apresentar o entendimento do (IIA, 2005b) sobre os papéis de cada um dos três elementos de governo da organização referidos, em específico quanto às suas responsabilidades sobre os riscos e controlos dos SI.

- Comité de Auditoria → Engloba a supervisão de matérias Financeiras, de Controlo Interno, de Gestão de Risco e de Ética. Os controlos de SI são um elemento importante em cada uma daquelas matérias pelo que o Comité deve:
  - Incluir questões relevantes de SI na agenda do Comité, exigindo reporte ao CIO.
  - Exigir fiabilidade dos SI para com as com obrigações de processamento e reporte financeiro da organização.
  - Supervisionar a adequada avaliação dos controlos de SI, em particular nas questões importantes de negócio relacionadas com o desenvolvimento e aquisição de novos SI.
  - Rever o planeamento anual do departamento de Auditoria Interna de modo a que as grandes questões de SI sejam incluídas.
  - Assegurar que os controlos de SI são alvo de Auditorias.
  - Analisar os resultados dos trabalhos de Auditoria e monitorizar a resolução das excepções (*findings*) reportadas.
  - Estar alerta para questões de SI que tenham impacto em questões éticas.
- CEO (*Chief Executive Officer*) → O responsável máximo pelo controlo geral da estratégia e da operacionalidade da organização deve considerar os SI em múltiplos aspectos, nomeadamente:
  - Definir objectos corporativos e exigir medidas de desempenho para os SI.
  - Compreender e aprovar a estratégia para os SI da organização.
  - Aprovar globalmente os recursos e a organização das áreas de SI.
  - Actuar como um guardião sobre os factores críticos de sucesso da organização em relação aos SI.
  - Identificar questões relevantes de SI para discussão na Gestão de Topo e nos Comités.
  - Ser o responsável de última instância pela globalidade do sistema de Controlo Interno da organização, como resultado dos diversos sistemas de Controlo Interno existentes em cada processo ou área da organização, incluindo o dos SI.
- CIO (*Chief Information Officer*) → Tem a responsabilidade global na organização sobre todos os SI e sobre os seus controlos, devendo:
  - Compreender as necessidades e alterações do negócio que exijam novos SI.
  - Explorar e seleccionar a introdução de novas tecnologias relevantes para a organização.

- Desenvolver uma parceria com os gestores dos restantes processos de negócio para assegurar alinhamento com a estratégia, assegurar a conformidade e gerir os riscos no que diz respeito aos SI.
- Efectuar a medição do desempenho operacional dos SI como suporte aos objectivos do negócio.
- Planear e controlar os recursos de SI.
- Desenhar e manter um sistema de controlo interno nos SI, sendo o seu máximo responsável.
- Assegurar que os SI estão a fornecer os serviços e a suportar os utilizadores internos e os clientes finais, proporcionando os meios necessários para que possa ser verificado pela Auditoria de SI.
- Permitir adequados níveis de formação aos recursos humanos de SI para que mantenham as competências e os conhecimentos actualizados.

No que diz respeito ao posicionamento da função Auditoria de SI, no contexto de um departamento de Auditoria e Gestão de Risco, defende-se que coexista com as funções de Auditoria de Processos de Negócio (função semelhante) e de Gestão de Risco (função complementar). Ao nível do departamento, podemos dizer que o objectivo é auditar e gerir os riscos de SI, tanto dos processos de negócio das unidades operacionais, como dos processos de negócio das unidades de suporte (entre as quais a de SI).

O papel da Auditoria de Processos de Negócio é em tudo semelhante ao que se tem vindo a defender para a Auditoria de SI ao longo deste texto. A diferença entre as duas Auditorias reside no facto desta última ser mais especializada (nos processos de SI), enquanto que a primeira é mais abrangente e generalista (pode auditar todos os restantes processos de negócio). Este tipo de Auditoria é também frequentemente designado de Auditoria Operacional, uma vez que avalia a eficácia dos processos de negócio e sugere recomendações no sentido de melhorar a sua eficiência operacional. Idealmente, se os Auditores de Processos de Negócio e os Auditores de SI tivessem competências profissionais convergentes entre si (normalmente existem diferenças e especializações), então poderíamos ter uma só área de Auditoria com competências para auditar qualquer processo de negócio. A crescente dependência dos processos de negócio face aos SI poderá, com o tempo, acelerar e tornar necessária essa convergência.

Quanto ao papel da função de Gestão de Risco, a sua exploração será facilitada se começarmos por analisar a seguinte citação do (IIA, 2005b):

"*Control and risk represent opposite sides of the same coin. Controls exist to help mitigate risk; identification of control deficiencies highlights areas of potential risk. Conversely, by examining risk, auditors can identify areas where controls are needed and/or are not working*."

Pela interpretação da citação, conclui-se que os controlos são instrumentos de mitigação do risco, pelo que os Auditores devem avaliar os riscos para identificar deficiências nos controlos. Essa avaliação dos riscos beneficia da relação de proximidade existente entre as funções de Auditoria e de Gestão de Risco. Segundo o (IIA, 2004), estas deverão partilhar grande parte das competências e dos conhecimentos, como por exemplo os requisitos do Governo das Sociedades (*Corporate Governance*), as técnicas de Gestão de Projectos, as capacidades analíticas, as capacidades de relacionamento com as áreas de negócio, etc. Existem contudo diferenças já que a Gestão de Risco tem um papel muito mais próximo dos Gestores dos processos de negócio, tendo por isso um menor grau de independência por comparação com a Auditoria (não deixando porém de ter de ter um elevado grau de objectividade). Os Gestores de Risco possuem igualmente áreas específicas de conhecimentos (exemplo: modelos de avaliação e gestão dos riscos) que a maior parte dos Auditores não possuem.

Independentemente das posições do IIA, de uma forma simplificada podemos dizer que a Auditoria avalia os controlos dos processos de negócio e a Gestão de Risco ajuda os gestores dos processos de negócio a identificar e a gerir os seus riscos. Por consequência, poderíamos ser levados a interpretar que a Auditoria e a Gestão de Risco estariam em lados opostos, mas na verdade são duas funções que se complementam ("*opposite sides of the same coin").*

Existem dois factos que suportam a ideia acima apresentada sobre complementaridade das duas funções e que já foram explorados neste texto. Por um lado, o actual paradigma de que a Auditoria deve seguir uma abordagem baseada no risco. Por outro lado, o objectivo que possuem de potenciar uma melhoria contínua por parte da organização, dado que um dos produtos resultantes do trabalho de ambas as funções é a definição de acções correctivas ou de melhoria para os processos de negócio. No fundo, existe um denominador comum às duas funções que é o risco, tendo ambas uma preocupação e um fim comum que é a diminuição dos níveis gerais de risco da organização. Apenas a forma de atingir esse fim é que difere.

Neste papel de complementaridade, no seio do departamento de Auditoria e Gestão de Risco, a função de Gestão de Risco tem a importante responsabilidade de efectuar (pelo menos anualmente) uma identificação global dos principais riscos de negócio, incluindo os de SI (ver exemplo de metodologia de Gestão de Risco aplicada aos SI na secção 2.3.2). Deste exercício deve resultar uma prioritização de processos e sub-processos de negócio que deverão ser alvo de Auditorias, devendo ser considerados como um contributo (*input*) para a elaboração do planeamento anual da Auditoria de Processos de Negócio e da Auditoria de SI.

Para completar a compreensão do posicionamento das funções na organização, bem como das suas diferenças de papéis, sugere-se que sejam recordadas as definições de Auditoria (na secção 2.1.1) e de Gestão de Risco (na secção 2.1.2).

A figura seguinte, proposta do autor do presente trabalho, serve para concluir e sistematizar, em termos conceptuais, o tema do posicionamento da função de Auditoria de SI.

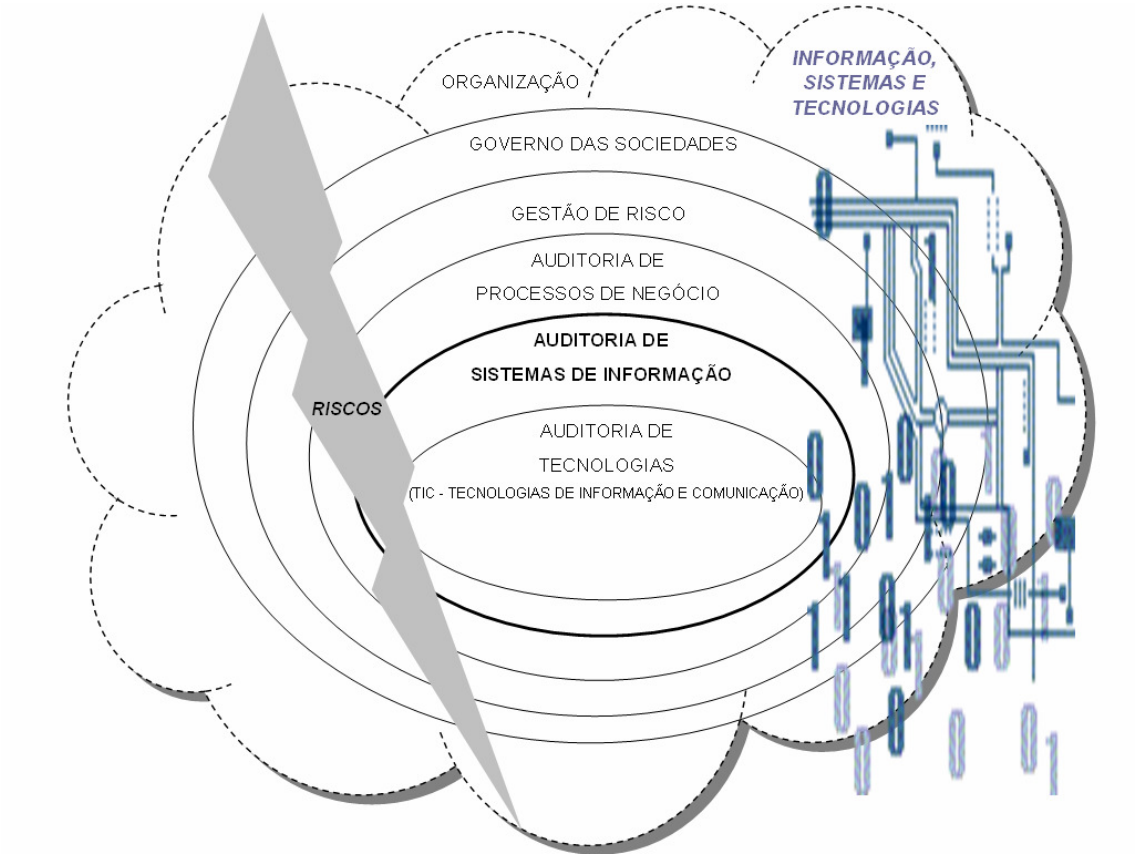


Figura 3.3 - Posicionamento Conceptual da Função Auditoria de SI

Fonte: Proposta elaborada pelo autor

Comecemos por interpretar esta representação conceptual, dizendo que o espaço de actuação da Auditoria de SI é a organização, sujeita de um modo transversal a todo o tipo de riscos. São também transversais e omnipresentes, em toda a organização, três dos principais objectos que são alvo da Auditoria de SI: a Informação, os Sistemas e a Tecnologia.

Considerando os riscos transversais a toda a organização, considerando também os riscos como um dos denominares comuns entre a Auditoria e a Gestão de Risco, e considerando ainda a Gestão de Risco como uma função mais próxima do negócio na gestão desses riscos, entende-se então a função de Gestão de Risco como mais abrangente, estando por isso as funções de Auditoria conceptualmente nela incluídas. Aliás, a Gestão de Risco e a Auditoria são consideradas dois instrumentos de Governo das Sociedades (*Corporate Governance*).

A seguinte afirmação do (IIA, 2005a) corrobora esta ideia de abrangência da Gestão de Risco e reafirma a necessidade de tratar os SI enquanto parte integrante dos processos de negócio:
"*Risk management applies to the entire spectrum of activity within an organization, not just to the application of IT. IT cannot be considered in isolation, but must be treated as an integral part of all business processes.*"

Dado que se considera os processos de SI como parte integrante dos processos de negócio, então também se conceptualiza a Auditoria de SI como uma parte especializada da Auditoria de Processos de Negócio. De modo semelhante, dado que os actuais SI das organizações são quase todos baseados em TIC e são de difícil dissociação destas, então a Auditoria de SI deve também abranger no seu âmbito a Auditoria de Tecnologias.

Uma vez entendido o posicionamento da função Auditoria de SI, nomeadamente o seu contexto de reporte organizacional independente e as suas relações de semelhança e de diferença com outras funções que também analisam os riscos, avançaremos de seguida para a definição do âmbito de actuação da Auditoria de SI.

3.3 O ÂMBITO DA FUNÇÃO

De um modo muito simplista podemos dizer que pode caber no âmbito da Auditoria de SI tudo aquilo que é do universo dos SI. Coloca-se, no entanto, a questão de como definir este universo e, em seguida, a abrangência do respectivo âmbito? A presente secção trata desta problemática.

3.3.1 A DEFINIÇÃO DO UNIVERSO DA AUDITORIA DE SI

Adaptou-se a seguinte representação gráfica e os conceitos do (ITGI, 2000) para nos guiar na determinação do universo da Auditoria de SI.

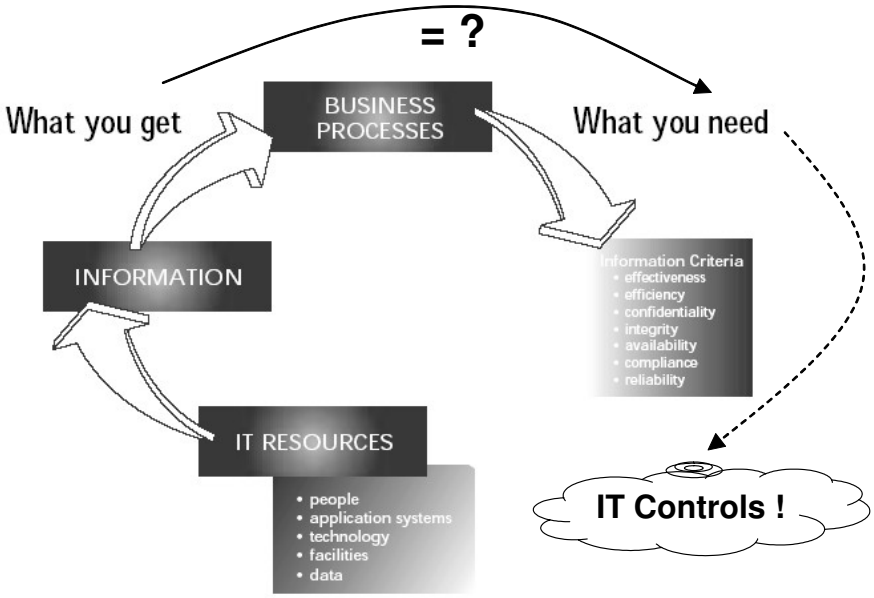


Figura 3.4 - A Definição do Universo da Auditoria de SI

Fonte: Adaptado da versão original de (ITGI, 2000): "*The Framework's Principles*"

Desde logo, identificam-se 3 principais factores: os Processos de Negócio, a Informação e os Recursos de SI. A conjugação e interacção destes 3 factores determinará o espaço que potencialmente pode ser alvo das Auditorias de SI, ou seja, o seu universo.

A informação que é necessária para suportar os objectivos e os requisitos do negócio é obtida pela aplicação combinada dos 5 tipos de recursos de SI (*IT Resources*) representados na figura. Por sua vez, estes recursos necessitam de ser geridos através de processos de SI.

Para satisfazer os objectivos de negócio, a informação deverá respeitar determinados critérios, ou seja, os 7 requisitos de negócio para a informação (*Information Criteria*) representados na figura. Para nos assegurarmos que estes requisitos da informação são cumpridos, é necessária a definição, a implementação e a monitorização de controlos de SI adequados. É precisamente aqui, na monitorização dos controlos, que se situa globalmente o âmbito da Auditoria de SI.

Os controlos de SI são pois um instrumento que as organizações recorrem para reduzir os níveis de risco e a incerteza na resposta à seguinte questão: a informação que é obtida (*What you get*) possui realmente as características necessárias (*What you need*)? Na próxima secção detalharemos os possíveis níveis, dimensões e tipos controlos de SI.

Exploraremos agora cada um dos 3 principais factores da equação que determina o universo da Auditoria de SI: os processos de negócio, os recursos de SI e a informação.

Quanto aos processos de negócio, já tivemos oportunidade de os analisar anteriormente (na secção 3.2.1) pelo que já ficou compreendida a necessidade dos processos de SI serem encarados como processos de negócio e, como tal, serem alvo de Auditoria à semelhança dos restantes processos de negócio.

Quanto aos recursos de SI, e utilizando as definições do (ITGI, 2000), podemos dizer que os seguintes recursos de SI fazem parte do universo da Auditoria dos SI:

- As Pessoas *(People)* → Inclui as competências do pessoal, o seu conhecimento e o seu potencial de produtividade para planear, organizar, adquirir, produzir, suportar e monitorar os serviços dos SI.
- Os Sistemas Aplicacionais *(Application Systems)* → Consideram-se como sendo a soma dos procedimentos manuais e programados.
- A Tecnologia *(Technology)* → Inclui o *hardware*, os sistemas operativos, os sistemas gestores de bases de dados, as redes, os dispositivos multimédia, etc.
- As Instalações *(Facilities)* → São todos os recursos físicos que albergam e suportam os SI.
- Os Dados *(Data)* → Consideram-se como sendo os objectos no seu sentido mais lato, internos ou externos, estruturados ou não estruturados, gráficos, sons, etc.

Quanto à informação, deve respeitar essencialmente dois grandes grupos de requisitos: os fiduciários e os de segurança. Os requisitos fiduciários são os defendidos pelo COSO no seu modelo de Controlo Interno e, como extensão deste, no seu modelo de Gestão de Risco Corporativo (IIA, 2007b): a eficácia e eficiência nas operações; a fiabilidade da informação que é alvo de reporte; e a conformidade com as leis e regulamentos. Os requisitos de segurança são os geralmente aceites e indicados pelos modelos estruturados que tratam o tema da segurança da informação: a confidencialidade; a integridade; e a disponibilidade.

Recorrendo novamente às definições do (ITGI, 2000), os 7 critérios representados na figura aos quais a informação suportada pelos SI deve obedecer e que devem integrar o âmbito da Auditoria de SI são:

- Eficácia *(Effectiveness)* → Informação relevante e pertinente para os processos de negócio, produzida de forma atempada, correcta, consistente e usável.
- Eficiência *(Efficiency)* → Produção de informação através do uso óptimo dos recursos (os mais produtivos e económicos).
- Confidencialidade *(Confidentiality)* → Protecção de informação sensível para evitar ser utilizada ou revelada de forma não autorizada.
- Integridade *(Integrity)* → Informação exacta e completa, válida de acordo com os valores e expectativas do negócio.
- Disponibilidade *(Availability)* → Informação disponível quando requerida pelos processos de negócio, incluindo a salvaguarda dos recursos necessários e das suas capacidades associadas.
- Conformidade *(Compliance)* → Cumprimento das leis e regulamentos aos quais os processos de negócio estão sujeitos.
- Fiabilidade *(Reliability)* → Produção de informação apropriada e fiável para a gestão executar as operações e cumprir as suas responsabilidades de reporte financeiro e de reporte de conformidade.

Em resumo, a Auditoria de SI deverá avaliar todos os controlos sobre o modo como aqueles 5 tipos de recursos de SI são usados, através de processos de SI, e se estes disponibilizam a informação aos processos de negócio de acordo com os 7 critérios mencionados.

Sendo este o universo da Auditoria de SI, será que esta consegue cobri-lo convenientemente no seu âmbito?

É importante compreender que o âmbito de cada Auditoria de SI varia no seu grau de abrangência e de análise dos processos de SI, dos recursos de SI e dos critérios da informação. De facto, algumas Auditorias de SI apenas analisam um ou vários destes elementos, deixando outros fora de âmbito.

Segundo (Sayana, 2002), é imprescindível analisá-los a todos, mas não necessariamente ao mesmo tempo numa só Auditoria. Para além das habituais limitações de tempo e disponibilidade de mão-de-obra, as competências dos Auditores para analisar cada um desses elementos podem também variar. Na realidade, os SI são cada vez mais complexos e constituídos por diversas componentes que, em conjunto, formam uma solução de negócio. Uma adequada análise sobre estes SI só poderá ser conseguida se todas as componentes forem auditadas. Neste contexto, parece válida a expressão que nos diz que elo mais fraco determina a robustez de toda uma cadeia. A totalidade da cadeia poderá ser analisada através de uma série de Auditorias.

No entanto, os resultados das diversas Auditorias necessitam de ser analisados conjuntamente. Isto permitirá ao Auditor de SI e à gestão da organização uma visão global do estado dos controlos e dos níveis de risco de SI, permitindo uma cobertura gradual do universo da Auditoria de SI.

Para encerrar esta secção, deixa-se uma nota do (IIA, 2006) sobre a utilidade da determinação do universo da Auditoria de SI. Os recursos de Auditoria de SI não são ilimitados e as necessidades de auditar os SI são crescentes. Daí que uma correcta definição do universo da Auditoria de SI numa organização seja uma base de ajuda a partir da qual se possa elaborar um plano de Auditorias que balanceie de um modo eficaz as necessidades de auditar com as

restrições de recursos. Idealmente, os recursos de Auditoria deveriam ser determinados em função das necessidades das Auditorias. Caso o plano de Auditorias seja anual, podemos dizer que constituirá o âmbito da Auditoria de SI para um determinado ano.

Retomaremos a questão do planeamento na secção 3.5.1. Por agora, na secção seguinte, desenvolveremos os níveis, dimensões e tipos controlos de SI que podem constituir o âmbito das Auditorias de SI.

3.3.2 Os Níveis, Dimensões e Tipos de Controlo sujeitos à Auditoria de SI

A ideia de que o âmbito da Auditoria de SI pode ser global, no sentido de abrangente a todos os níveis da organização e em todas as dimensões dos SI, é transmitida de um modo adequado pelo seguinte modelo estruturado do (IIA, 2005a).

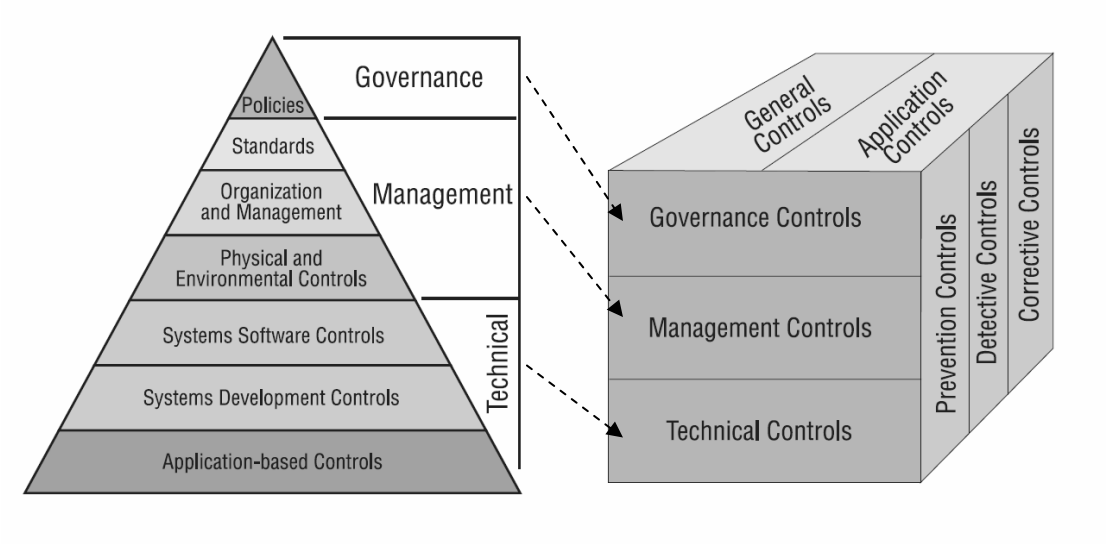


Figura 3.5 - O Âmbito da Auditoria de SI: Níveis e Dimensões dos Controlos de SI

Fonte: Adaptado das versões originais de (IIA, 2005a): "*IT Controls*" & "*Some Control Classifications*"

A pirâmide do lado esquerdo da figura apresenta uma hierarquia de 7 tipos de controlos de SI que devem ser considerados, tanto na implementação desses controlos numa organização, como nas actividades de Auditoria aos próprios controlos. Estes não são mutuamente exclusivos (são inter-dependentes) e estão agrupados em 3 grandes níveis: controlos de Governo, de Gestão e Técnicos. Numa outra perspectiva, que está transposta para o cubo no lado direito da figura e que também não é mutuamente exclusiva, os controlos podem ainda ser classificados como Gerais ou Aplicacionais e podem ser de natureza Preventiva, Detectiva ou Correctiva.

A tabela seguinte arruma estes conceitos de controlos de SI e concretiza com alguns exemplos desses controlos, contribuindo para a percepção do que é o âmbito da Auditoria de SI.

TIPOS DE CONTROLOS DE SI	
Controlos de **Governo**	Ao nível do Governo das Sociedades, os controlos de SI pretendem garantir que uma eficaz Gestão da Informação e dos SI é enquadrada e suportada por adequadas Políticas, devendo estas estar relacionadas com os objectivos e as estratégias da organização. Não cabe à gestão de topo da organização efectuar a Gestão da Informação e dos SI, nem executar Auditorias aos sues controlos, mas sim supervisionar e criar condições para que sejam executadas. ▪ **Políticas** → Dado que os SI são vitais para a operacionalidade de muitas organizações, deverão existir Políticas escritas relativas a todo o âmbito dos SI, devidamente aprovadas pela gestão de topo e divulgadas por toda a organização. **Exemplos** de Políticas: níveis globais de segurança e privacidade; classificação da Informação; distinção da responsabilidade sobre os dados e os sistemas (*ownership*); requisitos gerais para o plano de contingência/ recuperação dos SI, etc.
Controlos de **Gestão**	A Gestão deve garantir que os controlos de SI necessários ao atingimento dos objectivos da organização estão implementados. A Gestão deve reconhecer os riscos da organização, os seus processos e os activos e deve implementar diversos tipos de mecanismos para mitigar esses riscos: ▪ **Normas** → As normas (*standards*) servem para suportar os requisitos das Políticas e definem formas de operar na organização, compatíveis com os objectivos desta. Permitem à organização manter a totalidade do ambiente operacional dos SI de forma mais eficiente. **Exemplos** de Normas: desenvolvimento de sistemas; configuração de *software*; controlo de aplicações; estruturas de dados; documentação de SI; etc. ▪ **Organização e Gestão** → Como em qualquer outra função da organização, o modo como se estrutura e gere a função SI é determinante para a definição de linhas de reporte e de responsabilização e para uma eficaz implantação dos controlos de SI. **Exemplos** de controlos de Organização e Gestão: segregação de funções; controlo financeiro; gestão da mudança (*change management*); gestão de formação; etc. ▪ **Controlos Físicos e da Envolvente** → Todas os equipamentos de SI e as respectivas infra-estruturas físicas em que se encontram deverão estar devidamente protegidos. **Exemplos** de controlos Físicos e da Envolvente: servidores localizados em centros de dados (*DataCenters*); procedimentos de recuperação (*disaster recovery*); etc.

Controlos **Técnicos**	Os controlos Técnicos são os pilares dos restantes controlos dos SI da organização. São mecanismos que permitem automatizar controlos e implementar na prática algumas das Políticas para a Informação e para os SI definidas pela gestão da organização, através de: ▪ **Controlos de Software** → São os controlos relativos à utilização das redes, dos sistemas e, em última instância, do próprio software pelos utilizadores (*users*). **Exemplos** de controlos de Software: gestão de acessos; intrusão; encriptação; alterações; etc. ▪ **Controlos de Desenvolvimento de Sistemas** → Dizem respeito ao desenvolvimento e aquisição de sistemas tendo por base um método comum com controlos eficazes em cada uma das fases desse processo. **Exemplos** de controlos de Desenvolvimento de Sistemas: documentação de requisitos de utilizadores; formalização de desenho de arquitectura; processos de manutenção e gestão de alterações; técnicas de gestão de projectos; etc. ▪ **Controlos baseados em Aplicações** → São controlos internos às próprias aplicações que garantem a integridade dos processos de negócio que estão automatizados e que se baseiam nessas aplicações. **Exemplos** de controlos baseados em Aplicações: controlos de entrada; controlos de processamento; controlos de saída; histórico de transacções; etc.
Controlos **Gerais**	Os **Controlos Gerais**, também designados de Controlos Infraestruturais, referem-se ao como é gerida a generalidade dos sistemas, dos processos e dos dados que numa organização fazem parte do domínio dos SI. **Exemplos** de controlos Gerais: segurança da Informação; gestão de acessos; aquisição e desenvolvimento de sistemas; procedimentos de *backup*; etc.
Controlos **Aplicacionais**	Os **Controlos Aplicacionais** referem-se ao domínio de uma aplicação ou processo de SI específico. **Exemplos** de Controlos Aplicacionais: edição de dados; balanceamento de totais; relatórios de erros; etc.
Controlos **Preventivos**	Os **Controlos Preventivos** são aplicados para prevenir a ocorrência de erros, omissões ou incidentes de segurança. **Exemplos** de controlos Preventivos: validadores de inserção de dados; antivírus; *firewalls*; etc.
Controlos **Detectivos**	Os **Controlos Detectivos** são aplicados para detectar erros ou incidentes que trespassaram eventuais controlos Preventivos. **Exemplos** de controlos Preventivos: identificação de utilizadores (*users*) que excederam determinados limites autorizados; identificação de padrões de dados incorrectamente manipulados; etc.
Controlos **Correctivos**	Os **Controlos Correctivos** são aplicados para corrigir erros, omissões ou incidentes quando estes são detectados. **Exemplos** de controlos Correctivos: correcção de dados incorrectamente inseridos; remoção de software ilegal; recuperação de sistemas ou dados; etc.

Tabela 3.1 - O Âmbito da Auditoria de SI: Tipos de Controlos de SI

Fonte: Elaborado e compilado pelo autor a partir dos conceitos do (IIA, 2005a): "*Understanding IT Controls*"

Como podemos constatar pela tabela, o âmbito da Auditoria de SI pode ser bastante abrangente. Podem ser efectuadas Auditorias de SI de diversos tipos, desde as de âmbito mais alargado

como as Auditorias a Controlos Gerais de SI, passando por Auditorias de Organização e Gestão de SI, até às mais específicas como as Auditorias Aplicacionais.

Por outro lado, as Auditorias de SI podem ter subjacente tanto uma abordagem aos processos de SI (exemplos: configuração de *software*, segregação de funções, etc.), ou aos recursos de SI (exemplos: servidores, documentação de requisitos de utilizadores, etc.) ou ainda à própria informação (exemplos: segurança da informação, classificação da informação, etc.).

Desta diversidade do âmbito depreende-se que as Auditorias de SI podem variar muito no seu grau técnico e no seu grau de especificidade. Note-se que este facto terá implicações nas competências exigidas aos Auditores de SI, a serem ajustadas em função dessas necessidades.

A figura e a tabela atrás exploradas são uma forma de arrumar e classificar os controlos de SI que constituem o âmbito da Auditoria de SI. No entanto, existem certamente outras formas.

Segundo (Carneiro, 2004), existem duas grandes linhas caracterizadoras do âmbito: por um lado, a Operatividade dos SI e, por outro, os Controlos de Gestão da função SI. É pela avaliação da Operatividade que a Auditoria de SI deve começar por se preocupar. Por Operatividade entende-se a capacidade que a organização possui para manter os seus SI, pelo menos num nível mínimo que permita o funcionamento da organização. A Auditoria à Operatividade pode passar pela avaliação dos Controlos Técnicos Gerais de Operatividade (exemplo: compatibilidade entre *software* e *hardware*) e pelos Controlos Técnicos Específicos (exemplo: configuração de parâmetros aplicacionais). Por sua vez, dever-se-ão seguir as Auditorias aos Controlos de Gestão da função SI, verificando o cumprimento das normas existentes na função SI e a sua coerência e alinhamento com a restante organização. Este tipo de Auditorias deverão começar por avaliar as Normas Gerais dos SI (exemplo: áreas de SI com lacunas de normas) e só depois avaliar os Procedimentos Gerais dos SI (exemplo: procedimentos de *backup* e recuperação).

Com esta breve descrição de uma visão diferente e complementar sobre os controlos de SI, conclui-se esta secção que se espera tenha contribuído para melhorar a percepção daquilo que pode constituir o âmbito da Auditoria de SI.

3.4 OS REFERENCIAIS METODOLÓGICOS DA FUNÇÃO

Como tivemos oportunidade de compreender na secção anterior, os controlos de SI podem estar associados a diferentes níveis: Governo, Gestão e Técnicos. No topo, devem ser definidas as políticas de Governo dos SI, a partir das quais se derivam as normas/controlos a aplicar nos níveis de Gestão e Técnicos. Este exercício de definição de normas/controlos para os SI é, hoje em dia, facilitado pela existência de normas (*standards*) internacionais de SI que habitualmente incorporam modelos estruturados (*frameworks*) e que aqui optámos por designar por referenciais. Estes referenciais poderão constituir verdadeiras metodologias para a execução das funções de Gestão dos SI e também para serem utilizados na função de Auditoria de SI.

Esta secção aborda a adopção destes referenciais metodológicos pelas organizações, bem como quais é que se adequam aos níveis de controlo de SI acima referidos e, fundamentalmente, como se podem adequar às actividades de Auditoria de SI.

3.4.1 A ADOPÇÃO DE REFERENCIAIS

As organizações podem encarar o Governo dos SI (*IT Governance*) com uma abordagem *ad-hoc*, através da criação dos seus próprios referenciais, baseados na experiência existente na organização ou, em alternativa, podem adoptar normas internacionais que foram desenvolvidas e aperfeiçoadas recorrendo à experiência acumulada ao longo de anos, por um conjunto alargado de organizações e de profissionais que se tentam posicionar na vanguarda dos SI. Esta última opção é apresentada e defendida por (Spafford, 2003) como sendo a mais acertada. Para este autor, existem benefícios na adopção de referenciais pois estes têm as seguintes características:

- São já existentes → Poderão não existir vantagens em investir tempo e esforço no desenvolvimento de um referencial metodológico próprio baseado na experiência e no conhecimento limitado de uma só organização quando já existem normas internacionais de SI disponíveis.
- São estruturados → As normas internacionais de SI habitualmente incorporam modelos estruturados que facilitam a compreensão das normas e a sua adaptação pelas organizações.

Para além disso, o facto de serem estruturados permite que todas as partes interessadas nos SI (*stakeholders*) tenham uma referência que é comum e que permite perceber aquilo que podem esperar dos SI.

- Incorporam as melhores práticas → As normas vão sendo construídas e melhoradas progressivamente ao longo dos anos, passando por um processo de avaliação por inúmeras organizações e profissionais de SI. Esta experiência acumulada de melhores práticas não é possível de alcançar com o esforço de uma só organização.
- Permitem a partilha de conhecimento → Adoptando normas globalmente aceites para os SI, as organizações podem beneficiar da partilha de conhecimento e de ideias (exemplos: grupos de utilizadores, *websites*, revistas, livros, etc.). Os referenciais próprios de uma só organização não beneficiam desta partilha.
- São auditáveis → Sem a existência de normas de Gestão de SI, a missão da Auditoria de SI é dificultada ou, pelo menos, não fica tão facilitada para ser executada de um modo mais eficaz. Isto significa que, para além da Gestão de SI dever utilizar estas normas, os próprios Auditores de SI deverão também utilizá-las, em vez das habituais práticas *ad-hoc* de Auditoria. O intuito deverá ser auditar os SI da organização por comparação com, pelo menos, uma norma de SI internacionalmente aceite. Tendo esta posição de partida, recorrentemente deverão ser efectuadas recomendações de acordo com a norma adoptada e, de preferência, adoptar outras normas complementares.

Ainda na linha de opinião de (Spafford, 2003), não existe uma resposta pré-determinada para a questão: Qual o melhor referencial a seleccionar para a Gestão de SI e para a Auditoria de SI?

Mais do que seleccionar um referencial, as organizações devem ser capazes de ter uma visão apreciativa sobre os diversos referenciais de SI existentes e planear a implementação dum referencial seu que combine/integre as melhores práticas de entre vários referenciais já existentes, garantindo compatibilidade com as necessidades da organização.

A implementação de referenciais pode derivar duma necessidade sentida internamente na organização ou de um estímulo externo. Aquele autor dá como exemplo o facto de entidades reguladoras e até mesmos os clientes deverem pressionar as organizações para implementarem

normas base relacionadas com a segurança dos SI. Assim, o domínio da segurança deve ser o ponto de partida de qualquer organização para a implementação de normas de SI. No entanto, as organizações não se devem limitar a este tipo de normas, devendo progressivamente estende-las para outros domínios dos SI.

Neste contexto, o caminho passa por não só adoptar as normas mas também adaptá-las e integrá-las num referencial que seja útil para a organização. Hoje em dia, os profissionais de SI já não deverão questionar a utilidade da sua adopção, mas sim o modo como fazer a correcta adaptação.

Na adaptação correcta das normas, há que garantir que elas incorporam, pelo menos, um conjunto mínimo de princípios de Governo dos SI que, segundo o (ITGI & OGC, 2005), passam por:

- Alinhamento Estratégico → Alinhar as normas de SI com foco no negócio e em soluções colaborativas com este.
- Acréscimo de Valor → Acrescentar valor à organização através de normas que se centrem na optimização de custos e na valorização dos SI.
- Gestão do Risco → Gerir os riscos com impacto nos SI (já em exploração ou ainda em projecto de investimento), através de normas que deverão contemplar a salvaguarda dos activos de SI, bem como a recuperação de desastres e a continuidade de negócio.
- Gestão dos Recursos → Gerir os recursos de SI através de normas que promovam a optimização do conhecimento (recursos humanos) e da infra-estrutura (recursos físicos).
- Medição do Desempenho → Medir o desempenho dos SI através de normas que permitam controlar os projectos de SI e monitorar a prestação dos serviços de SI.

Como podemos constatar através destes princípios resumidos por (ITGI & OGC, 2005), os referenciais de SI deverão garantir alinhamento com o negócio e com o Governo das Sociedades (*Corporate Governance*) em geral, isto para além dos requisitos técnicos que são já habitualmente considerados. Neste enquadramento, a adopção de referenciais deverá permitir a definição das responsabilidades (*accountability*) e dos níveis de decisão (*decision rights*) para os SI. Possuir uma organização bem definida (responsabilidades sobre SI) e os papéis de cada um

clarificados (decisão sobre os SI) são dois objectivos de Gestão de SI que ficam facilitados quando se utilizam referenciais de SI. Por outro lado, estes dois objectivos deverão ser encarados também como dois objectivos de controlo de SI, a avaliar pela Auditoria de SI.

Para (LeBlanc, 2004), deve ser efectuado um esforço para estabelecer pontos de integração entre alguns dos diversos referenciais de SI disponíveis e determinar quais as áreas de cada um que podem ser aplicáveis a cada organização em particular.

Para ilustrar uma possível utilização dos referenciais, este autor evocou os conceitos do método *Six Sigma*. Este é um método estatístico de melhoria da qualidade dos processos, desenvolvido pelo grupo Motorola, baseado numa visão de serviço ao cliente. O método prevê 5 principais fases: Definição (*Define*); Medição (*Measure*); Análise (*Analyse*); Melhoria (*Improve*) e Controlo (*Control*). Embora este método tenha sido originalmente desenvolvido para processos de fabrico industrial com o intuito de reduzir a produção de defeituosos, o referido autor sugere que os conceitos poderão ser transpostos para os serviços de SI e TIC, implementando um programa de melhoria contínua do serviço.

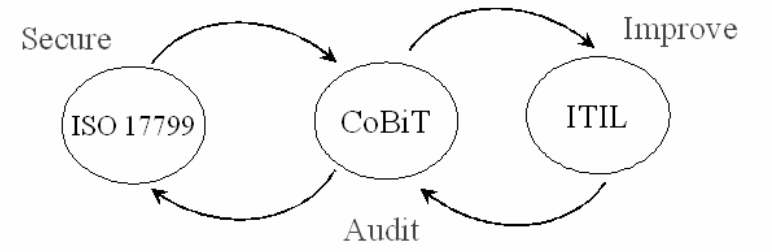


Figura 3.6 - Três Referênciais Metodológicos Integrados

Fonte: Versão original extraída de (LeBlanc, 2004): "*Integrated Trio*"

Neste contexto de melhoria contínua, poderemos efectuar uma possível interpretação do esquema proposto por (LeBlanc, 2004) que relaciona três dos referenciais metodológicos. Em primeiro lugar, numa fase de Definição (*Define*), os SI devem ser tornados seguros (*Secure*), condição base para que os serviços de SI possam ser prestados. Em fases seguintes, decorre a prestação dos serviços de SI aos clientes, durante as quais deve ser efectuada a Medição (*Measure*) e a Análise (*Analyse*) dos dados relativos à qualidade dos serviços. Estas duas

actividades poderão ser efectuadas periodicamente no âmbito de uma Auditoria (*Audit*) ou serem actividades já habituais no processo de prestação do serviço. Numa fase seguinte, após a interpretação destes dados, devem ser identificadas medidas para Melhoria (*Improve*) dos serviços. O ciclo recomeça no sentido inverso, numa fase de Controlo (*Control*), em que se deverá controlar através de uma Auditoria (*Audit*) as melhorias entretanto implementadas. Na sequência destas, poderá fazer sentido efectuar a Definição (*Define*) de novas medidas de segurança que melhorem a qualidade dos serviços de SI. Deste modo, o ciclo de melhoria contínua inverteu-se novamente e reiniciou-se, continuando sucessivamente na busca da melhoria da qualidade dos SI.

O referido autor defende que o referencial metodológico de SI mais adequado para a definição das medidas de Segurança (*Secure*) é a ISO 17799, para a Auditoria (*Audit*) é o CobiT e para a Melhoria (*Improve*) é o ITIL.

De seguida, na próxima secção, são desenvolvidos os conceitos destes três referenciais metodológicos mencionados, onde será possível avaliar a adequação de cada um deles.

3.4.2 Uma Selecção de 3 Referenciais: CobiT, ITIL e ISO 17799

Estes três referenciais seleccionados (CobiT, ITIL e ISO 17799) são os mais mencionados pela literatura que aborda a Auditoria de SI e são também os utilizados de forma mais comum pelos profissionais de SI a nível internacional.

Na tabela seguinte é efectuada uma apresentação dos três referenciais, comparando-os quanto a alguns dos seus elementos caracterizadores. De seguida é efectuada uma apresentação dos respectivos modelos estruturados, acompanhada por breves comentários.

Note-se que não é do âmbito deste trabalho desenvolver ou detalhar os referenciais. A sua caracterização e breve descrição tem apenas como objectivo dar a conhecê-los a alto nível,

fazendo a ponte para a próxima secção em que se identificam as actividades de Auditoria de SI previstas nesses referenciais.

	COBIT	ITIL	ISO 17799
Nome	▪ *Control Objectives for Information and related Technology*	▪ *The Information Technology Infrastructure Library*	▪ *ISO 17799 Information Technology - Code of Practice for Information Security Management*
Entidade Responsável	▪ *IT Governance Institute / ISACA - Information Systems Audit and Control Association (USA)*	▪ *OGC – The Office of Government Commerce (UK)*	▪ *ISO - International Organizational for Standardization & IEC - International Electrotechnical Comission (Joint Technical Committee ISO/IEC JTC 1) (Switzerland)*
Primeira versão	▪ CobiT *1st Edition* (1996)	▪ ITIL v1 Library (1988)	▪ ISO/IEC 17799:2000
Última versão	▪ CobiT *4th Edition* (2005)	▪ ITIL v3 Library (2007)	▪ ISO/IEC 17799:2005
Versão analisada	▪ **CobiT *3rd Edition* (2000)**	▪ **ITIL *v2 Library* (1999)**	▪ **ISO/IEC 17799:2000**
Relacionados / Antecedentes / Subsequentes	▪ Em 1997 são lançados os *SISAS - Statements on Information Systems Auditing Standards* que definem o modo como os Auditores de SI devem executar as Auditorias de SI. ▪ Com o mesmo propósito, e substituindo todos os anteriores, em 2005 são lançados os *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*.	▪ Com a contribuição do itSMF (*Information Technology Service Managment Forum*), a partir de 2000 o ITIL passou a ser considerado como a melhor prática para as organizações conseguirem a certificação na *British Standard for IT Service Management* (BS 15000): *- Part 1 : Specification for Service Management* *- Part 2 : Code of Practice for Service Management* ▪ Espera-se que a BS 15000 se transforme definitivamente no standard ISO/IEC 20000.	▪ Teve origem em 1993numa *British Standard* (BS 7799), da qual existiram duas partes: *- Part 1 : Information Technology – Code of Practice for Information Security Management* *- Part 2 : Information Security Management Systems – Specification with Guidance for Use* ▪ *Part* 1 transformou-se na ISO 17799 em 2000 e a *Part* 2 na ISO 27001 em 2005. ▪ Durante 2007 a ISO/IEC 17799:2005 (*Part* 1) passará a ISO/IEC 27002, inserida na nova série de standards ISO/IEC 2700x dedicada à Segurança.
Génese	▪ Auditar os processos de SI	▪ Organizar e estruturar as áreas dos SI	▪ Garantir a segurança da informação
Objectivo	▪ Governo dos SI	▪ Gestão de Serviços de SI	▪ Gestão da Segurança da Informação
Foco	▪ Alinhamento dos SI com o Negócio	▪ Qualidade dos Serviços de SI	▪ Segurança da Informação
Visão	▪ Visão de gestão dos processos de SI	▪ Visão operacional dos serviços de SI	▪ Visão sistémica da informação
Conveniência	▪ Orientador, integrador, controlador	▪ Auxiliador, estruturador, aperfeiçoador	▪ Basilar, protector
Proficiência	▪ Em controlos	▪ Em processos	▪ Em procedimentos
Destinatários	▪ Gestores de Topo ▪ Gestores de SI ▪ Auditores de SI	▪ Gestores de Serviços de SI ▪ (Auditores de SI)	▪ Gestores da Segurança da Informação ▪ (Auditores de SI)
Níveis de controlos (na versão analisada)	▪ N1 → 4 domínios ▪ N2 → 34 processos de controlo de alto nível ▪ N3 → 318 actividades de controlo detalhadas	▪ N1 → 2 módulos/livros *core* + 5 módulos/livros complementares ▪ N2 → 11 processos *core* + (n/d) processos complementares ▪ N3 → (n/d) processos detalhados	▪ N1 → 10 áreas ▪ N2 → 37 controlos de segurança de alto nível ▪ N3 → 127 controlos de segurança detalhados

Tabela 3.2 - Comparação de Elementos Caracterizadores: CobiT vs. ITIL vs. ISO 17799

Fonte: Compilado pelo autor a partir de várias fontes, incluindo (ITGI,2000), (OGC,2004) e (BSI, 2005)

Pela análise dos elementos caracterizadores apresentados na tabela anterior pode-se concluir que de um modo geral, e salvo as situações que serão de seguida indicadas, dos 3 referenciais apresentados, o CobiT será o referencial a ser aplicado preferencialmente na Auditoria de SI.

As razões que fundamentam esta conclusão são:

- Na génese do CobiT esteve a necessidade de criar um referencial para auditar os processos de SI. O ITIL teve uma origem não tão abrangente (a organização e a estruturação das áreas de SI) enquanto que o ISO 17799 nasceu especializado apenas na segurança da informação.
- A entidade responsável pela elaboração do CobiT é uma Associação de Auditores de SI (*ISACA – Information Systems Audit and Control Association*), o que não acontece com os outros dois referenciais.
- O CobiT possui uma visão de gestão dos processos de SI e privilegia o alinhamento destes com o negócio (factores que são importantes para o paradigma defendido para a Auditoria de SI, tal como vimos na secção 3.2.1). O ITIL também considera o alinhamento com o negócio (como iremos ver mais à frente), mas está focado na qualidade dos Serviços de SI e possui uma visão mais operacional, factores que o tornam mais adequado para Auditoria de SI quando os objectos da Auditoria forem serviços e não processos de SI abrangentes. O ISO 17799 será o referencial mais adequado nos casos de auditoria à informação e à sua segurança nos SI, uma vez que possui uma visão sistémica da informação.
- O CobiT é útil para as organizações enquanto instrumento orientador e integrador de controlos de SI em todos os níveis de Governo dos SI, pelo que também será um referencial sobre o qual todos os tipos controlos de SI poderão ser auditados. O ITIL poderá ser um referencial adequado para auditar os processos de Gestão de Serviços de SI e o ISO 17799 para auditar os procedimentos básicos de Gestão da Segurança da Informação.
- Como consequência, os destinatários privilegiados do CobiT são os Auditores de SI, sendo também utilizado pelos Gestores de Topo e Gestores de SI. Nos casos do ITIL e do ISO 17799, a utilização pelos Auditores de SI deve ser favorecida apenas nas situações anteriormente indicadas, uma vez que estes dois referenciais são mais adequados para utilização pelos Gestores de Serviços de SI e pelos Gestores da Segurança da Informação respectivamente.

De seguida será efectuada uma breve apresentação dos modelos estruturados (*frameworks*) que representam os 3 referenciais, pela ordem em que têm sido tratados (CobiT, ITIL e ISO 17799).

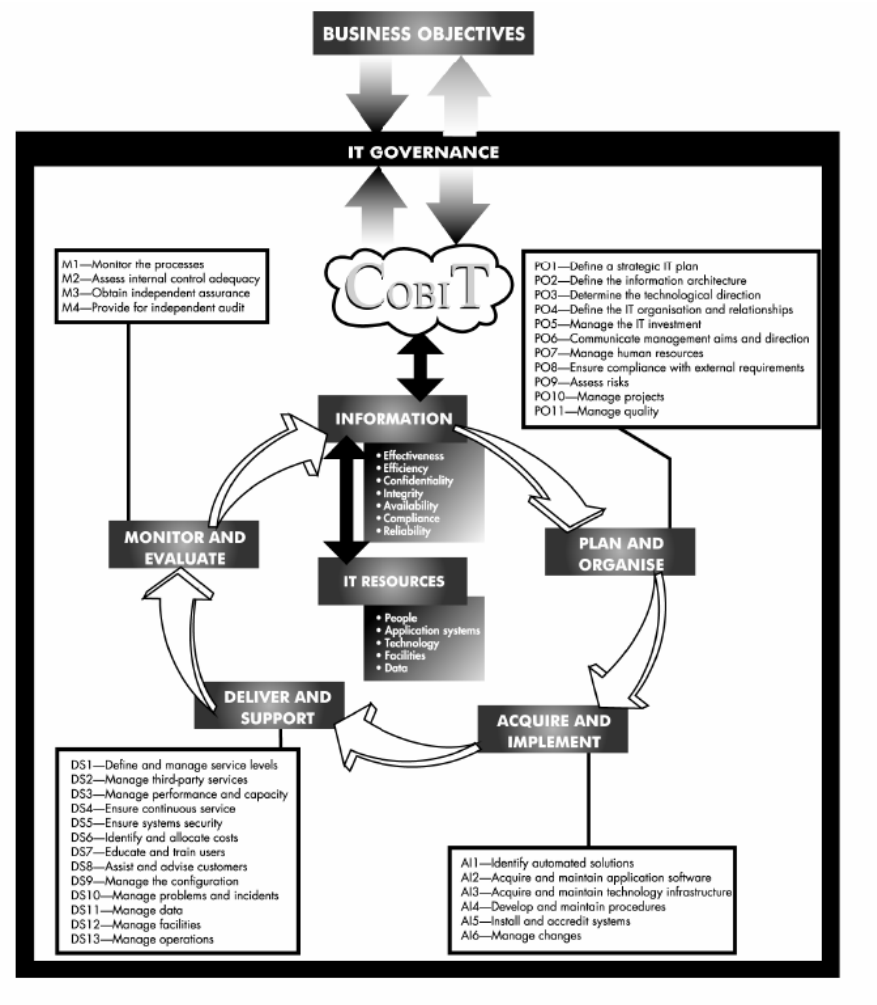


Figura 3.7 - *Framework* CobiT

Fonte: Versão original extraída de (ITGI, 2004): "*COBIT IT Processes Defined Within the Four Domains*"

A principal premissa do CobiT, visível no topo da figura, é a orientação para o negócio, ou seja, todos os processos de SI devem estar alinhados com o Governo dos SI que, por sua vez, deverá estar alinhado com os objectivos de negócio (por via do Governo das Sociedades).

Este modelo estruturado considera 5 tipos de recursos de SI (as pessoas, os sistemas aplicacionais, a tecnologia, as instalações e os dados) que, em conjunto, possibilitam a produção e o suporte da informação de negócio, tendo em conta 7 princípios essenciais (eficácia, eficiência, confidencialidade, integridade, disponibilidade, conformidade e fiabilidade).

Para providenciar a informação que o negócio necessita para atingir os seus objectivos, os recursos de SI são geridos através de processos de SI. Cada um destes processos deverá possui controlos de SI subjacentes.

O referencial CobiT considera os controlos de SI agrupados em 4 grandes domínios que trabalham em conjunto, de um forma cíclica, para possibilitarem a existência de uma organização bem suportada em termos de SI, optimizada com base nas prioridades e nos recursos da organização. Os 4 domínios são:

- Planear e Organizar (*PO - Plan and Organize*)
- Adquirir e Implementar (*AI - Acquire and Implement*)
- Produzir e Suportar (*DS - Deliver and Support*)
- Monitorar e Avaliar (*M - Monitor and Evaluate*)

Cada um destes 4 domínios é constituído por um conjunto de processos de SI (34 no total) que correspondem a objectivos de controlo de alto nível. Por sua vez, estes processos são constituídos por actividades de SI (318 no total) que correspondem a objectivos de controlo detalhados.

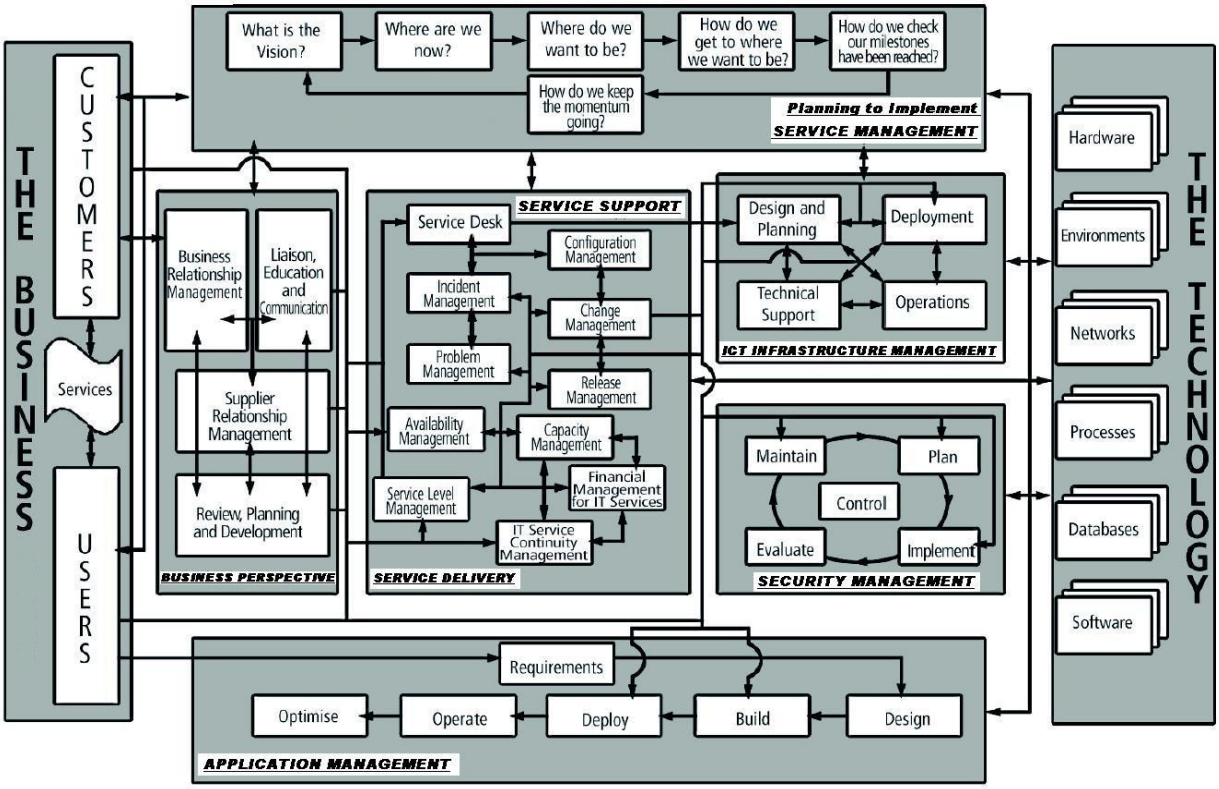


Figura 3.8 - *Framework* ITIL

Fonte: Adaptado da versão original de (OGC, 2004): "*The 'big picture' of ITIL Processes*"

O referencial ITIL toma como ponto de partida, não só a tecnologia existente, mas também as necessidades do negócio ao nível de Serviços de SI (visível na figura nos blocos mais à esquerda e mais à direita). O ITIL centra-se fundamentalmente na Gestão dos Serviços de SI que tem como objectivos a produção (*delivery*) e o suporte (*support*) dos Serviços de SI que sejam adequados aos requisitos da organização (bloco no centro da figura).

O ITIL é considerado por grande parte dos Gestores de SI como sendo um conjunto coerente de melhores práticas (*guidelines*) para a Gestão de Serviços de SI e para a totalidade dos processos com eles relacionados (*end-to-end processes*). Privilegia as seguintes abordagens: promoção da qualidade dos Serviços de SI; visão holística da Gestão dos Serviços de SI; orientação para o negócio (cliente/utilizador); e uso eficaz/eficiente dos SI.

Os 2 módulos nucleares (*core*) do modelo estruturado e respectivos processos são:

- Suporte aos Serviços (*Service Support*) → Gestão de Incidentes (*Incident Management*); Gestão de Problemas (*Problem Management*); Gestão de Configurações (*Configuration Management*); Gestão de Alterações (*Change Management*); Gestão de Versões (*Release Management*); Apoio aos Serviços (*Service Desk*).
- Produção dos Serviços (*Service Delivery*) → Gestão de Capacidade (*Capacity Management*); Gestão de Disponibilidade (*Availability Management*); Gestão de Níveis de Serviço (*Service Level Management*); Gestão de Continuidade de Serviços (*IT Service Continuity Management*); Gestão Financeira dos Serviços (*Financial Management for IT Services*).

Os restantes 5 módulos complementares do ITIL são mais latos, pois para além da Gestão dos Serviços de SI, abordam aspectos relacionados com a definição e o desenvolvimento de processos eficazes de SI. Os temas tratados pelos seus respectivos processos são os seguintes:

- Gestão da Infraestrutura de TIC (*ICT Infrastructure Management*) → É muito abrangente em termos de processos de gestão das tecnologias (arquitectura e planeamento, entrada em produção, operação, suporte técnico, etc.).
- Gestão de Aplicações (*Application Management*) → Inclui processos de desenvolvimento de *software* usando uma perspectiva de ciclo de vida de desenvolvimento, com foco na rigorosa definição dos requisitos aplicacionais em função das necessidades do negócio.
- Gestão da Segurança (*Security Management*) → Aborda os processos de planeamento, de gestão e de resposta a incidentes relativos aos níveis de segurança da informação e das TIC.
- Planeamento da Implementação da Gestão dos Serviços (*Planning to Implement Service Management*) → Prevê os processos essenciais no planeamento e na implementação da Gestão de Serviços de SI.
- A Perspectiva de Negócio (*The Business Perspective*) → Aborda os processos de relacionamento e de comunicação da Gestão dos SI com o negócio, incluindo a restante organização e entidades externas.

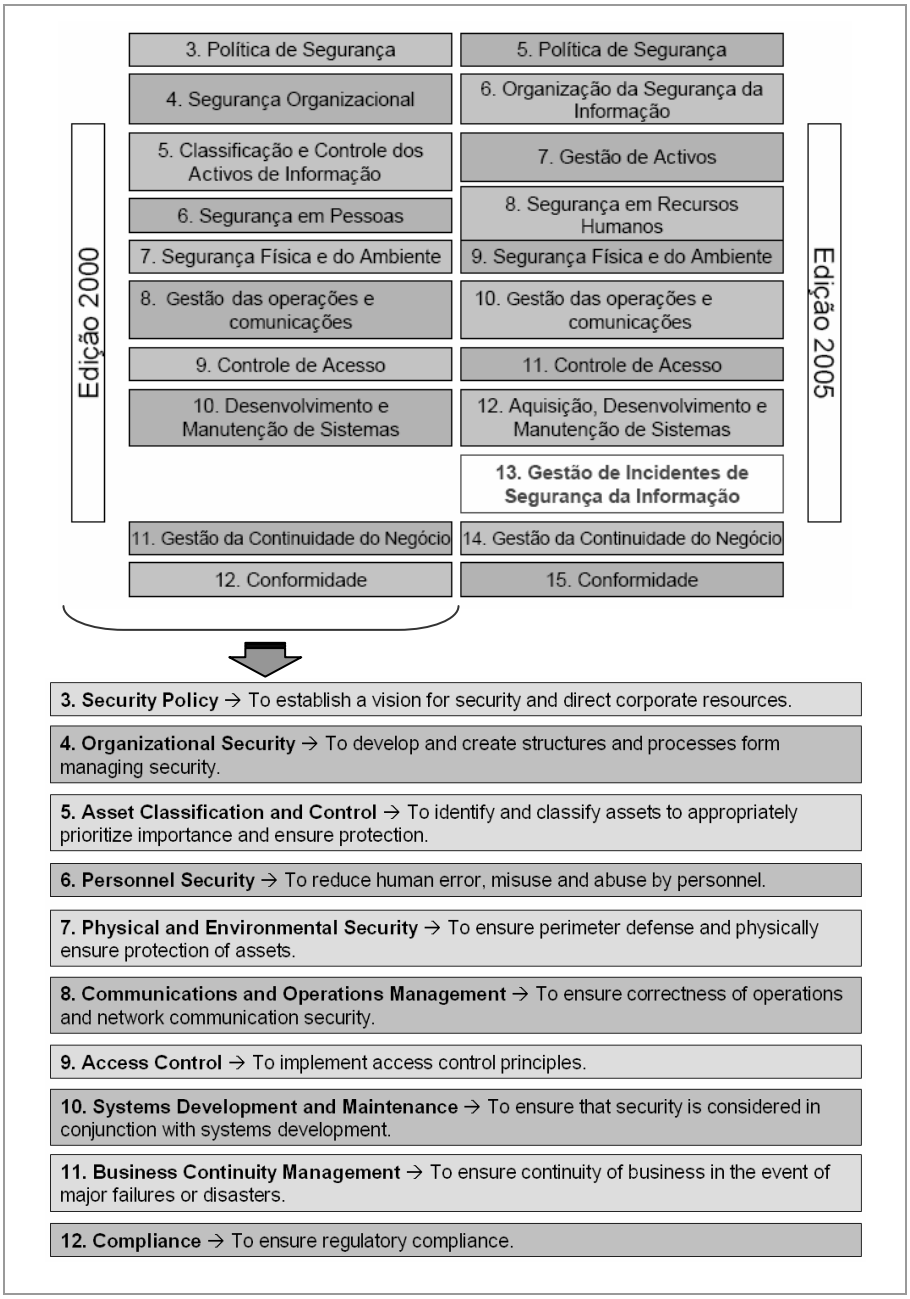


Figura 3.9 - *Framework* ISO 17799

Fonte: Adaptado das versões originais de

(BSI, 2006): "ISO 17799:2000 x 2005" & (Dhillon, 2006): "*Summary of ISO 17799 Controls*"

No que diz respeito ao referencial ISO 17799, não existe um modelo estruturado formalmente definido, dado não existir uma representação gráfica original (à semelhança das existentes no CobiT e no ITIL). No entanto, para facilitar a apresentação do ISO 17799, o autor da presente

investigação elaborou uma representação gráfica básica, adaptando a informação de duas fontes (BSI, 2006) e (Dhillon, 2006).

O referencial ISO 17799 constitui um Código de Boas Práticas para Gestão da Segurança da Informação. Tem por objectivo a implementação de controlos de segurança da informação nas organizações. Deve ser encarado como uma base a partir da qual podem ser desenvolvidas políticas de segurança e práticas de gestão da informação nas organizações, permitindo melhorar a sua confiança na informação.

Este referencial é constituído por 10 grandes áreas que, por sua vez, se desdobram em diversos controlos de segurança de alto nível e controlos de segurança detalhados. Na representação gráfica encontram-se indicadas as 10 áreas bem como uma breve descrição de cada uma (a numeração inicia-se no número 3. dado que os capítulos 1. e 2. da norma dizem respeito ao âmbito e aos termos e definições).

As orientações sobre segurança da informação previstas na ISO 17799, que se concretizam nos controlos de segurança, têm fundamentalmente duas motivações:

- Requisitos legais → Protecção e não divulgação de dados pessoais; Protecção de informação interna; Protecção de direitos de propriedade intelectual.
- Boas práticas geralmente aceites → Política de segurança da informação; Atribuição de responsabilidades pela segurança da informação; Escalada de problemas; Gestão da continuidade de negócio.

Os controlos de segurança da informação podem ser complementados ou melhorados através da aplicação do referencial ISO 27001 - Requisitos para Sistemas de Gestão da Segurança da Informação. Trata-se de um instrumento complementar que permite à gestão monitorizar e controlar a segurança da informação, minimizar o risco da sua utilização indevida e assegurar conformidades com requisitos legais e regulatórios.

3.4.3 As Actividades de Auditoria de SI previstas nos Referenciais

Uma vez efectuada a apresentação e descrição dos modelos estruturados relativos aos 3 referenciais em análise, estamos agora em condições de proceder à identificação de quais as actividades directamente relacionadas com Auditoria de SI ou que são específicas desta e que os referenciais prevêem.

Para tal, dado que na secção anterior se concluiu que o CobiT é o referencial mais abrangente para a Auditoria de SI, tomou-se o CobiT como ponto de partida para a identificação das actividades de Auditoria de SI. Recorreu-se igualmente aos referenciais ITIL e ISO 17799 para a identificação dessas actividades uma vez que estes referenciais são mais específicos em alguns aspectos.

Aplicou-se a metodologia de análise abaixo descrita, da qual resultou a tabela resumo da próxima página. Os resultados detalhados da análise encontram-se no **Anexo 1: Actividades de Auditoria de SI previstas no CobiT, ITIL e ISO 17799**.

Metodologia de análise:

- Para efectuar a correspondência entre os objectivos de controlo do CobiT e os controlos do ITIL e ISO 17799, utilizou-se como suporte o trabalho desenvolvido por (ITGI & OGC, 2005): "*Mapping ITIL and ISO 17799 to CobiT Control Objectives*"
- Tomou-se o referencial CobiT como sendo a base da análise, ficando este colocado do lado esquerdo da tabela. Seguem-se na tabela o ITIL e ISO 17799.
- Para cada um destes 3 referenciais, dividiram-se os controlos em três níveis (Nível 1, 2 e 3), de acordo com os próprios critérios de classificação de cada um dos referenciais (para o ISO 17799 apenas existiu informação para efectuar o exercício até o Nível 2).
- Para cada um dos níveis de controlo do CobiT (Nível1: Domínio; Nível 2: Controlo de alto nível; Nível 3: Controlo detalhado) verificou-se se o respectivo nome indicava alguma actividade directamente relacionada ou específica de Auditoria de SI. Em caso de dúvida, foi analisado o texto do controlo. De um modo subsidiário, efectuou-se o mesmo tipo de exercício

para o ITIL e ISO 17799. Nos casos em que o CobiT não previa actividades de Auditoria mas o ITIL e ISO 17799 previam, enquadraram-se as actividades destes dois últimos no CobiT.

- Todos os casos em que existia pelo menos uma actividade de Auditoria de SI foram indicados na tabela de análise, de acordo com a legenda e os resultados detalhados que são apresentados no **Anexo 1**.

CobiT			ITIL			ISO 17799	
Level 1	Level 2	Level 3	Level 1	Level 2	Level 3	Level 1	Level 2
PO - Plan and Organise	PO1 - Define a Strategic IT Plan	1	Planning to Implement Service Management	1	1	-	-
	PO4 - Define the IT Organisation and Relationships	1	-	-	-	12 - Compliance	1
	PO6 - Communicate Management Aims and Direction	5	Security Management; Planning to Implement Service Management; Service Support; Service Delivery	4	4	12 - Compliance	1
	PO8 - Ensure Compliance With External Requirements	6	-	-	-	4 - Organizational Security 5 - Asset Classification and Control 7 - Physical and Environmental Security 8 - Communications and Operations Management 10 - Systems Development and Maintenance 12 - Compliance	10
	PO9 - Assess Risks	8	ICT Infrastructure Management; Service Delivery; The Business Perspective	4	5	3 - Security Policy 4 - Organizational Security 5 - Asset Classification and Control 7 - Physical and Environmental Security 9 - Access Control 10 - Systems Development and Maintenance	10
AI - Acquire and Implement	AI1 - Identify Automated Solutions	1	-	-	-	9 - Access Control 10 - Systems Development and Maintenance 12 - Compliance	4
	AI2 - Acquire and Maintain Application Software	1	Appplication Management	-	1	4 - Organizational Security 9 - Access Control 10 - Systems Development and Maintenance	3
	AI3 - Acquire and Maintain Technology Infrastructure	1	ICT Infrastructure Management	2	2	12 - Compliance	1
DS - Deliver and Support	DS5 - Ensure Systems Security	5	Security Management	1	1	12 - Compliance	2
	DS7 - Educate and Train Users	1	-	-	-	12 - Compliance	1
	DS11 - Manage Data	5	-	-	-	12 - Compliance	1
	DS13 - Manage Operations	1	-	-	-	12 - Compliance	1
M - Monitor	M1 - Monitor the Processes	4	ICT Infrastructure Management; Service Delivery; Service Support; The Business Perspective; Planning to Implement Service Management	7	11	12 - Compliance	1
	M2 - Assess Internal Control Adequacy	4	-	-	-	3 - Security Policy 4 - Organizational Security 6 - Personnel Security 8 - Communications and Operations Management 12 - Compliance	8
	M3 - Obtain Independent Assurance	8	-	-	-	4 - Organizational Security 12 - Compliance	4
	M4 - Provide for Independent Audit	8	-	-	-	12 - Compliance	1

Includes:
Technical competence, skills and knowledge

Tabela 3.3 - Actividades de Auditoria de SI previstas nos Referenciais (resumo)

Fonte: Levantamento elaborado pelo autor com base nos dados de (ITGI & OGC, 2005):
"*Mapping ITIL and ISO 17799 to CobiT Control Objectives*"

Como principais conclusões, quanto ao CobiT, podemos destacar a existência de 7 objectivos de controlo de alto nível (PO6, PO8, AI1, AI2, M1, M2, M3) que incluem referências a actividades directamente relacionadas com Auditoria de SI (assinaladas a sombreado mais claro na tabela resumo acima). Para além disso, existem 2 objectivos de controlo de alto nível que se referem a

actividades específicas de Auditoria de SI ou de Gestão de Risco de SI (assinaladas a sombreado mais escuro na tabela resumo acima):

- Avaliação de Riscos (*PO9 – Assess Risks*)
- Auditoria Independente (*M4 – Provide for Independent Audit*)

Pela observação da tabela detalhada no **Anexo 1**, verifica-se que o objectivo de controlo "Auditoria Independente" (M4) corresponde, de um modo geral, aos conteúdos que constituem os designados "Referenciais, Orientações e Procedimentos para Auditoria de SI" (*IS Standards, Guidelines and Procedures for Auditing*) emitidos pela (ISACA, 2005).

Os "Referenciais de Auditoria de SI" (*IS Auditing Standards*) são de utilização obrigatória nos relatórios de Auditoria pelos Auditores de SI que sejam profissionalmente certificados pela ISACA. Por sua vez, as "Orientações de Auditoria de SI" (*IS Auditing Guidelines*) são detalhes de como cumprir os Referenciais, podendo existir situações em que o Auditor não siga exactamente as Orientações, devendo justificar o modo como o trabalho foi executado. Por último, os "Procedimentos de Auditoria de SI" (*IS Auditing Procedures*) são exemplos dos passos de execução da Auditoria, sendo de natureza informativa.

Os "Referenciais de Auditoria de SI" (*IS Auditing Standards*) previstos pela ISACA para a profissão de Auditor de SI são os seguintes:

- Carta de Auditoria (*S1 - Audit Charter*)
- Independência (*S2 - Independence*)
- Ética Profissional e Referenciais (*S3 - Professional Ethics and Standards*)
- Competências (*S4 - Competence*)
- Planeamento (*S5 - Planning*)
- Desempenho do Trabalho de Auditoria (*S6 - Performance of Audit Work*)
- Relatórios (*S7 - Reporting*)
- Actividades de Acompanhamento/seguimento (*S8 - Follow-Up Activities*)
- Irregularidades e Actos Ilegais (*S9 - Irregularities and Illegal Acts*)
- Governo dos SI (*S10 - IT Governance*)
- Uso da Avaliação de Riscos no Planeamento de Auditoria (*S11 - Use of Risk Assessment in Audit Planning*)

Destaca-se a existência de um referencial para as Competências (*S4 - Competence*) que aborda as competências técnicas e não técnicas, bem como os conhecimentos que os Auditores de SI devem possuir (desenvolveremos este ponto no Capítulo 4, relativo ao Modelo de Competências).

Para encerrar as conclusões sobre as actividades de Auditoria de SI previstas no referencial CobiT, deixa-se aqui uma citação em que a (ISACA, 2005) atribui uma forte ênfase à relação entre os referenciais (*standards*) e as competências (*skills*) profissionais:
"*The specialised nature of information systems auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing*."

No que diz respeito ao referencial ITIL, tal como se pode constatar pela análise da tabela detalhada no **Anexo 1**, não possui nenhum controlo de Nível 1 (Módulos) ou de Nível 2 (Processos) dedicados especificamente à Auditoria de SI.

No entanto, existem alguns controlos de Nível 3 (Processos Detalhados) com actividades directamente relacionadas com Auditoria de SI e que estão mais adequados ou aprofundados do que os outros dois referenciais (exemplos: 4.3 - *Audit and Evaluate* ; 5.1.1 - *Business view on risk* ; 7.4 - *Ongoing monitoring and process reviews* ; 8.9.3 - *Central Computer and Telecommunications Agency Risk Analysis and Management Method*).

Relativamente ao referencial ISO 17799, dada a sua natureza procedimental, atribui um grande destaque às questões de Conformidade. De facto, recorrendo novamente à tabela detalhada no **Anexo 1**, verifica-se a existência de um controlo de Nível 1 (Área *12 - Compliance*) que contém os seguintes três controlos de Nível 2 (Controlos de segurança de alto nível) com actividades directamente relacionadas com Auditoria de SI:

- Conformidade com requisitos legais (*12.1 - Compliance with legal requirements*)
- Revisão da política de segurança e da conformidade técnica (*12.2 - Reviews of security policy and technical compliance*)
- Considerações sobre Auditoria de SI (*12.3 - System audit considerations*)

Em forma de conclusão sobre as actividades de Auditoria de SI previstas nos referenciais, podemos afirmar que o CobiT é o que possui mais actividades directamente relacionadas e até indica algumas específicas para Auditoria de SI. O ITIL é, dos 3 referenciais, o menos direccionado para as actividades de Auditoria de SI, enquanto que o ISO 17799 está mais vocacionado para actividades de Auditoria de SI relacionadas com a conformidade da segurança da informação.

Constata-se pois que existem algumas partes destes 3 referenciais que orientam, em específico, o modo como as actividades de auditoria de SI devem ser executadas. Relativamente às restantes partes, e não entrando em contradição com a conclusão acima, considera-se que qualquer uma delas poderá ser utilizada pelos Auditores de SI como uma referência dos processos de SI sobre a qual os poderão auditar. Tal como tivemos oportunidade de entender na secção 3.4.1, o importante é não executarmos a Auditoria de SI de um modo *ad-hoc*, mas sim adoptarmos um ou mais referenciais (ou uma combinação destes) que sejam úteis para o trabalho do Auditor.

3.5 Os Processos da Função

Esta secção trata fundamentalmente de processos de Gestão das Auditorias de SI que o Auditor deverá realizar. Começar-se-á por identificar um modelo e um conjunto de orientações a ter em conta na definição de um planeamento anual para as Auditorias de SI. Situando-nos já ao nível das Auditorias individuais, apresentaremos algumas visões sobre as fases que constituem uma Auditoria de SI. Uma vez compreendidas as principais fases e respectivos principais conteúdos, estaremos em condições de compreender que estas fases de uma Auditoria podem ser geridas como se tratassem das fases de um projecto. Utilizando o modelo estruturado da Gestão de Projectos, passar-se-á à definição da estrutura de uma Auditoria de SI. Completar-se-á com a apresentação de um conjunto de técnicas de Gestão das Auditorias de SI, a aplicar em cada um dos principais parâmetros que definem uma Auditoria (objectivos, âmbito, tempo, recursos, comunicação, qualidade, riscos, produtos resultantes, etc.).

3.5.1 O Planeamento das Auditorias de SI

Os principais factores a tomar em consideração na elaboração de um planeamento para as Auditorias de SI estão contidos no seguinte comentário da (ISACA, 2005) que se transcreve:
"*For an internal audit function, a plan should be developed/updated, at least annually, for ongoing activities. The plan should act as a framework for audit activities and serve to address responsibilities set by the audit charter. The new/updated plan should be approved by the Audit Committee...*"

Esta passagem consta dos "*IS Standards, Guidelines and Procedures for Auditing and Control Professionals*", nos quais existe uma norma (*standard*) relativa ao planeamento (*S5* - Planning). Nesta é definida a obrigatoriedade de um plano de Auditoria de SI que cubra os objectivos da função e que esteja em conformidade com os regulamentos aplicáveis, incluindo os constantes das normas profissionais do Auditor e da carta de Auditoria. O plano deverá sintetizar a natureza, os objectivos, os recursos e o período de tempo relativos a cada auditoria, devendo ser aprovado pelo Comité de Auditoria da organização. O plano da Auditoria de SI deverá ser documentado e construído utilizando uma abordagem ao risco.

Esta abordagem ao risco, já anteriormente tratada (na secção 2.3.2 - Auditoria baseada no Risco), é o instrumento chave através do qual todo o plano deve ser desenvolvido.

O seguinte pensamento de (Sayana, 2002) vem precisamente corroborar a necessidade de uma abordagem ao risco no planeamento das Auditorias de SI:
"*The auditor is faced with the questions of what to audit, when and how frequently. The answer to this question is to adopt a risk-based approach.*"

Como se percebe, o planeamento das Auditorias de SI não serve apenas para indicar "o que" se vai auditar, mas é também um instrumento para determinar "quando" e com que "frequência" se deve auditar. Já agora, permita-se acrescentar um outro factor importante: o "porquê" auditar? A resposta a esta última questão reside no risco. Na elaboração do planeamento devem-

se escolher, para serem auditados, os processos e os SI que maior risco trazem ou poderão vir a trazer para o negócio em determinado período de tempo.

Como elaborar então um planeamento de Auditoria de SI que tenha em conta o negócio e os seus riscos? Para percebermos como conceber um planeamento deste tipo, recorreu-se ao seguinte modelo descritivo da autoria de (McNamee and Selim, 1998):

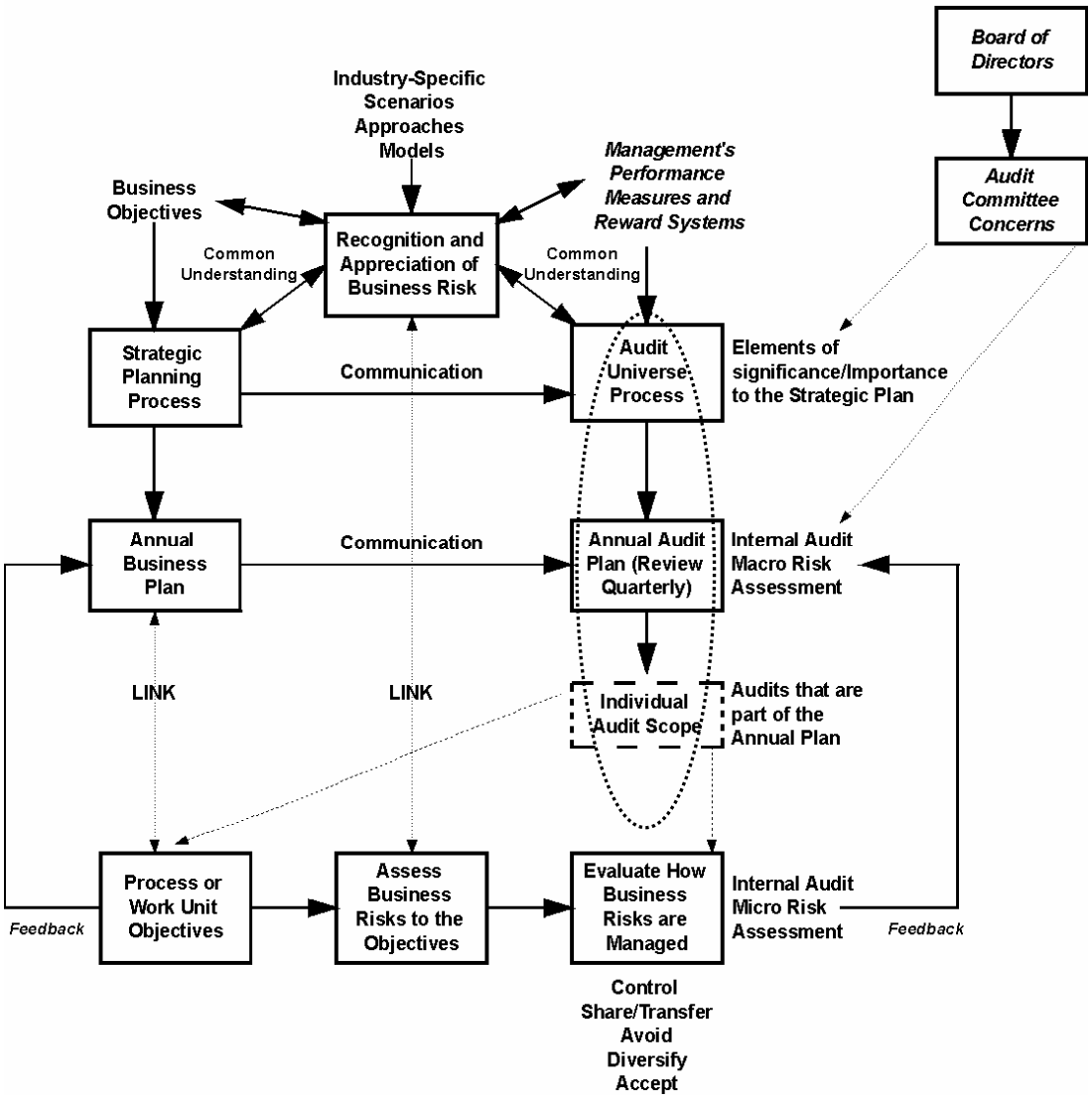


Figura 3.10 - Modelo de Planeamento para a Função Auditoria de SI

Fonte: Adaptado da versão original de (McNamee and Selim, 1998):

"*A Model for Improving Internal Audit service to the organization through Risk Management techniques*"

Comecemos então por interpretar este modelo, dizendo que o risco (*Recognition and Appreciation of Business Risks*) é o elo de ligação entre o lado do negócio (lado esquerdo da figura) e o lado da Auditoria (lado direito da figura). Situando-nos no lado do negócio, podemos constatar que os objectivos de negócio determinam o plano estratégico (*Strategic Planning Process*), que por sua vez determina o plano anual de negócios (*Annual Business Plan*), que tem impacto nos processos e nas áreas de negócio (*Process or Work Unit Objectives*). Uma vez que a Auditoria de SI deverá estar alinhada com as necessidades do negócio, então do lado da Auditoria o planeamento deverá seguir um raciocínio semelhante. Situando-nos então do lado da Auditoria (no conjunto das 3 actividades destacadas com uma elipse a tracejado), partindo do universo da Auditoria (*Audit Universe Process*), deverá ser elaborado um plano anual de Auditorias (*Annual Audit Plan*) que determinará o âmbito de cada Auditoria individual (*Individual Audit Scope*) e terá impacto no modo como as áreas de negócio avaliam e gerem os seus riscos (*Evaluate How Business Risks are Managed*).

Segundo os referidos dois autores, o sucesso de um modelo de planeamento deste tipo passa pela necessária comunicação entre os dois lados. Assim, na prática, para a determinação do seu universo de actuação, a Auditoria de SI deverá conhecer o plano estratégico dos SI. De igual modo, para a elaboração do planeamento anual, a Auditoria de SI deverá conhecer o plano operacional do SI para esse mesmo ano. Ao contrário de outras abordagens mais tradicionais em que os Auditores de SI utilizavam os planos de SI para validar os planeamentos da Auditoria de SI, este modelo defende que os planos dos processos de negócio, neste caso os planos dos SI, deverão ser determinantes activos na elaboração do planeamento da Auditoria. Como já afirmámos anteriormente, os riscos de negócio mais relevantes ao nível dos SI deverão ser os determinantes do âmbito anual da Auditoria de SI. O modelo admite que as organizações usem cenários de risco na avaliação de risco anual, pois são mais apropriadas para sectores de negócio em consolidação ou com ritmo de mudança elevado. O modelo vai ainda mais longe quando afirma que as metodologias de avaliação de risco a utilizar (factores de risco, modelos de risco, etc.) possam ser derivadas directamente da especificidade de cada processo de negócio (*Industry-Specific Scenarios Approaches Models*) em vez de serem determinadas unicamente pelos processos de Auditoria. Ao nível das Auditorias individuais, mais uma vez

serão os riscos do processo ou do SI em causa que determinarão o planeamento dessa Auditoria, incluindo quais os testes a efectuar e o tipo de relatório mais adequado para emitir.

Note-se ainda o facto deste modelo prever os dois órgãos de governo da organização (a Gestão de Topo e o Comité de Auditoria) que têm como responsabilidades contribuir para a elaboração e dar aprovação ao universo da Auditoria e ao seu planeamento anual. É, no entanto, da responsabilidade do departamento de Auditoria da organização transmitir a estes órgãos de governo uma cultura e percepção de risco, alinhada com as restantes áreas da organização, e informá-los sobre as exposições aos riscos da organização.

Como se constata, para além da abordagem ao risco, é dado grande destaque à relação com o negócio nas actividades de planeamento. Apenas uma nota para deixar claro que esta relação não é uma novidade, nem uma necessidade exclusiva da Auditoria de SI. Existem outras actividades de planeamento no domínio dos SI em que esta necessidade também é reconhecida. A este propósito deixámos aqui um apontamento da visão de (Amaral e Varajão, 2000):
"A actividade de planeamento de SI é desencadeada como parte integrante da actividade de planeamento estratégico da organização. (...) O planeamento de SI deverá estar integrado e alinhado com o planeamento do negócio, sendo extremamente importante ter a noção de que o mesmo é uma forma de planeamento da mudança organizacional..."

O (IIA, 2006) tece um conjunto de considerações sobre o modo como as Auditorias de SI devem ser definidas e que são relevantes aquando da elaboração do planeamento:
"*The way in which IT audits are defined plays a large role in the overall effectiveness of the IT audit function. (...) Audit committee wants IT audit findings to be tied to the business issues*."

Segundo esta perspectiva, o desafio está em encontrar o nível correcto de granularidade aquando da definição das Auditorias de SI. Neste contexto, o IIA fornece algumas orientações a ter em consideração e que se resumem de seguida:

- Evitar o uso de definições/designações de Auditorias de SI demasiado abrangentes → É comum existirem nos planeamentos da Auditoria de SI as chamadas "Auditorias aos Controlos Gerais". Estas podem tornar-se relativamente inúteis, sobretudo em grandes

organizações, dado que, ou não cobrem todo o universo dos SI, ou para fazê-lo, tornam-se intermináveis no tempo. Por outro lado, há que ter muito cuidado na designação que se atribui às Auditorias pois podem induzir em erro a Gestão de Topo e a Gestão dos SI quanto à verdadeira abrangência do plano de Auditorias.

- O planeamento deve tocar todos os níveis de SI → O planeamento deve considerar, em cada ano, pelo menos uma Auditoria em cada um dos níveis de controlo dos SI: Governo, Gestão, Técnico (ver os níveis na secção 3.3.2). Se tal não acontecer, existe sempre o risco da organização considerar o planeamento omisso ou incompleto como um todo.
- O planeamento deve prever Auditorias que formem conjuntos lógicos de relatórios sobre determinados temas → As Auditorias devem ser planeadas de modo a fornecer um reporte eficaz e lógico dos resultados. Para ilustração, as Auditorias aplicacionais raramente são eficazes se forem divididas em Auditorias independentes (exemplo: dever-se-á auditar todos os módulos de SAP e não apenas o módulo financeiro). De modo semelhante, as Auditorias às tecnologias da rede corporativa tendem a ser mais eficazes quando efectuadas ao nível de toda a organização (exemplo: não auditar a segurança da rede em uma só localização/instalação).
- O planeamento e respectivo orçamento devem cobrir os riscos de forma apropriada → O planeamento das Auditorias e o orçamento do departamento devem ser um resultado do processo de avaliação de riscos de SI, não devendo ser definidos antes de se proceder a essa avaliação. Esta deve ser efectuada no contexto da avaliação de riscos efectuada para toda a organização (a este propósito, ver na secção 3.2.2 o papel da função Gestão de Risco). Contrariamente ao que acontece com outros tipos de Auditoria Interna com histórico mais longo nas organizações (exemplos: Auditoria Financeira, Auditoria de Qualidade, etc.), a estimativa de um orçamento para Auditoria de SI pode ser induzida em erro caso utilize técnicas de comparação com outras Auditorias ou se guie por ordens de grandeza. O orçamento da Auditoria de SI deve ser estimado em função da avaliação dos riscos de SI, deve possuir um processo de pré-planeamento robusto e deve contar com os contributos da Gestão dos SI.

Uma vez definido o modelo a utilizar e as orientações a ter em conta na definição de um planeamento anual das Auditorias de SI, na próxima secção tratar-se-á de identificar as fases que constituem cada uma das Auditorias individuais previstas nesse planeamento.

3.5.2 As Fases das Auditorias de SI

De seguida dar-se-ão a conhecer as principais fases que habitualmente constituem uma Auditoria e concretizaremos, indicando de forma breve, alguns exemplos dos conteúdos de cada uma das fases.

Para tal, apresentaremos três visões diferentes, mas compatíveis, das fases das Auditorias. Note-se que algumas destas visões não são específicas da Auditoria de SI (por exemplo, são do domínio da Auditoria de Processos de Negócio ou da Auditoria de Qualidade). No entanto são abordagens que são realmente aplicáveis na prática também à Auditoria de SI. Aliás, como vimos na secção 2.4.1, é desejável a integração de metodologias entre diferentes tipos de Auditorias Internas.

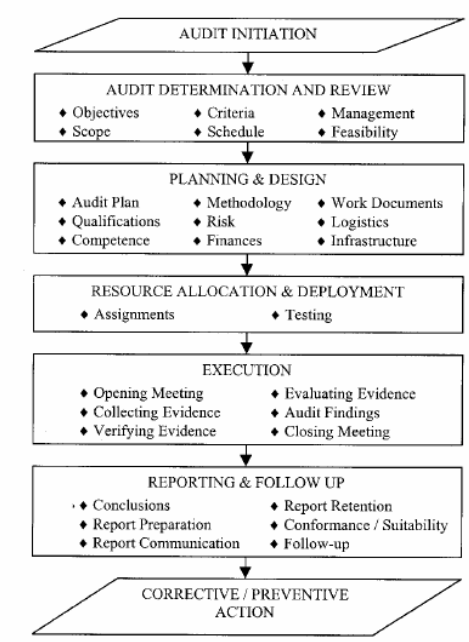


Figura 3.11 - As Fases da Auditoria de SI: sequência decomposta em conteúdos

Fonte: Versão original extraída de (Karapetrovic and Willborn, 2001): "*Audit flow and audit system reliability.*"

A sequência de fases apresentadas na figura anterior são da autoria de (Karapetrovic and Willborn, 2001). Estes consideram que o processo de Auditar consiste numa série de actividades interrelacionadas. A Auditoria é despoletada em função do planeamento anual das Auditorias onde deverá estar prevista, ou excepcionalmente, em função de uma necessidade pontual devidamente justificada. Na primeira fase, são desenvolvidas actividades com vista à determinação da Auditoria, nomeadamente a definição dos seus objectivos, âmbito, cronologia e critérios de Auditoria a utilizar, entre outras. Segue-se uma fase de planeamento e desenho da Auditoria, cujo principal objectivo é a sua preparação. Aqui devem ser providenciados os recursos necessários, incluído a identificação das qualificações profissionais dos Auditores (formação, experiência, etc.) e as suas competências (alinhadas com os objectivos da Auditoria). Nesta fase é efectuada a selecção das metodologias de teste e o desenho dos testes a executar na Auditoria. Deverão ser identificados os riscos da Auditoria (note-se que são os riscos da própria Auditoria não cumprir os seus objectivos e não os riscos de negócio ou riscos de SI que já deverão ter sido identificados na fase anterior). Os referidos autores prevêem uma fase intermédia em que a Auditoria já definida é então atribuída a uma equipa de Auditores que a vão executar. Na fase de execução, as evidências de Auditoria são recolhidas e verificadas, sendo comparadas com os critérios de Auditoria para a determinação de eventuais excepções (*findings*). Estas actividades deverão ser executadas de acordo com as técnicas de auditoria definidas nas fases anteriores e dentro do âmbito delimitado na primeira fase. Na última fase, são reportadas às partes interessadas na Auditoria, não só as conclusões (sobre a conformidade dos processos auditados com os critérios de Auditoria), mas também a definição de acções preventivas ou correctivas a efectuar (oportunidades para a melhoria contínua). Estas podem ser alvo de Auditorias de seguimento/acompanhamento (*follow-up*) sobre o estado de implementação dessas acções.

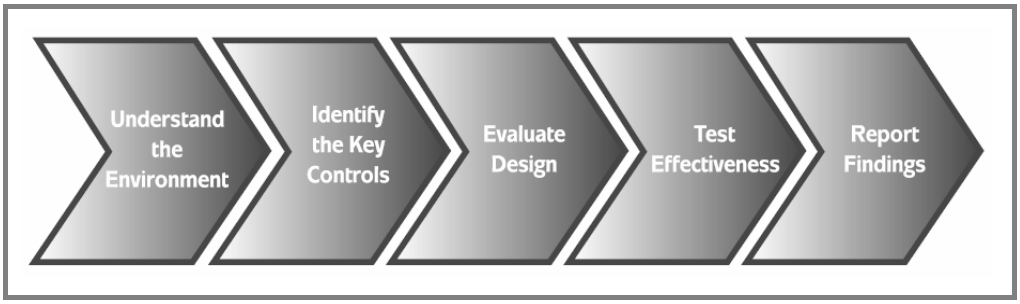


Figura 3.12 - As Fases da Auditoria de SI: sequência lógica de actividades

Fonte: Versão original extraída de (IIA, 2006): "*Audit Process Overview*"

A visão apresentada pelo (IIA, 2006) difere nas fases e nos seus conteúdos face à visão anterior, não existindo, contudo, grandes diferenças nos princípios fundamentais. Trata-se de uma visão apresentada pelo IIA para o contexto da Auditoria de SI, mas o próprio IIA reconhece não existirem muitas diferenças em relação às fases de Auditorias mais genéricas, como por exemplo as Auditorias de Processos de Negócio:

"*The process for executing an IT audit is, in theory, no different than the process for executing an operational audit."*

Tendo em conta a similitude com outros tipos de Auditorias Internas, o IIA não detalhou as fases apresentadas, limitando-se a enunciar que o Auditor de SI deve planear a Auditoria, identificar e documentar os controlos chave, testar a arquitectura e a eficácia operacional dos controlos e concluir a Auditoria elaborando relatórios com os resultados.

Não obstante, as fases apresentadas pelo IIA merecem alguns comentários, pois denotam, mesmo assim, alguns factores diferenciadores. Estes encontram-se essencialmente na primeira fase considerada: a compreensão da envolvente (*Understand the Environment*). De um modo um pouco diferente face ao que acontece noutros tipos de Auditorias Internas, o Auditor de SI tem nesta fase que compreender os processos ou os SI alvo da Auditoria e tentar encontrar o ou os referenciais (*standards*) que mais se lhes adequam. Muitas organizações podem ainda não ter implementado um sistema de referenciais para todos os seus processos de SI e, por outro lado, cada envolvente de SI tem as suas especificidades. No entanto, existe sempre uma base comum

que o Auditor de SI pode tomar como uma referência sobre a qual pode auditar: os objectivos de controlo dos SI. Daí que a segunda fase seja a identificação dos controlos chave, cujo seu desenho será avaliado na terceira fase e cuja sua eficácia será testada na quarta fase.

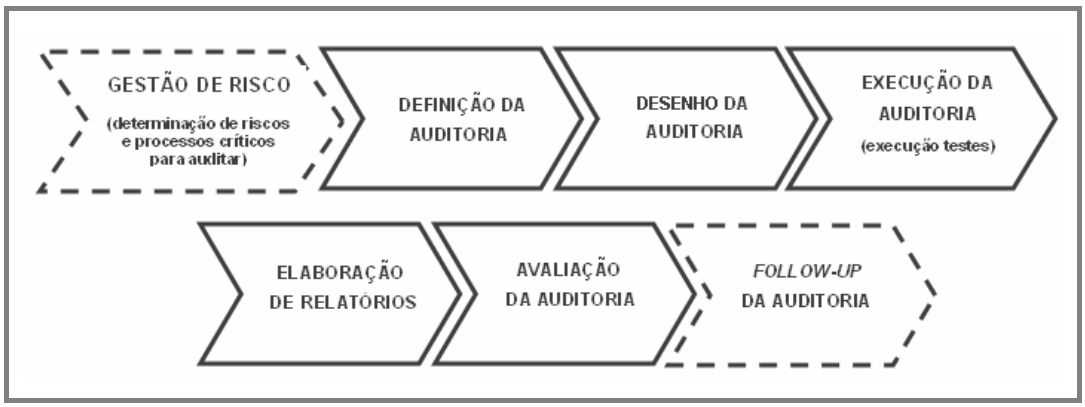


Figura 3.13 - As Fases da Auditoria de SI: sequência formal tipo projecto

Fonte: Adaptado da versão original de (Silva, 2004b): "Modelo de Processo (Fluxo do Projecto / Auditoria)"

A terceira visão apresentada, proposta pelo autor do presente trabalho (Silva, 2004b), é uma visão genérica, adaptável a qualquer tipo de Auditoria Interna baseada numa abordagem ao risco, pelo que também é aplicável no domínio da Auditoria de SI. Esta será, aliás, a visão das fases de Auditoria de SI que usaremos daqui em diante, ao longo deste texto, tomando-a como uma sequência de fases, organizadas à semelhança de um projecto.

A primeira fase, a Definição da Auditoria, deverá ter em conta a informação proveniente do processo de avaliação dos riscos de negócio, efectuado pela função de Gestão de Risco (a este propósito, ver na secção 3.2.2 o papel da função Gestão de Risco). Com base nesta informação, deverão ser determinados os riscos e processos críticos de SI que serão avaliados na Auditoria em causa. Nesta fase de Definição da Auditoria é efectuada uma delimitação da Auditoria, incluindo a definição dos seus requisitos. Na secção 3.5.4 ("A Definição da Estrutura das Auditorias de SI") são apresentados em detalhe os requisitos/conteúdos que deverão idealmente constituir esta fase. Apenas uma nota para indicar que é nesta fase que se escolhem os referenciais a utilizar. Na fase de Desenho da Auditoria é efectuado um levantamento detalhado dos controlos de SI existentes e são desenhados os testes de Auditoria. Na fase seguinte, na

Execução da Auditoria, são executados os testes anteriormente desenhados, de acordo com os parâmetros definidos na fase de Definição (objectivos, âmbito, tempo, custo, qualidade, etc.). Na fase de Elaboração de Relatórios, procede-se à formalização das conclusões obtidas nas fases anteriores, apresentando as excepções encontradas (*findings*), sugerindo as recomendações de correcção ou de melhoria e acordando com as áreas auditadas as respectivas acções a desenvolver. Os relatórios deverão também contextualizar e fornecer uma breve visão sobre o trabalho efectuado nas fases anteriores à da Execução. A última das fases diz respeito à Avaliação da Auditoria que deverá ser efectuada sob duas vertentes. Por um lado, internamente pela equipa de Auditoria, avaliando se a Auditoria cumpriu os seus objectivos de acordo com os referencias e demais requisitos de qualidade definidos na fase de Definição da Auditoria. Por outro lado, avaliando externamente, quanto à satisfação das necessidades pelos clientes da Auditoria, ou seja, pela Gestão de Topo, pelos Gestores dos SI responsáveis pelos processos ou SI auditados e, nalguns casos, pelos Gestores dos processos de negócio que beneficiam directamente dos SI auditados. Por fim, existe ainda uma fase opcional de *Follow-Up* da Auditoria, a qual poderá ocorrer num determinado período de tempo após a conclusão da Auditoria, em que se procede à avaliação do estado de resolução das excepções (*findings*) e à identificação do estado de implementação das acções de correcção ou de melhoria.

Como poderá ter sido perceptível ao longo desta secção, a gestão das fases de uma Auditoria de SI e dos respectivos conteúdos possuem diversas semelhanças com a gestão de um projecto, pelo que exploraremos esta teoria na secção seguinte.

3.5.3 A Gestão das Auditorias de SI como a Gestão de um Projecto

Analisaremos a seguinte afirmação do (PMI, 2004) sobre as fases dos projectos, de modo a podermos concluir sobre a aplicabilidade deste conceito às Auditorias de SI:

"*The completion and approval of one or more deliverables characterizes a project phase. (...) The deliverables, and hence the phases, are a part of a generally sequential process designed to ensure proper control of the project and to attain the desired product or service, which is the objective of the project.*"

Nas Auditorias de SI, a conclusão de um ou vários produtos resultantes (*deliverables*) caracteriza na realidade uma fase da Auditoria. Veja-se o exemplo do Documento de Definição de Auditoria, cuja sua conclusão marca o final da fase de Definição de Auditoria (este Documento de Definição de Auditoria será explorado na secção 3.5.4). Para além disso o referido documento tem de ser aprovado pelas partes interessadas (*stakeholders*) na Auditoria (exemplo: responsáveis pelos processos ou SI que serão alvo da Auditoria). O mesmo tipo de raciocínio pode ser aplicado a outros produtos resultantes da Auditoria, dos quais se dão mais dois exemplos. O fecho dos Relatórios marca o final da fase de Elaboração de Relatórios, tendo estes que ser aprovados pelos responsáveis dos processos ou SI auditados. Os formulários com os parâmetros de avaliação marcam o final da fase de Avaliação da Auditoria e têm implícita a aprovação de quem os preenche (habitualmente os destinatários da Auditoria, ou seja, a Gestão de Topo e os responsáveis pelos processos auditados).

As Auditorias de SI são um processo constituído por um conjunto de actividades, agrupadas em fases. Este agrupamento tem como finalidade possibilitar que as actividades da Auditoria de SI possam ser controladas de um modo mais adequado. Para além disso, o objectivo final de uma Auditoria de SI pode ser entendido sob duas perspectivas. Numa perspectiva de produto, os produtos finais da Auditoria (*Project Deliverable*) serão os Relatórios de Auditoria. Também pode ser encarado sob uma perspectiva de serviço, em que este diz respeito ao fornecimento de uma garantia sobre o estado dos controlos dos SI (numa visão mais conservadora) ou ao fornecimento de um trabalho de consultoria interna de SI (numa visão menos conservadora).

Tendo em conta os argumentos atrás apresentados e analisando a também figura seguinte, podemos concluir que, de facto, as Auditorias de SI podem ser geridas como projectos!

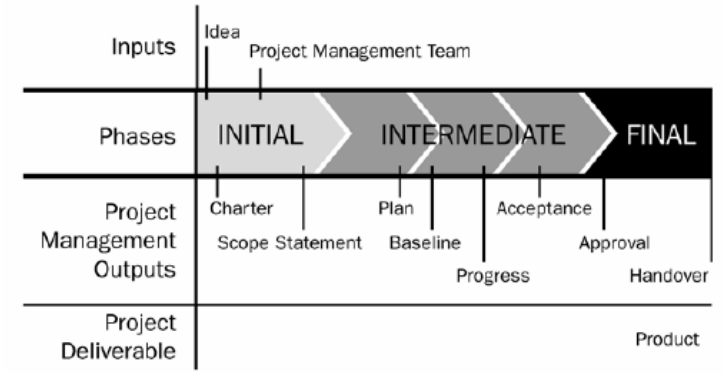


Figura 3.14 - As Fases da Auditoria de SI como Fases de um Projecto

Fonte: Versão original extraída de (PMI, 2004): "*Typical Sequence of Phases in a Project Life Cycle*"

Para cada um dos pontos indicados, representados acima na figura da autoria do PMI, iremos apresentar alguns exemplos correspondentes, aplicados à realidade das Auditorias de SI:

- Ideia (*Idea*) → Corresponde à causa (*trigger*) que despoleta a Auditoria. Normalmente está prevista no planeamento anual das Auditorias, ou excepcionalmente, pode surgir de uma necessidade pontual devidamente justificada
- Carta (*Charter*) → Corresponde à chamada Carta de Auditoria, sendo um documento padrão que legitima e autoriza o trabalho da equipa de Auditoria de SI. Pode ser adaptado/complementado com conteúdos específicos em função de cada Auditoria. É habitualmente enviado, no início da primeira fase, aos responsáveis pelos processos auditados (embora tenha esta designação, pode ser enviado, por exemplo, por e-mail).
- Equipa de Projecto (*Project Management Team*) → Corresponde à identificação da equipa que vai gerir e executar a Auditoria, incluindo o elemento responsável pela Auditoria (papel de gestão e execução) e os restantes Auditores (papel de execução).
- Documento de Definição de Âmbito (*Scope Statement*) → Corresponde ao Documento de Definição de Auditoria (que será explorado na secção 3.5.4).
- Plano (*Plan*) → Corresponde ao planeamento detalhado da Auditoria que é elaborado na fase de Desenho da Auditoria. Trata-se habitualmente de um refinamento do calendário de alto nível que é apresentado no Documento de Definição de Auditoria.
- Estrutura base (*Baseline*) → Corresponde igualmente ao planeamento detalhado da Auditoria que é elaborado na fase de Desenho da Auditoria. Trata habitualmente não só o parâmetro tempo (calendário), mas também todos os restantes parâmetros detalhados da

Auditoria (objectivos, âmbito, tempo, recursos, comunicação, qualidade, riscos, produtos resultantes), passando a ser o referencial a partir do qual qualquer alteração terá de ser avaliada e, consequentemente, aprovada.

- Relatórios de Progresso (*Progress*) → Correspondem aos relatórios de progresso, habitualmente emitidos durante a fase de Execução da Auditoria que é a mais longa. Destinam-se a informar as partes interessadas sobre o andamento da Auditoria (mais utilizado em Auditorias muito extensas).
- Aceitação (*Acceptance*) → Corresponde à aceitação dos Relatórios de Auditoria, por parte dos responsáveis directos pelos processos Auditados. Trata-se habitualmente da validação dos Relatórios Operacionais no que respeita aos testes efectuados e ao reconhecimento das excepções encontradas (*findings*).
- Aprovação (*Approval*) → Corresponde igualmente à aceitação dos Relatórios de Auditoria, por parte dos responsáveis de mais alto nível pelos processos Auditados. Trata-se habitualmente da aprovação dos Relatórios Executivos, incluindo as principais conclusões e as principais acções de correcção ou de melhoria.
- Passagem de responsabilidade (*Handover*) → Corresponde à passagem do plano de acções detalhado, da Equipa de Auditoria de SI para os responsáveis pelos processos auditados, passando estes a ter a responsabilidade de implementar as acções que foram definidas na sequência da execução da Auditoria, dentro dos tempos e responsabilidades acordados.
- Produto resultante do projecto (*Project Deliverable*) → Corresponde à entrega, às partes interessadas, das versões finais de todos os Relatórios de Auditoria e documentos relacionados.

De um modo geral, podemos também efectuar as seguintes correspondências quanto às fases:

- Fases Iniciais (*Initial Phases*) → Definição da Auditoria.
- Fases Intermédias (*Intermediate Phases*) → Desenho da Auditoria; Execução da Auditoria; Elaboração de Relatórios.
- Fases Finais (*Final Phases*) → Avaliação da Auditoria.

Existem ainda outros factores que confirmam a aplicabilidade da teoria da Gestão de Projectos à gestão das Auditorias de SI. Estas podem ser entendidas como projectos na medida em que, entre outros, possuem também os seguintes elementos caracterizadores que formalmente definem um Projecto (Silva, 2004b):

- Cada uma das Auditorias tem uma missão diferente para cumprir e possui particularidades que a distingue das restantes Auditorias de SI.
- As Auditorias são compostas por um conjunto de actividades que se diferenciam entre elas pelos seus objectivos.
- Desenrolam-se tendo como restrições os tempos, os custos, os desempenhos e a qualidade.
- São controladas e planeadas de acordo com critérios previamente definidos.
- São desempenhadas por Equipas que são formadas especificamente para uma determinada Auditoria (a partir de um conjunto disponível de Auditores no Departamento de Auditoria) e suportadas por meios que podem variar consoante o tipo de Auditoria.
- Apresentam uma sequência de fases distintas, implicando um início e um fim, e que se traduzem num modelo/fluxo (ver Figuras da secção 3.5.2.).
- As fases de uma Auditoria de SI seguem um modelo em cascata, prevendo-se também a possibilidade de uma fase dar lugar a interacções e ajustes em fases anteriores.
- Não é obrigatória a existência de todas as fases em todas as Auditorias de SI (como por exemplo as fases Gestão de Risco e *Follow-Up* da Auditoria).

Como se pode verificar, existem diversas actividades da Auditoria de SI que correspondem aos designados processos de Gestão de Projectos. Estes processos estão formalizados no *PMBOK – Project Management Body of Knowlegdge*, cujo modelo estruturado está representado na próxima figura.

Nesta figura estão sintetizados os 44 processos de Gestão de Projectos, agrupados em 9 áreas de conhecimento: Integração, Âmbito, Tempo, Custo, Qualidade, Recursos Humanos, Comunicação, Risco e Aprovisionamento.

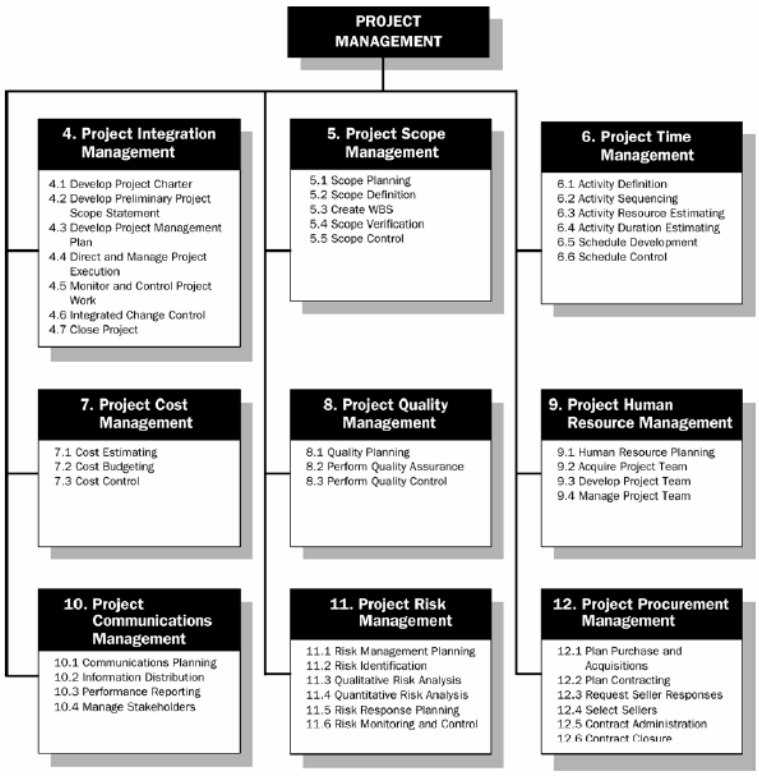


Figura 3.15 - *Framework* PMBOK

Fonte: Versão original extraída de (PMI, 2004):

"*Overview of Project Management Knowledge Areas and Project Management Processes*"

Como base nestas 9 áreas do conhecimento, que não exploraremos em detalhe, desenvolveram-se os conteúdos da próxima secção relativos à estruturação de uma Auditoria de SI. Como se constatará, não foram utilizadas todas estas áreas do conhecimento, os processos destas foram agrupados de forma ligeiramente diferente e com designações também, por vezes, diferentes.

No entanto, a ideia importante a reter é o exercício de adaptação que foi efectuado, visando encaixar as actividades da Auditoria de SI no referencial PMBOK. À semelhança do que já defendemos em secções anteriores, o importante é não executarmos as Auditorias de SI de um modo *ad-hoc*, mas sim adoptarmos um referencial que seja útil para o trabalho do Auditor. Neste caso, o referencial não diz respeito aos objectos alvo da Auditoria, mas sim ao próprio trabalho de gerir uma Auditoria de SI.

3.5.4 A Definição da Estrutura das Auditorias de SI

Inicia-se esta secção avançando a ideia de que a estruturação de uma Auditoria de SI pode ser posta em prática através da aplicação dos conceitos de gestão de uma Auditoria como um Projecto (secção 3.5.3) em cada uma das fases que constituem uma Auditoria de SI (secção 3.5.2).

De facto, partindo da abordagem de projecto exposta na secção anterior, utilizando algumas das 9 áreas de conhecimento e alguns dos 44 processos de Gestão de Projectos previstos no PMBOK, é possível construir uma estrutura para uma Auditoria de SI.

A definição da estrutura deverá ser explicitada num Documento de Definição de Auditoria. Este proporciona às diferentes partes interessadas (*stakeholders*) um verdadeiro guião com todos os aspectos relevantes que determinam a Auditoria.

O documento é produzido na fase inicial da Auditoria, ou seja, na fase de Definição da Auditoria. Esta assume a importante função ser aquela onde se procede à estruturação da Auditoria, determinando-se os parâmetros iniciais de alto nível. Apresentam-se os objectivos da Auditoria e efectua-se uma macro-definição da mesma. São identificados os produtos resultantes (*deliverables*) necessários para alcançar os objectivos da Auditoria. São definidas as linhas orientadoras da Auditoria e as suas fronteiras lógicas (âmbito lógico). Posteriormente, durante a fase de Desenho da Auditoria, o âmbito inicial é confirmado e refinado, detalhando-se todos os restantes parâmetros.

Para além dos aspectos mencionados, podemos dizer, resumidamente, que o Documento de Definição de Auditoria tem como principais atribuições:

- Identificar e documentar os SI, os processos e os riscos de negócio analisados na Auditoria.
- Ajustar as expectativas e identificar todas as partes interessadas (*stakeholders*) na Auditoria.
- Estabelecer os responsáveis da Auditoria e os responsáveis das áreas auditadas.
- Estimar a Auditoria em termos de esforço, duração e recursos.

- Identificar os referenciais metodológicos e de qualidade a utilizar na Auditoria.
- Identificar possíveis riscos que tenham impacto no bom andamento e no atingimento dos objectivos da Auditoria.
- Promover a visão colectiva e o comprometimento da equipa de Auditoria e demais intervenientes quanto aos objectivos da Auditoria e necessidades para os atingir.

Na tabela seguinte, apresenta-se uma proposta de sistematização de alguns dos possíveis conteúdos a incluir na estrutura de um Documento de Definição de Auditoria de SI.

ESTRUTURA	CONTEÚDOS
Objectivos da Auditoria	▪ Breve explicação do propósito do documento ▪ Origem e justificação para a Auditoria ▪ Objectivos gerais da Auditoria ▪ Objectivos específicos da Auditoria ▪ Objectivos de negócio suportados pelos SI a analisar ▪ Definição das condições para redefinição/alterações dos objectivos e seus responsáveis ▪ etc...
Âmbito da Auditoria	▪ Processos de Negócio (tabela de processos) ▪ Riscos de Negócio (descrição e classificação dos riscos) ▪ Causas/motivações (*drivers*) dos riscos (tabela) ▪ Cruzamento de Riscos vs. Processos de Negócio (tabela) ▪ Desagregação do SI ou do processo de SI alvo da Auditoria (diagrama de contexto, diagrama de entidade/relação, estrutura da informação, estrutura analítica de tarefas - *work breakdown structure*) ▪ Indicadores de negócio, dos processos e dos sistemas alvo da Auditoria (numérico e gráfico) ▪ Aplicações Informáticas (mapeamento/esquemas das aplicações) ▪ Sistemas (mapeamento/esquemas dos sistemas) ▪ Arquitecturas (mapeamento/esquemas de arquitecturas) ▪ Tipo de informação/dados a analisar (tipificação) ▪ Período temporal da análise ▪ Definição das condições para redefinição/alterações de âmbito e seus responsáveis ▪ etc...
Planeamento Temporal da Auditoria	▪ Calendário de alto nível ▪ Principais marcos temporais (*milestones*) ▪ Breve referência e descrição das fases da Auditoria ▪ Definição das condições para redefinição/alterações do planeamento temporal e seus responsáveis ▪ etc...
Planeamento de Recursos da Auditoria	▪ Responsável pela Auditoria ▪ Equipa de Auditoria ▪ Equipamentos/instalações ▪ Tecnologias/ferramentas informáticas de suporte à Auditoria ▪ Necessidades de competências específicas dos Auditores e controlo do seu desenvolvimento (se aplicável) ▪ Necessidades de formação dos Auditores (se aplicável) ▪ Orçamento para subcontratação (se aplicável) ▪ Critérios de pedido de propostas e selecção de fornecedores (se aplicável) ▪ Definição das condições para redefinição/alterações dos recursos e seus responsáveis ▪ etc...

Comunicação da Auditoria	▪ Partes interessadas na Auditoria (*stakeholders*) que devam ser alvo de comunicação inicial/intermédia/final ▪ Áreas organizacionais envolvidas/auditadas (Organigramas) ▪ Papeis e responsabilidades dos intervenientes na Auditoria ▪ Definição dos Relatórios de Progresso e de Desempenho e respectivos destinatários e periodicidade ▪ Definição das condições para redefinição/alterações da comunicação e seus responsáveis ▪ etc...
Qualidade da Auditoria	▪ Referenciais metodológicos utilizados na Auditoria (ex: metodologia proprietária, CobiT, ITIL, ISO 17799, etc.) ▪ Legislações, regulamentos e políticas internas/externas utilizadas na Auditoria ▪ Indicadores de qualidade do desempenho e de controlo do progresso face aos objectivos e plano da Auditoria ▪ Critérios de avaliação e intervenientes na Avaliação da Qualidade no final da Auditoria ▪ Definição das condições para redefinição/alterações dos referenciais de qualidade e seus responsáveis ▪ etc...
Riscos da Auditoria	▪ Suposições/restrições/condicionantes ▪ Identificação dos riscos com impacto na Auditoria ▪ Estratégias de resposta aos riscos da Auditoria ▪ Controlo e acompanhamento dos riscos da Auditoria ▪ Definição das condições para redefinição/alterações dos riscos e seus responsáveis ▪ etc...

Produtos Resultantes da Auditoria	▪ Breve referência e descrição dos produtos resultantes (*deliverables*) finais:
	  ▪ Relatório Operacional de Auditoria de SI
	  ▪ Relatório Executivo de Auditoria de SI
	  ▪ Outros produtos resultantes finais que resultem dos objectivos da Auditoria
	▪ Breve referência e descrição dos produtos resultantes (*deliverables*) intermédios:
	  ▪ Documento de Definição de Auditoria de SI
	  ▪ Relatórios de Progresso e Desempenho
	  ▪ Outros produtos resultantes intermédios que resultem das fases da Auditoria
	▪ Definição das condições para redefinição/alterações dos produtos resultantes e seus responsáveis
	▪ etc...

Tabela 3.4 - Documento de Definição de Auditoria de SI

Fonte: Adaptado e compilado pelo autor a partir da própria versão original (Silva, 2004b):

"Documento de Definição de Auditoria de SI"

3.5.5 AS TÉCNICAS DE GESTÃO DAS AUDITORIAS DE SI

Inicia-se esta secção informando que as técnicas de Gestão de uma Auditoria que se vão apresentar de seguida enquadram-se ainda no domínio da Função (pertencem ao Modelo Funcional). Estaríamos perante uma situação diferente se apresentássemos as técnicas de Execução de uma Auditoria (pertencem às Metodologias de Execução) que já estão fora do domínio desta investigação.

Aproveitaremos igualmente para comentar os conteúdos de cada uma das componentes da última tabela apresentada ("Documento de Definição de Auditoria de SI"). Assim, ao longo dos próximos parágrafos são efectuadas algumas considerações práticas sobre técnicas de Gestão de uma Auditoria de SI, inspiradas nas técnicas de Gestão de Projectos defendidas pelo (PMI, 2004) e na sua adaptação efectuada para as Auditorias de SI por (Silva, 2004b).

Sobre os Objectivos:

- A inclusão na Definição de Auditoria dos motivos da Auditoria é fundamental para a sua compreensão e justificação. Os motivos constituem uma importante precedência (*input*) para o desenvolvimento dos requisitos da Auditoria. Os motivos implícitos tornam-se em requisitos explícitos sob a forma de objectivos a alcançar e produtos resultantes (*deliverables*) a produzir.
- A explicitação da origem da Auditoria facilita a macro-identificação dos problemas, organizacionais ou de SI, existentes à partida e que se pretendem resolver com a Auditoria.
- As Auditorias podem ter como uma das origens o plano estratégico da organização do qual faz parte o Planeamento Anual do Departamento de Auditoria, devendo explicitar-se na Definição de Auditoria essa origem.
- A justificação da Auditoria deve ser efectuada com base nos objectivos a alcançar. As expectativas quanto à Auditoria só ficarão satisfeitas, tornando os objectivos em resultados. Como condição prévia, há que formalizar a aceitação do âmbito da Auditoria junto das partes interessadas, aceitando assim os objectivos propostos para atingir os resultados (os produtos resultantes previstos).
- Na Definição da Auditoria os objectivos a incluir não se devem limitar aos objectivos da própria Auditoria. Recomenda-se que façam também referência aos objectivos do negócio que são suportados pelo SI que se vai auditar. Estes dois tipos de objectivos devem ser compatíveis.
- A inclusão e formulação dos objectivos deve ter em conta a perspectiva dos diversos clientes da Auditoria (Áreas Auditadas, Gestão de Topo, Accionistas, etc.).

- Os objectivos a incluir na Definição de Auditoria deverão ter as seguintes propriedades: realísticos, credíveis, práticos, fáceis de usar/aplicar, consistentes, exactos, focados na melhoria dos processos e SI a analisar e que incorporem relações de causa-efeito verificáveis.
- A definição dos objectivos de uma Auditoria de SI, para que não se torne incompleta, não se deve resumir a um conjunto de tarefas isoladas das subsequentes fases da Auditoria. Dado que a fase de Definição de Auditoria poderá ter de ser revisitada durante a Auditoria, existe a possibilidade de ao longo desta se tornar a Definição de Âmbito mais completa quanto aos objectivos.

Sobre o Âmbito:

- No iniciar da Auditoria, deve-se ter em conta a prioritização dos riscos de negócio, dos processos de negócio (e respectivos SI de suporte), previamente identificados pela função de Gestão de Risco do Departamento de Auditoria, através dos seus métodos e técnicas específicas da Avaliação de Risco. Por outro lado, no iniciar da Auditoria dever-se-á também ter em conta eventuais causas/motivações apresentadas pelos Gestores de Topo (ex: administradores) responsáveis pelas áreas a auditar.
- Deve-se contudo evitar que a definição do âmbito seja pré-determinada apenas pelas causas/motivações indicadas pela Gestão de Topo que é, em última instância, a responsável pelo Plano de Auditorias. A Gestão de Topo acaba por pré-determinar, por vezes, um âmbito apenas aparente pois não dispõe das metodologias apropriadas para a definição de âmbito que só a Equipa de Auditoria possui.
- A sistematização dos processos, sistemas, aplicações e arquitecturas de SI a auditar, sob a forma de mapeamentos, esquemas e indicadores, é fundamental para explicitar os objectos alvo da auditoria e deixar claro quais são os incluídos e os excluídos do âmbito. De modo semelhante, a estruturação dos tipos de informação/dados a analisar facilita a delimitação do âmbito.
- De modo a assegurar que o trabalho de Auditoria produz o que estava definido nos seus requisitos, é necessário efectuar uma decomposição eficaz dos produtos resultantes da Auditoria. É importante segmentar os pontos da Auditoria em módulos fáceis de gerir e que façam correspondência com os diversos objectivos. Aconselha-se a utilização de técnicas de

estruturação analítica de tarefas (*WBS - Work Breakdown Structures*) para desagregar os SI ou processos de SI. Aconselha-se a aplicação deste tipo de técnicas que já tenham sido testadas em Auditorias similares realizadas anteriormente, sendo por isso já conhecidas do cliente da Auditoria e ajustadas às suas expectativas quanto ao tipo e forma de resultados a obter. Poder-se-á recorrer à criação de modelos/formatos (*templates*) para servirem de referência em trabalhos futuros.

- Em todas as Auditorias existe um processo de descoberta natural resultante de factores como omissões, problemas, criatividade, falta de entendimento e influências externas, que pressionam o alargamento do seu âmbito. No entanto, o alargamento do âmbito da Auditoria deverá ser aceitável sempre que se verifique que:
  - As alterações sejam claramente identificadas e classificadas quanto à sua natureza e origem.
  - Os diferentes intervenientes na Auditoria estiverem de acordo com as justificações para as alterações de âmbito e as diversas partes interessadas sejam notificadas sobre essas alterações.
  - O impacto na Auditoria seja entendido, através da análise do impacto que poderá ter nas outras variáveis da Auditoria (custos, tempo, qualidade, recursos humanos, etc.).
  - As alterações de âmbito sejam devidamente aprovadas pelos responsáveis previamente definidos.
- Deverão ser previstos critérios e procedimentos de controlo de alterações de âmbito, que poderão utilizar ferramentas tais como:
  - Documento de Identificação de Pedido de Alteração de Âmbito, sendo este despoletado pela detecção da necessidade de alterar/acrescentar pontos ao âmbito. Tem por objectivo documentar, avaliar e decidir sobre modificações pretendidas ou descobertas que interfiram no âmbito da Auditoria.
  - Resumo de Pedidos de Alteração de Âmbito que sumariza os pedidos de alteração existentes ao longo do ciclo de vida de uma Auditoria.
- Recomenda-se ainda a criação de um histórico de alterações de âmbito das todas as Auditorias de SI realizadas, de modo a que se possam tirar conclusões e ensinamentos úteis de como proceder para gerir futuras redefinições de âmbito.

Sobre o Tempo:

- Os períodos de tempo em que decorrerão as fases da Auditoria e eventuais marcos (*milestones*), tais como emissões finais de relatórios ou outros documentos intermédios, deverão estar devidamente previstos e articulados numa calendarização, servindo de referência para todas os intervenientes directos na Auditoria (Equipa de Auditoria e Auditados) e também para outras partes indirectamente interessadas (*stakeholders*).
- Em caso de necessidade de se efectuar uma redefinição do planeamento temporal da Auditoria, devem ser especificadas as possíveis opções alternativas e identificados eventuais impactos noutras Auditorias de SI que estejam ou venham a decorrer.

Sobre os Recursos:

- Caso exista algum tipo de recursos físicos (ex: equipamentos, instalações, aplicações informáticas, etc.) e de recursos humanos (ex: competências/conhecimentos, necessidades de formação, recursos subcontratados, etc.) que habitualmente não são utilizados nas Auditorias de SI mas que sejam necessários devido às especificidades da Auditoria em causa, deverão ser identificados e devidamente caracterizados em termos de requisitos, de modo a que o responsável pela Auditoria ou o responsável pelo Departamento de Auditoria preveja e mobilize os meios necessários para os obter antes do início do trabalho de campo da Auditoria.
- De um modo semelhante, mas a um nível superior na organização, o Departamento de Auditoria deverá garantir junto da Gestão da organização os recursos (humanos, físicos, financeiros) necessários à execução das Auditorias pois é aquela quem tem poderes para os atribuir. O sucesso de cada uma das Auditorias está dependente da obtenção desses recursos.
- No caso de eventuais fornecedores subcontratados para a Auditoria, deverão ser previstos critérios para avaliação da sua capacidade (ex: critérios previstos no Sistema de Qualidade ISO 9001/2). Estes poderão ser úteis nos casos de Auditorias aplicacionais em que a função de Auditoria de SI recorre a subcontratação de fornecedores com competências técnicas

especializadas para o efeito. No Documento de Definição de Auditoria, no planeamento dos recursos, dever-se-á considerar todas as eventuais subcontratações necessárias.

Sobre a Comunicação:

- Deverá existir um documento escrito, habitualmente designado de Carta de Auditoria (*Audit Charter*), no qual se formaliza a autorização para iniciar a Auditoria, devendo também constar a origem/motivos da sua realização (por exemplo, indicar que faz parte do Plano Anual de Auditoria aprovado). Esse documento formal deverá ser validado ao nível da Gestão de Topo. Nele deverá ser nomeado o responsável da Auditoria, atribuindo-lhe assim a responsabilidade e a autoridade para mobilizar na organização os recursos e a disponibilidade das áreas auditadas, necessárias para o desenrolar da Auditoria.
- Aconselha-se a realização de uma reunião de abertura com os responsáveis dos processos ou SI que vão ser alvo da auditoria para se explicitarem pessoalmente os motivos da Auditoria e se apresentar o Documento de Definição da Auditoria.
- Nesta reunião, assim como em toda a comunicação durante a Auditoria, deverá ser sempre passada a mensagem de que a Auditoria será conduzida numa perspectiva de colaboração positiva com as áreas auditadas, tendo por princípio a identificação de riscos e a formulação das respectivas acções que contribuirão para a melhoria dos processos e dos SI dessas áreas, ou seja, excluir à partida qualquer tipo de postura de inspecção e incriminatória.
- O Documento de Definição da Auditoria deverá ser redigido de modo a ser a base para um entendimento e, simultaneamente, identificar as diversas partes interessadas na Auditoria (Equipa de Auditoria, Áreas Auditadas, Gestão de Topo, etc.).
- Este documento tem a função de ajustar as expectativas dos diversos interessados na Auditoria pois divulga os objectivos desta e define quais os produtos resultantes (Relatórios Operacionais e Executivos, Relatórios de Progresso e Desempenho, etc) e quais as partes interessadas poderão contar com esses produtos resultantes.
- Deve ser efectuada uma validação do Documento de Definição de Auditoria através da sua aceitação formal, pelas diferentes partes envolvidas. Note-se que o objectivo desta validação é obter uma aceitação dos conteúdos e um comprometimento quanto à Auditoria. Por outro

lado, existem outras formas e metodologias mais adequadas de validação, relacionadas com a Qualidade, para avaliar a correcção do próprio trabalho de Definição de Auditoria.

- É fundamental assegurar que as áreas da organização responsáveis pelos SI auditados entendam qual o contributo que é suposto darem para os produtos resultantes previstos na Auditoria. Todas as áreas organizacionais envolvidas na Auditoria (ou os colaboradores individualmente, consoante os casos), deverão ser notificadas e esclarecidos quanto aos seus papéis e responsabilidades na Auditoria.

Sobre a Qualidade:

- O Controlo da Qualidade justifica-se pelo facto de se dever avaliar a qualidade da Auditoria face ao estipulado no documento de Definição de Auditoria, pois é neste que se estrutura toda a Auditoria a um nível macro e se definem os referenciais metodológicos a utilizar.
- As referências metodológicas geralmente utilizadas (ex: CobiT, ITIL, ISO 17799) deverão ser mencionadas no Documento de Definição de Auditoria pois, face ao âmbito previsto para a Auditoria e as suas especificidades, poderá ser necessário escolher uma das metodologias (ou um conjunto delas) que seja mais apropriada e justificar brevemente essa escolha.
- O mesmo tipo de procedimento deve ser considerado quando se utilizam legislações, regulamentos e políticas, quer internas ao Departamento de Auditoria ou à própria organização, quer externas.
- Poderão também existir outras referências metodológicas mais específicas que sejam necessária utilizar. Exemplos destas são as Normas da Qualidade ISO/IEC 15504 para processos de avaliação de software, que incorporam modelos de processos e linhas orientadoras para conduzir análises a software, podendo ser utilizadas nas Auditorias aplicacionais.
- É fundamental planear a Auditoria através de um Documento de Definição de Auditoria para que este sirva como instrumento de controlo das suas alterações e de suporte a futuras decisões no decorrer da Auditoria. Entendem-se como alterações, as redefinições, as adições, as eliminações e as mudanças que sejam relevantes e referentes a quaisquer elementos previstos no Documento de Definição de Auditoria e que possam ter impacto na Qualidade desta. Os critérios e os responsáveis por autorizar estas alterações deverão estar definidos.

- Para se validar a correcção do próprio trabalho de Auditoria em termos de Qualidade, poder-se-á recorrer, entre outras, às seguintes actividades:
  - Avaliar a fase de Definição de Âmbito em relação à sua condução e tarefas executadas.
  - Avaliar no final da Auditoria a fase de Definição por comparação com os produtos resultantes (*deliverables*).
  - Obter a aprovação dos produtos resultantes, de modo a poderem ser dados como terminados de acordo com critérios de acabamento previamente definidos.
  - Avaliar o desempenho da Equipa de Auditoria, através de indicadores de qualidade do desempenho e de controlo do progresso face aos objectivos e plano da Auditoria, efectuada pelas áreas clientes da Auditoria (ex: Áreas Auditadas, Gestão de Topo, etc.)
- A implementação dum processo de avaliação da Qualidade deverá ter também como objectivo entender as necessidades e expectativas que a organização tem face à função de Auditoria de SI. Os resultados dessa avaliação deverão servir como um dos factores de entrada (input) para o processo de Melhoria Contínua da Qualidade da função A avaliação poderá passar por entrevistas, inquéritos de satisfação, inquéritos de desempenho, etc.
- Recomenda-se a criação de um plano de gestão da Qualidade de uma Auditoria de SI que poderá passar pela adopção, entre outras, das seguintes ferramentas de controlo de Qualidade:
  - Registo (*log*) de questões em aberto relacionadas com a gestão e o controlo da Auditoria e que possam ter impacto ou risco de afectar o cumprimento de algum dos critérios de Qualidade definidos.
  - Lista de verificação (*check-list*) para validar que foram efectuados todos as tarefas previstas no Documento de Definição de Auditoria.
  - Comparação com outros pontos de referência (*benchmarking*), nomeadamente com os critérios de Qualidade adoptados nas Auditorias de Processos de Negócio efectuadas pelo mesmo Departamento de Auditoria, facilitando uma percepção integrada de Qualidade pelas áreas clientes da Auditoria na organização, quer sejam de Auditorias de SI ou Auditorias de Processos de Negócio.

Sobre os Riscos:

- Por vezes existem circunstâncias únicas ou situações que podem influenciar o âmbito ou a execução de uma Auditoria e que estão relacionadas com suposições que se assumem implicitamente. As suposições que têm um impacto significativo na Auditoria em termos de requisitos, tipo e forma de resultados devem ser identificadas explicitamente na Definição da Auditoria.
- A Definição da Auditoria tem por objectivo visionar o desenvolvimento da Auditoria antes da sua concretização, de forma a identificar estrangulamentos, dificuldades ou incompatibilidades. Para não criar expectativas que depois não se venham a concretizar, devem ser identificadas as restrições e os factores condicionantes e, se necessário, alertar para o que está fora de âmbito do Auditoria.
- Uma Auditoria de SI pode estar sujeita a riscos que condicionam a forma como o trabalho se desenrola. Estes riscos podem ter, entre outras, as seguintes origens e respectivas causas:
  - A área auditada na organização: desejos da área auditada ou condições impostas explicitamente (ex: disponibilidade de colaboração das áreas auditadas, recusa explícita em fornecer acesso a informação alvo de auditoria, etc.)
  - O processo ou o SI alvo da Auditoria: complexidade do processo, aspectos tecnológicos na fase de testes (ex: plataformas, aplicações, etc.)
  - A equipa de Auditoria: factores pessoais e de conhecimento (ex: desmotivação, falta de conhecimentos técnicos, disponibilidade de tempo, etc.)
  - A Gestão da organização: solicitações *ad-hoc*, motivos que deram origem ao pedido da Auditoria nem sempre estão explícitos, a forma dos produtos resultantes da auditoria não vão de encontro às suas expectativas (ex: vontade de alargamento do âmbito da Auditoria, redefinição de prioridades, redefinição de produtos resultantes, etc.)
  - A restante organização: limitações da organização no seio da qual a Auditoria se desenrola (ex: disponibilidade de recursos, questões estratégicas, etc.)
  - A envolvente externa: circunstâncias externas à Auditoria (ex: legislação, etc.)

Sobre os Resultados:

- Para esclarecer as diversas partes interessadas na Auditoria quanto ao tipo de produtos resultantes que poderão vir a receber, deverá ser efectuada uma descrição da estrutura e dos conteúdos dos produtos resultantes, quer sejam os intermédios, quer sejam os finais.
- Os Relatórios de Progresso pretendem manter as partes informadas sobre o progresso da Auditoria face ao planeado no Documento de Definição de Auditoria, nas suas diversas dimensões, mas essencialmente no cumprimento de tempos, custos e âmbito. Os Relatórios de Desempenho pretendem informar sobre as avaliações de Qualidade efectuadas, nomeadamente sobre a capacidade de execução da Auditoria pelos Auditores de SI, de acordo com os referenciais metodológicos previstos e dentro dos padrões de Qualidade definidos.
- Os Relatórios Operacionais e Executivos constituem os dois principais produtos resultantes da Auditoria. Os Relatórios Operacionais deverão conter todo o detalhe da Auditoria de SI efectuada, incorporando todo o trabalho desenvolvido desde a fase de Desenho até à fase de Relatório, sendo o produto resultante mais completo e abrangente de toda a Auditoria. O Relatório Operacional tem como destinatários privilegiados as Áreas Auditadas. Os Relatórios Executivos deverão conter as principais conclusões da Auditoria e a exploração resumida de algumas das excepções (*findings*), e recomendações/acções mais relevantes. O Relatório Executivo deve ser elaborado tendo em conta que é um instrumento de comunicação de alto nível, cujos destinatários mais prováveis serão a Gestão de Topo, incluindo os responsáveis directos pelos processos e SI analisados.

§ § §

Para encerrar este capítulo, é útil apresentar a seguinte ideia. A utilização sistemática dum documento de Definição de Auditoria, e dos respectivos conteúdos que foram descritos e discutidos sob a forma de técnicas de Gestão de Auditorias de SI, poderá ser um ponto de partida para o desenvolvimento de uma Metodologia formal e detalhada para cada uma das fases que constituem uma Auditoria de SI. Este objectivo está, contudo, fora do âmbito desta investigação.

Esta possível "Metodologia de Auditoria de SI" constituiria uma visão Táctica-Operacional de como executar e gerir as diversas fases de uma Auditoria de SI. A Metodologia deveria estar enquadrada e articulada com uma visão mais Política-Estratégica para a função Auditoria de SI. Esta última visão poderia ser materializada num documento designado de "Modelo Funcional de Auditoria de SI" que compilaria os diversos pontos abordados ao longo do capítulo que agora se encerra: objectivos, organização, âmbito, referenciais metodológicos e processos da função Auditoria de SI.

Após se ter identificado e detalhado os pontos acima mencionados que constituem um possível Modelo Funcional, no capítulo seguinte apresentar-se-á uma proposta de Modelo de Competências que pretende ser um instrumento para utilizar na identificação das competências que um Auditor de SI deve possuir, devendo estas estar alinhadas com as necessidades funcionais aqui preconizadas.

4 MODELO DE COMPETÊNCIAS DE AUDITORIA DE SI

Este capítulo tem um carácter complementar no contexto do presente trabalho de investigação. De acordo a lógica de investigação apresentada inicialmente (ver secções 1.2 e 1.3.1), constitui-se como um complemento às ideias sistematizadas nos capítulos anteriores, dado que o Modelo Funcional da Auditoria de SI não deverá ser dissociável das competências que um Auditor de SI deve possuir.

O principal objectivo deste Capítulo 4 é construir e propor um Modelo de Competências para o Auditor de SI, designado pelo autor como "MICASI - Modelo de Identificação de Competências do Auditor de SI". O modelo proposto resulta da combinação e adaptação de dois referenciais distintos que correspondem aos dois principais tipos de competências do Auditor de SI: as Competências de Gestão (baseado num modelo de competências de Gestão de Projectos) e as Competências Técnicas (baseado no Modelo Curricular da ISACA). Adicionalmente, apresentam-se os resultados da aplicação prática deste modelo através da realização de entrevistas semi-estruturadas a três profissionais de Auditoria de SI. O propósito destas entrevistas foi a classificação das competências que estes profissionais consideram como mais importantes para a actividade de Auditor de SI.

4.1 AS COMPETÊNCIAS DO AUDITOR DE SI

Para contextualização do tema das competências do Auditor, começar-se-á por efectuar uma identificação e exemplificação de alguns tipos de competências. Seguir-se-á a explicação dos determinantes das competências da Auditoria de SI, recorrendo a uma equação conceptual das competências que determinam o desempenho dos Auditores. Desta equação sobressairá a importância do Conhecimento, pelo que serão exploradas as quatro principais áreas de conhecimento do Auditor de SI. Associadas a estas estão dois grandes tipos de competências a comparar: as Competências de Gestão (*soft skills* ou *non-technical skills*) face às Competências Técnicas (*hard skills* ou *technical skills*).

4.1.1 O Contexto das Competências do Auditor

Esta secção tem por objectivo efectuar uma contextualização do tema das competências do Auditor, através da identificação de alguns exemplos de competências. A partir destes exemplos, reconhecer-se-á a existência de diversos tipos de competências, derivando daí a necessidade da existência de um Modelo de Competências para as classificar e arrumar devidamente.

Antes de mais, é relevante definir "competência". Num contexto genérico, segundo o dicionário da (Porto Editora, 2007), competência é a "qualidade de quem é capaz de resolver determinados problemas ou de exercer determinadas funções", sendo uma "aptidão" em determinada "área de actividade". Pode também ser entendida como a "capacidade que uma pessoa tem para avaliar (algo ou alguém)" com "idoneidade". No contexto profissional, segundo o glossário de termos do (ISACA, 2007), as competências profissionais referem-se a "*proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards*". Como se irá constatar, estas duas definições de "competência" são compatíveis e coerentes com os dois principais tipos de competências que serão identificados para o Auditor de SI ao longo deste Capítulo 4.

A identificação das competências dos Auditores não é, surpreendentemente, um tema nosso contemporâneo. Segundo (Jacka, 2006), foram recentemente descobertos manuscritos do século XIX com a letra de uma música dedicada aos Auditores. Trata-se de um documento original de W. S. Gilbert e Arthur Sullivan, uma famosa dupla de autores e compositores de operetas e libretos cómicos. A letra da música insere-se na obra "*The Auditors of Penzance*" e oferece-nos uma aproximação do que seriam as competências já consideradas como relevantes para um moderno Auditor do século XIX!

Na página seguinte apresentam-se partes dessa letra, tendo-se destacado (em negrito) as expressões ou palavras relacionadas com as competências do Auditor. Este documento servirá para dar o mote no tema das competências, uma vez que refere várias que identificaremos posteriormente.

Analisando o documento, conclui-se que os seus autores possuíam uma espantosa visão sobre a função do Auditor e que continua plena de actualidade!

I am the very model of a modern
audit manager.
I'm known as a **professional**, a **leader**,
and **encourager**.
I **never** come off **too obsequious**
or too monarchical.
But **fill employees' needs** that Maslow
laid out hierarchical.
To **threaten** or **cajole would be**
to act like a **barbarian**.
Instead my **tactics are Pavlovian**
and those **Skinnerian**.
I've mastered **motivation**, backstop
training, and **empowerment**.
And even think I comprehend the
things that Larry Sawyer meant.

I've analyzed **how best to handle**
people of type "Y" and "X".
And have the names of Covey,
Peters, and Drucker on Rolodex.
In short, I am professional, a leader,
and encourager.
I am the very model of a modern
audit manager.

I **quote** the **standards**, **ethics code**,
and each **practice advisory**.
I **know** of **charters**, **quality**,
and all things **supervisory**.
I'm very well acquainted with the
thoughts on **objectivity**.
And I maintain my **independence**
through overt passivity.
I speak on **risks** confronted both
inherent and residual.
And proffer that **controls** should
separate each individual.
On **governance** I understand the
various requirements.
And know how best to **verify** and
test control environments.

While I review **effectiveness** and
verify **efficiencies**,
It's more important that I point out
each and all **deficiencies**.
In short I am professional, a leader,
an encourager.
I am the very model of a modern
audit manager.

In fact, when I know what is meant
by **ERM** and **self-assess**.
When I can **meet an auditee** and
quickly make him acquiesce.
When I can **look at documents** inside
the current workpapers
and **understand the steps the fraudsters**
took in their berserk capers.
When **I know more of operations** than
the chief executive,
And **passed each of the CIA parts**
in sittings consecutive.
In short, I show of all the others
I am number one atop.
You'll say a better audit manager
has never run a shop.

However, I am at my best when
everything I **delegate**.
Because I'm real unclear on **how to**
business this would all **relate**.
But still I'm a professional, a leader,
and encourager.
I am the very model of a modern
audit manager.

ALL :
In short, he is professional, a leader,
and encourager.
He is the very model of a modern
audit manager.

Figura 4.1 - A Canção do Auditor

Fonte: Extraído de (Jacka, 2006): "*The Audit Manager's Song*"

De facto, a letra refere algumas das tradicionais competências do Auditor, como por exemplo: ser profissional; possuir formação; respeitar a ética; ser objectivo e independente; identificar relações e comportamentos de causa-efeito; verificar os controlos; identificar deficiências; detectar a fraude; etc.

No entanto, de um modo surpreendente, refere muitas outras competências que, mesmo hoje em dia, ainda necessitam de ser melhoradas por parte de alguns Auditores, como por exemplo: ser encorajador; não ser agressivo ou arrogante; ser empreendedor; saber lidar com os outros; conhecer os referenciais metodológicos; saber determinar os riscos; compreender a Gestão de Risco; conhecer os requisitos de Governo das Sociedades (*Corporate Governance*); reconhecer a importância da análise da eficácia e da eficiência; conhecer os processos operacionais e relacionar com o negócio; etc.

Para além das inúmeras competências que se acabaram de ilustrar, existem determinados temas normalmente associados ao contexto da identificação das competências dos Auditores. De um modo breve, abordar-se-á de seguida alguns desses temas, recorrendo a um conjunto de contributos de autoria diversa.

Num artigo de recolha de opiniões, elaborado pelo (ISCJ, 2000), acerca do tema da identificação de competências aquando do recrutamento de Auditores de SI, podemos encontrar a seguinte afirmação:
"*Managers no longer just manage. They must be 'hands on' working managers and have the knowledge to participate in their audits. Seniors must be able to handle their own audits on a stand alone basis when required.*"

Constata-se que os especialistas em recrutamento de Auditores de SI privilegiam a identificação de competências de auto-proficiência, tanto ao nível dos gestores de equipas de Auditoria (*managers*), como ao nível dos auditores seniores. Para além disso, a competência para trabalhar em equipa, bem como a competência para comunicar eficazmente com as áreas de

negócio e para "vender" as ideias são igualmente identificadas. Estas são competências intrinsecamente relacionadas com o perfil pessoal do Auditor.

No que diz respeito ao perfil profissional, na opinião de (Gallegos, 2003), os Auditores de SI são recursos únicos possuidores de um conjunto de competências técnicas úteis para a organização, não só no papel de Auditores, mas também eventualmente como futuros Gestores de SI. Os Auditores de SI possuem elevado conhecimento sobre o ciclo de vida dos SI da organização e possuem fortes competências em SI, em TIC e em metodologias de Auditoria. Para além disso, deverão possuir também competências de comunicação e de gestão que nem sempre estão presentes noutras funções da organização. Este autor acrescenta que um factor crítico de sucesso para a manutenção e o desenvolvimento das competências é a formação, de modo a que o Auditores de SI tenham acesso a novas tecnologias, novos métodos, novas práticas, etc. Para a identificação das competências que o Auditor de SI deverá desenvolver, é aconselhável a existência de avaliações de desempenho (bianuais) nas quais se efectua um confronto com as competências e os conhecimentos adequados ao nível de carreira do Auditor em causa.

Relativamente à identificação de competências ao longo da carreira, (Sadowski, 1997) considera que um Auditor que se encontre a iniciar careira deverá possuir um nível mínimo de competências interpessoais e de competências técnicas. À medida que o Auditor vai progredindo nos níveis de carreira, as competências técnicas desenvolver-se-ão, mas serão sobretudo as competências de comunicação e de interacção que se deverão tornar mais exigentes.

No âmbito do perfil pessoal do Auditor, (Touquet, 1996) faz uma observação curiosa ao relacionar as competências de SI que os Auditores de SI possuem com outras ocupações (*hobbies*) que possam ter na sua vida pessoal. De facto, outras ocupações pessoais dos Auditores de SI podem ser uma origem para a identificação de competências relevantes para o trabalho de Auditor de SI. Aliás, os Auditores de SI podem ter, na sua vida pessoal, motivação para esses temas ou interesse na utilização de SI e de TIC, factos que potenciam conhecimentos úteis para as suas profissões.

Os autores (Power and Terziovski, 2005) efectuaram um trabalho de levantamento das posições de outros autores sobre as competências para Auditoria (genérica, não financeira), no qual identificámos duas ideias a destacar. Por um lado, os autores referenciam (Hutchins, 1993) quando este conclui que "(...) *auditors are frequently unfamiliar with the client's industry, quality system, process or products/services. This results in a poor quality audit which places conformity at risk.*" Por outro lado, os autores também mencionam (Russell and Regel, 1996) que defendem "*the active involvement of the auditor in the implementation of corrective actions*".

Como se constata pelas afirmações anteriores, o tema das competências do Auditor não pode ser dissociado do contexto da organização em que o Auditor actua, nem do papel que ele supostamente deve desempenhar enquanto elemento que contribui para a correcção ou melhoria dos controlos da organização. Deste modo, as competências do Auditor para conhecer o negócio e para se relacionar com a restante organização são essenciais para não se colocar em risco o próprio processo de Auditoria. Os autores (Power and Terziovski, 2005) mencionam ainda outras competências a identificar nos Auditores e que são relevantes para o sucesso dos processos de Auditoria, como por exemplo: prontidão; comunicação clara; objectividade na definição de critérios de Auditoria; foco na resolução de problemas; capacidade de decisão previamente validada; capacidade para discordar de modo sensível; comprometimento nas relações de trabalho estabelecidas; capacidade para conduzir reuniões de validação ou fecho de Auditoria; etc.

Como se percebe, percorreram-se uma série de ideias iniciais e opiniões dispersas sobre as competências, sendo algumas mais relacionadas com as competências inerentes ao próprio indivíduo e outras mais relacionadas com as competências do processo de Auditoria de SI. Deste modo, torna-se necessária a existência de um modelo que identifique as competências de forma adequada (devidamente arrumadas e classificadas), ou seja, um Modelo de Competências.

Note-se que algumas das competências que já foram apresentadas como desejáveis para o Auditor foram referidas no contexto da Auditoria em geral, sem especificar o tipo de Auditoria. No entanto, considera-se que essas competências que foram referidas são também aplicáveis especificamente aos Auditores de SI.

Contudo, antes de se propor uma arrumação e classificação para as competências específicas da Auditoria de SI, é relevante compreender quais são os principais factores que geralmente determinam essas competências.

4.1.2 Os Determinantes das Competências da Auditoria de SI

Acima de tudo, as competências dos Auditores são alvo de preocupação porque, tal como noutras profissões, são um factor crítico de sucesso para o bom desempenho da profissão de Auditor.

De acordo com os conceitos dos autores (Libby and Luft, 2003), a figura seguinte representa uma equação conceptual das competências que determinam o desempenho dos Auditores.

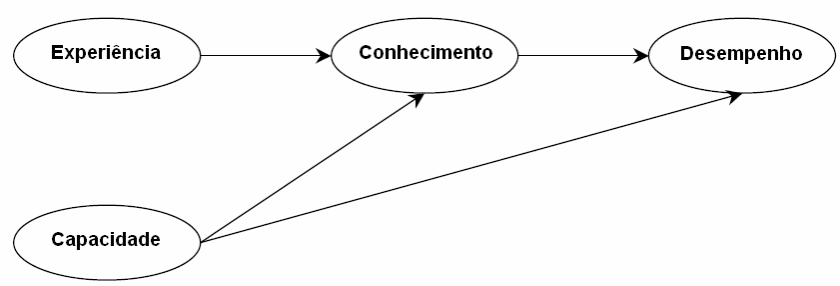


Figura 4.2 - Determinantes das Competências dos Auditores

Fonte: Adaptado da versão original de (Libby and Luft, 2003): "*The Determinants of Auditor Expertise*"

A Experiência e a Capacidade determinam o Conhecimento que, por sua vez, determina o Desempenho. Para além disso, o Desempenho é determinado também directamente pela Capacidade.

A explicação de cada um dos factores referidos e a sua relação com as competências do Auditor é a seguinte:

- Experiência → Determinada, em primeiro grau, pelas competências que o Auditor possui para analisar e para completar todas as tarefas de uma Auditoria. Determinada, em segundo grau, pela escolaridade que Auditor possui em Auditoria e pela formação profissional que obtém, bem como pela prática de discutir temas de Auditoria. Adicionalmente, note-se que diferentes metodologias de Auditoria implicam diferentes níveis de exigência nas tarefas a completar e nos produtos resultantes (*deliverables*) que são necessários para obter uma opinião de Auditoria objectiva e independente. Como consequência, as metodologias de Auditoria (normas, técnicas, ferramentas de suporte, etc.) têm impacto na Experiência que o Auditor vai adquirindo.
- Capacidade → Determinada pelas competências que o Auditor possui para executar tarefas de tratamento e análise de informação que contribuam para a resolução de problemas de Auditoria. Estas competências são genéricas e podem ser avaliadas através de testes psicométricos (exemplo: GMAT) pelo que não são competências específicas de Auditoria.
- Conhecimento → Determinado pelas competências que o Auditor possui em domínios gerais da Auditoria (exemplo: técnicas de avaliação de risco) e em domínios específicos da Auditoria (exemplo: requisitos de segurança de redes). O Conhecimento é definido como informação guardada na memória. No domínio da Auditoria, o Conhecimento do negócio é também fundamental, nomeadamente as estratégias de negócio, os processos de negócio que concretizam essas estratégias, os respectivos riscos de negócio associados e ainda os mecanismos de gestão, monitorização e controlo desses riscos.
- Desempenho → Determinado pelas competências que o Auditor possui para conseguir efectuar uma correcta correspondência entre a sua avaliação dos factos e os critérios de Auditoria, sendo estes, por exemplo, a eficácia ou eficiência do processo que está a auditar. Existem ainda outros determinantes indirectos do Desempenho, tais como a motivação do próprio indivíduo e o ambiente de execução da Auditoria (no sentido de metodologias de Auditoria).

Uma conclusão interessante a retirar desta equação conceptual é que o Desempenho não é determinado directamente pela Experiência em Auditoria (apenas indirectamente via Conhecimento), sendo a Capacidade do Auditor mais directamente determinante. Assim, é possível afirmar que a Capacidade do Auditor é o determinante base, sendo a Experiência e o Conhecimento (em conjunto) os determinantes potenciadores do Desempenho do Auditor.

Tal como os autores atrás referidos reconhecem, o ambiente de execução da Auditoria também é um determinante relevante das competências dos Auditores. No caso da Auditoria de SI, podemos dizer que são três os elementos que o constituem: a Auditoria (as metodologias), os SI (os alvos da Auditoria) e o negócio (o contexto no qual se executa a Auditoria).

Veremos de que modo aqueles três elementos se articulam, recorrendo a algumas das ideias e à adaptação da seguinte figura de (Baskerville and Myers, 2002).

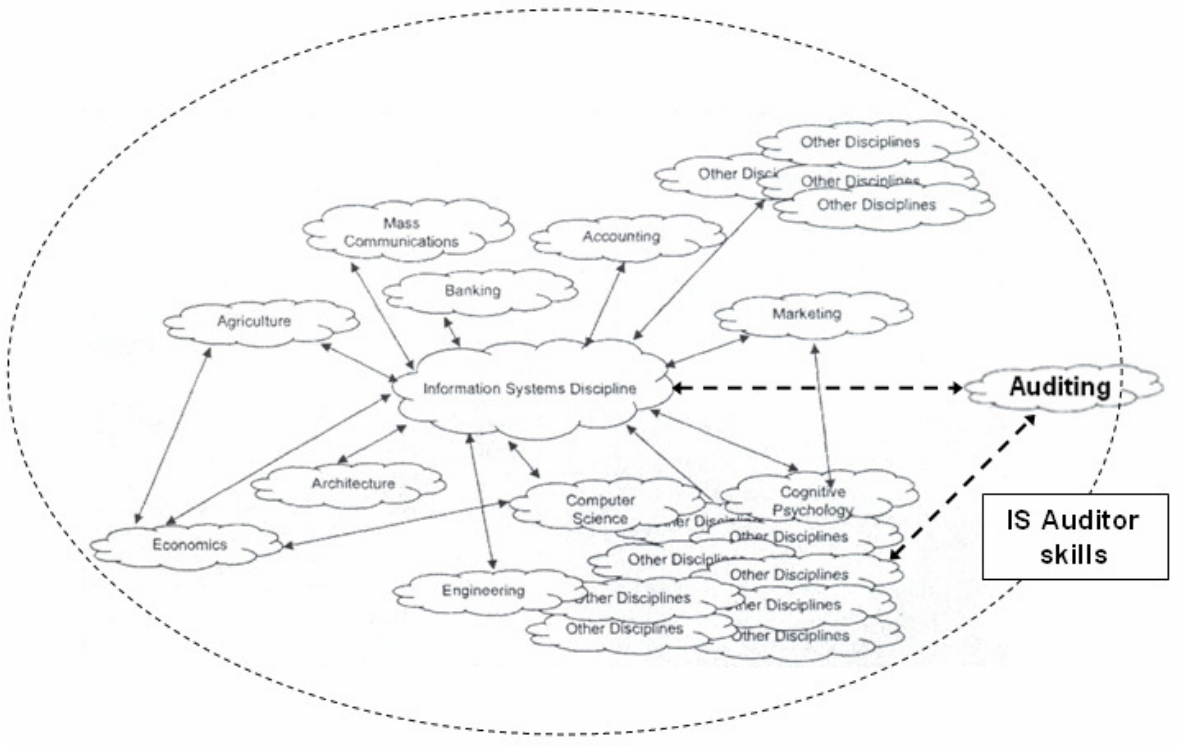


Figura 4.3 - Áreas de Conhecimento com Impacto nos SI

Fonte: Adaptado da versão original de (Baskerville and Myers, 2002):
"*IS as a Reference Discipline in a Discourse with Other Reference Disciplines*"

Segundo estes dois autores, numa visão convencional, os SI são uma área de conhecimento aplicada, formada a partir da aplicação de outras áreas de conhecimento fundamentais, designadas de disciplinas referenciais (exemplos: Engenharia, Economia, Arquitectura, etc.). Numa nova visão proposta pelos referidos autores, os SI deveriam passar a ser encarados como uma área de conhecimento de referência, por direito próprio. Neste sentido, os SI poderiam igualmente passar a ser uma referência que seja aplicada pelas outras áreas de conhecimento. Tal como a figura demonstra, as diversas disciplinas devem ser referenciais recíprocos e mútuos.

Se a Auditoria for considerada como sendo uma das outras áreas de conhecimento, então deduz-se a possibilidade da Auditoria ser uma área de conhecimento aplicada dos SI, resultando daqui a Auditoria de SI. De modo semelhante, cada uma das outras áreas de conhecimento pode representar uma área de negócio auditada (exemplo: Banca, Meios de Comunicação, etc.) ou corresponder a processos de negócio cujos seus SI são auditados (exemplos: Contabilidade, Marketing, etc.). Assim sendo, a Auditoria de SI deverá também aplicar conhecimentos dessas outras áreas de conhecimento. Como consequência, conclui-se que, não só a Auditoria, mas também essas outras áreas de conhecimento são determinantes das competências que o Auditor de SI terá que possuir.

Na verdade, o Auditor de SI deve possuir competências que lhe permitam ter conhecimento sobre os tipos de negócios nos quais está a auditar os respectivos SI. Esta conclusão é importante pois, como foi visto anteriormente, o Conhecimento pode ser o determinante que mais influencia o desempenho do Auditor de SI.

Tendo em conta esta relevância do Conhecimento, na próxima secção serão identificadas as principais áreas de conhecimento do Auditor de SI.

4.1.3 AS ÁREAS DE CONHECIMENTO DO AUDITOR DE SI

No sentido de sistematizar as principais áreas de conhecimento do Auditor de SI, elaborou-se a representação gráfica apresentada na próxima figura. Esta foi inspirada e adaptada a partir da versão original do (PMI, 2004) relativa à área de conhecimento da Gestão de Projectos (*Project Management Body of Knowledge*) e na qual são apresentadas as áreas de conhecimento necessárias a uma Equipa de Projecto. Note-se que se refere às competências para o conjunto dos elementos que constituem uma Equipa de Projecto e não para cada um dos Gestores de Projecto individualmente, uma vez que não é provável cada um dos elementos possuir os conhecimentos na sua totalidade.

Assim, aplicando um raciocínio semelhante, utilizar-se-ão novamente os conceitos da Gestão de Projectos aplicados à realidade da Auditoria de SI (de acordo com a lógica apresentada nas secções 3.5.3 a 3.5.5.). Desta aplicação resulta que a Equipa de Auditoria de SI deverá dominar, no seu conjunto, a área de conhecimento em Auditoria de SI, estando o conhecimento distribuído pelas diversas competências que cada Auditor de SI que constitui essa equipa possui.

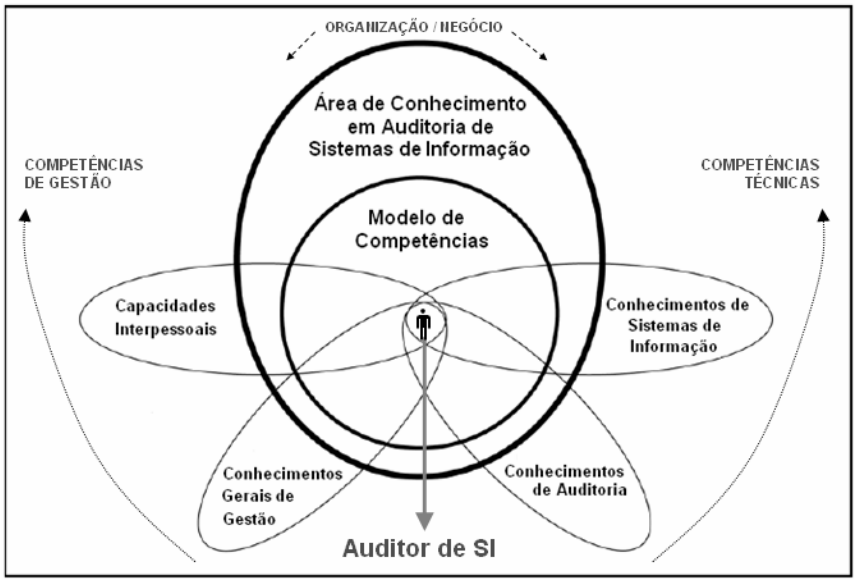


Figura 4.4 - Áreas de Conhecimento do Auditor de SI

Fonte: Proposta elaborada pelo autor, inspirada e adaptada da versão original de (PMI, 2004): "*Areas of Expertise Needed by the Project Team*"

Ao conjunto dos conhecimentos necessários ao adequado desempenho da função de Auditor de SI designou-se por área de conhecimento em Auditoria de SI. Esta é constituída pela intersecção de várias áreas de conhecimento, entre as quais identificaram-se as quatro áreas fundamentais representadas na figura: Capacidades Interpessoais, Conhecimentos Gerais de Gestão, Conhecimentos de Auditoria e Conhecimentos de SI. Associadas a cada uma destas áreas de conhecimento estão as competências do Auditor de SI que podem ser classificadas de Competências de Gestão e de Competências Técnicas. Da intersecção de todos estes conjuntos, resulta um conjunto específico de competências do Auditor de SI que se designou por Modelo de Competências. Existe ainda um factor adicional que deve influenciar a determinação da área de conhecimento do Auditor de SI: a organização em causa e o tipo de negócio, ou seja, a envolvente da Auditoria.

Começar-se-á por explorar este último factor. O conhecimento da organização e do respectivo negócio deverá estar disseminado, na proporção em que for relevante, em cada uma das quatro áreas de conhecimento fundamentais para o Auditor de SI: Capacidades Interpessoais (exemplo: depende do nível de interacção com as áreas auditadas); Conhecimentos Gerais de Gestão (exemplo: depende do tipo de processos de negócio que utilizam os SI que vão ser auditados); Conhecimentos de Auditoria (exemplo: depende dos referenciais metodológicos adoptados para a Auditoria); Conhecimentos de SI (exemplo: depende da sua complexidade, ou seja, se a produção de produtos ou a disponibilização de serviços da organização for fortemente baseada e directamente dependente de SI).

Numa interpretação complementar, efectuando uma leitura das áreas de conhecimento na figura no sentido da esquerda para a direita, vai-se progressivamente saindo de áreas de conhecimento que são mais apreciadas noutras funções (exemplo: Capacidades Interpessoais num Gestor Comercial), passando por outras possíveis áreas (exemplo: Conhecimentos Gerais de Gestão num Gestor Logístico), entra-se na função de Auditoria (exemplo: Conhecimentos de Auditoria num Auditor de Processos de Negócio) e finaliza-se em funções especializadas relacionadas com SI (exemplo: Conhecimentos de SI num Gestor de SI). No fundo, a função de Auditor de SI pode agregar todas estas quatro áreas de conhecimento, existindo uma tendência para tradicionalmente se situar mais nas duas do lado direito da figura.

De seguida, definir-se-ão os dois grandes tipos de competências, relacionando posteriormente com cada uma das quatro áreas de conhecimento fundamentais anteriormente referidas.

- Competências de Gestão → São as competências inerentes aos mecanismos de gestão do próprio indivíduo e aos conhecimentos gerais que o indivíduo possui que são relevantes para a sua profissão.
- Competências Técnicas → São as competências relacionadas com o processo de Auditoria de SI e com os conhecimentos que o indivíduo possui neste domínio.

As duas áreas de conhecimento do lado esquerdo da figura (Capacidades Interpessoais e Conhecimentos Gerais de Gestão) aproximam-se mais das Competências de Gestão. As duas áreas de conhecimento do lado direito (Conhecimentos de Auditoria e Conhecimentos de SI) aproximam-se mais das Competências Técnicas.

Para explicitar e exemplificar as áreas de conhecimento relativas às Competências de Gestão, recorrer-se-á ao (IIA, 2007a) pois este apresenta um bom referencial para a profissão de Auditor, o qual contém uma parte dedicada às Competências de Gestão (*Business Management Skills*). Estas competências estão descritas no documento relativo aos conteúdos do exame para obtenção da certificação profissional de Auditor (CIA - *Certified Internal Auditor*).

Relativamente à área de conhecimento das Capacidades Interpessoais, encontram-se naquele documento os seguintes exemplos de competências: gestão de equipas (dinâmicas de grupo, desenvolvimento de equipas, liderança, gestão pessoal, etc.); negociação (cooperação, resolução de problemas, etc.).

Relativamente à área dos Conhecimentos Gerais de Gestão, tem-se como exemplos: gestão estratégica (técnicas globais de análise, envolvente competitiva do sector, decisões estratégicas, ciclos de vida de produtos, etc.); envolvente global do negócio (cultural, legal, política, económica, financeira, etc.); comportamento organizacional (motivações organizacionais e funcionais, produtividade e eficácia organizacional, processos de comunicação organizacional, estruturas organizacionais, etc.).

Para explicitar e exemplificar as áreas de conhecimento relativas às Competências Técnicas, recorrer-se-á às ideias defendidas pela (ISACA, 2005) pois foram pensadas para a profissão de Auditor aplicada especificamente aos SI.

Nos "Referenciais de Auditoria de SI" (*IS Auditing Standards*) existe um referencial específico para as Competências (*S4 - Competence*), do qual se transcreve a ideia fundamental:
"*The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment. The IS auditor should maintain professional competence through appropriate continuing professional education and training."*

Como se verifica, a ideia fundamental é a competência profissional, dependente das competências e dos conhecimentos do Auditor de SI. Para além disso, o Auditor deverá manter essas competências actualizadas através de formação contínua. De acordo com a estrutura hierárquica de documentos da ISACA (*Standards* → *Guidelines* → *Procedures*), existe também uma orientação (*guideline*) que esclarece sobre o tema da competência (G30 - *Competence*). Nesta, a ISACA afirma que cabe à gestão da organização assegurar que os seus Auditores de SI são tecnicamente competentes e que a Equipa de Auditoria de SI possui, no seu conjunto, as competências e os conhecimentos necessários para efectuarem as Auditorias de forma eficaz, eficiente e também económica. Segundo a ISACA, estas competências e conhecimentos são as previstas na certificação CISA (*Certified Information System Auditor*).

Aliás, o (ISCJ, 2000) refere precisamente que o Auditor de SI deverá possuir idealmente, em termos de escolaridade e formação, uma licenciatura e uma certificação CISA (*Certified Information System Auditor*). Será uma mais-valia se possuir um mestrado, bem como certificações de outro tipo, tais como CPA (*Certified Public Accountant*), CIA (*Certified Internal Auditor*), CFE (*Certified Fraud Auditor*), CISSP (*Certified Information Systems Security Professional*), etc.

De acordo com o (ISACA, 2006), a certificação específica em Auditoria de SI (CISA) é composta pelo seguintes domínios que são alvo de avaliação no exame de certificação (à frente de cada área está indicado o peso percentual no total do exame):

- 1 – Processo de Auditoria de SI (*IS Audit Process*) [10%]
- 2 – Governo dos SI (*IT Governance*) [15%]
- 3 – Gestão do Ciclo de Vida de Sistemas e Infraestruturas (*Systems and Infrastructure Lifecycle Management*) [16%]
- 4 – Produção e Suporte de Serviços de SI (*IT Service Delivery and Support*) [14%]
- 5 – Protecção dos Activos de Informação (*Protection of Information Assets*) [31%]
- 6 – Continuidade de Negócio e Recuperação de Desastres (*Business Continuity and Disaster Recovery*) [14%]

Estes domínios representam, no seu conjunto, as áreas de conhecimento relativas às Competências Técnicas. O primeiro domínio apresentado, relativo ao Processo de Auditoria de SI, equivale à área de Conhecimentos de Auditoria. Os restantes domínios equivalem à área de Conhecimentos de SI. Como se verá mais à frente, estes domínios são muito aproximados dos principais agrupamentos de Competências Técnicas que se irão identificar e descrever no Modelo de Competências (ver na secção 4.2.1).

4.1.4 As Competências de Gestão vs. as Competências Técnicas

Uma vez identificadas as principais áreas de conhecimento do Auditor de SI, de seguida será apresentado um confronto de opiniões entre os dois grandes tipos de competências que constituem essas áreas de conhecimento: as Competências de Gestão vs. as Competências Técnicas.

A seguinte citação de (Sayana, 2002) ajuda a compreender a relevância de confrontar estes dois tipos de competências e, de forma subtil, dá pistas sobre o importante papel das Competências de Gestão.

"*IS audit often involves finding and recording observations that are highly technical. Such technical depth is required to perform effective IS audits. At the same time it is necessary to translate audit findings into vulnerabilities and businesses impacts to which operating managers and senior management can relate. Therein lies a main challenge of IS audit.*"

Efectuando uma possível interpretação das palavras anteriores, compreende-se a necessidade de transformar as excepções (*findings*) em vulnerabilidades para organização, bem como a importância de atribuir impactos numa linguagem e numa escala que sejam úteis ao negócio. O desafio de transformar conceitos técnicos de SI em informação de gestão útil para a restante organização só é atingível utilizando as Competências de Gestão. Este desafio justifica-se, logo à partida, pelos dois principais destinatários do trabalho do Auditor de SI. É indispensável que os Gestores responsáveis pelos processos operacionais de SI entendam, validem e se reconheçam nos problemas identificados pela Auditoria. É valioso que os Gestores de Topo compreendam o significado das conclusões que lhe são apresentadas de modo a antever possíveis consequências negativas para a organização e para poderem mobilizar os meios para as evitar.

No fundo, trata-se de um processo iterativo em que os produtos resultantes da Auditoria (*deliverables*) são produzidos utilizando fortemente as Competências Técnicas em conjugação com a utilização alternada de Competências de Gestão, quer nos momentos de compreensão e análise das situações (Conhecimentos Gerais de Gestão), quer nos momentos de comunicação e de relação com os intervenientes da Auditoria (Capacidades Interpessoais).

Nas opiniões recolhidas pelo (ISCJ, 2000), encontra-se a seguinte afirmação que questiona a necessidade dos Auditores de SI possuírem Competências Técnicas muito especializadas:
"*Because of the technological diversity found in various corporate systems, desired skills do vary. Experience required depends on the needs of a client, but there are some common requirements.* (...) *There is still room for specialists, but the more diversified a candidate's technical background, the more marketable he or she is.*"

A afirmação anterior revela que, embora haja necessidade de Auditores de SI muito especializados, o mercado de trabalho demonstra preferência por Auditores de SI mais diversificados. Segundo esta opinião, as empresas dependem fortemente do conhecimento dos Auditores de SI, nomeadamente das suas Competências Técnicas em Auditoria, mas consideram ser sobretudo a atitude do Auditor que o torna consistente.

Ora a atitude pertence ao domínio das Competências de Gestão, pelo que poderá existir no mercado uma tendência emergente para atribuir uma crescente importância a estas competências, diminuindo o foco nas Competências Técnicas.

Por outro lado, existem outras opiniões, como as de (Davis, Schillerand and Wheeler, 2007) que não deixam de reforçar a importância das Competências Técnicas, quer na área de Conhecimentos de Auditoria, quer na área de Conhecimentos de SI.

Quanto aos conhecimentos em Auditoria, estes autores referem que é essencial que a Equipa de Auditoria de SI contenha elementos que sejam Auditores de carreira, com experiência e saber teórico sobre os processos da área de Conhecimentos de Auditoria. No entanto, também é essencial a presença de Auditores que detenham conhecimento operacional dos SI, podendo os Auditores de SI serem ex-profissionais da área dos SI.

Quanto aos Conhecimentos em SI, estes autores referem o facto de determinado tipo de Auditores de SI efectuarem um trabalho que não é uma verdadeira Auditoria de SI pois limitam-se a analisar apenas o nível aplicacional dos SI. A causa desta limitação está muitas vezes na

falta de Competências Técnicas apropriadas em SI que lhes permitam conhecer, compreender e analisar devidamente os restantes níveis dos SI (ver os níveis de SI na secção 3.3.2).

Daqui se conclui que um modelo misto de áreas de conhecimento, tanto em Auditoria, como em SI, são essenciais para formar um corpo de Competências Técnicas adequado.

Numa outra linha de raciocínio, (Prakarsa, 1996) associa novamente o tema da especialização às Competências Técnicas:
"*Today, no one individual in the field knows all systems and platforms equally which has caused IS audit and control professionals to specialize. The future requires all IS audit and control auditors to continually learn and explore new technologies and methodologies*."

Esta afirmação exprime um dilema habitual nas Equipas de Auditoria de SI relativamente à manutenção dos seus níveis de Competências Técnicas, nomeadamente os Conhecimentos em SI. Devido à proliferação de diversos tipos de SI e TIC, os Auditores de SI são obrigados a aprender e explorar continuamente apenas determinados tipos de desenvolvimentos tecnológicos ou, então, as suas Competências Técnicas ficarão desactualizadas de um modo geral. Por outro lado, também poderá ter que existir especialização dos Auditores de SI em determinadas Competências Técnicas da área de Conhecimentos em Auditoria dado que há metodologias mais adequadas para serem seleccionadas e utilizadas consoante o tipo de SI ou TIC em causa.

Da discussão sobre a relevância das Competências Técnicas face às de Gestão (ou vice-versa), poder-se-á tirar uma ilação. O Auditor de SI poderá ser levado a optar pela especialização ou não. A dimensão da organização onde o Auditor de SI se encontra inserido, a variedade dos seus SI e TIC e ainda o tipo de negócio poderão justificar a especialização ou, pelo contrário, a diversificação de conhecimentos em Auditoria de SI.

Quanto mais especializado for o Auditor de SI em determinados SI ou TIC, mais críticas se tornam as Competências Técnicas e, dentro destas, as da área de Conhecimentos de SI. Por outro lado, quanto menos especializado for o Auditor de SI, a área de Conhecimentos em Auditoria assume maior importância. Neste caso, o Auditor de SI deverá dominar melhor a

metodologia e possuir conhecimento sobre diversos referenciais metodológicos de modo a identificar os que melhor se adequam a diferentes SI ou TIC, em diferentes contextos de Auditoria (exemplos: Auditorias de Controlos Gerais, Auditorias Aplicacionais, etc.)

Pode-se afirmar adicionalmente que quanto menos especializado for o Auditor, mais necessárias se tornam as Competências de Gestão. Neste caso, dada a diversidade de SI ou TIC a auditar, a área de conhecimento relativa às Capacidades Interpessoais assume maior relevância pois o Auditor de SI necessitará de interagir com variadas áreas de negócio que utilizam esses SI e TIC (com interlocutores frequentemente diferentes). A área dos Conhecimentos Gerais de Gestão também se torna mais necessária para a compreensão dos processos de negócio em causa (que podem variar muito consoante a utilização que estes fazem dos SI e TIC).

Para encerrar a confrontação das Competências de Gestão vs. Técnicas, apresenta-se na figura seguinte uma proposta de posicionamento conceptual das competências da função de Auditoria de SI.

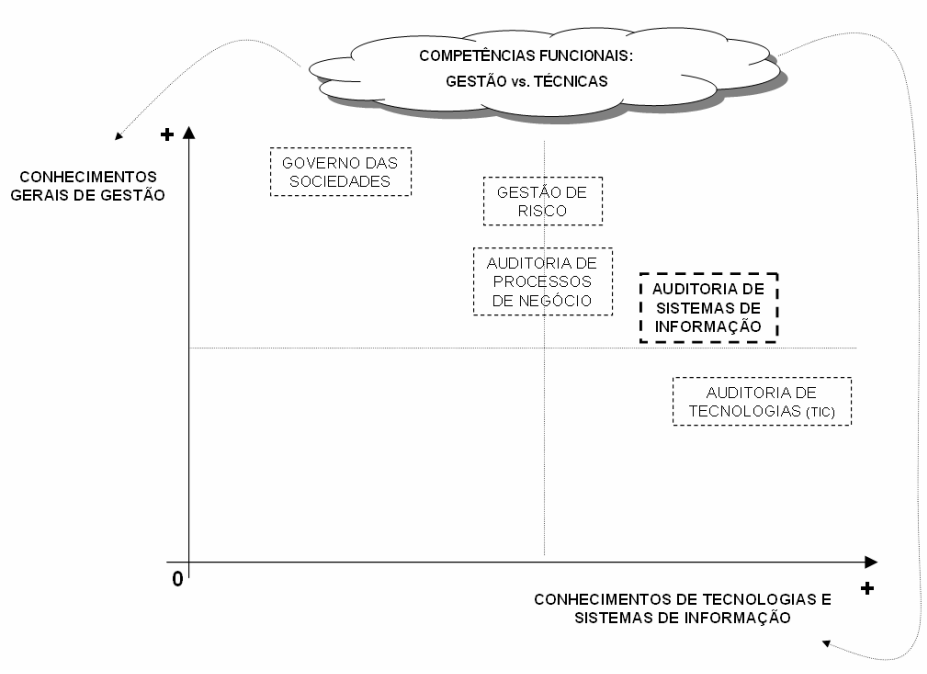


Figura 4.5 - Posicionamento Conceptual das Competências de Auditoria de SI

Fonte: Proposta elaborada pelo autor

Para explicitar esta proposta de posicionamento conceptual das competências, dentro das Competências de Gestão, focar-se-á nos Conhecimentos Gerais de Gestão e, dentro das Competências Técnicas, focar-se-á nos Conhecimentos de SI. A interpretação da figura deverá ter também em conta a proposta de posicionamento conceptual da função Auditoria de SI apresentada no Capítulo 3 (figura 3.2 da secção 3.2.2).

Como se pode constatar, à medida que se desce no nível dos instrumentos de Governo das Sociedades (*Corporate Governance*), diminui o nível exigido para os Conhecimentos Gerais de Gestão e aumenta o nível exigido para os Conhecimentos de SI. De facto, de entre os instrumentos de Governo das Sociedades apresentados (Gestão de Risco, Auditoria de Processos de Negócio e Auditoria de SI), é na Auditoria de SI que as Competências Técnicas sobre SI se tornam mais necessárias. Mais ainda, de acordo com o referido modelo de posicionamento da função, encarando a Auditoria de Tecnologias (TIC) como um subconjunto especializado da Auditoria de SI, então o nível exigido de Conhecimentos de SI e de TIC é ainda maior.

Em sentido inverso, o nível de Conhecimentos Gerais de Gestão aumenta, à medida que se sobe no nível dos instrumentos de Governo das Sociedades, dado que a abrangência/âmbito desses instrumentos é crescente. Repare-se que o Auditor de Processos de Negócio, por ter como âmbito todos os processos de negócio (não se limita aos de SI), é o que deve apresentar um balanceamento (*trade-off*) mais equilibrado entre Conhecimentos Gerais de Gestão e Conhecimentos de SI. Por comparação, acrescenta-se ao Gestor de Risco um nível mais elevado de Conhecimentos Gerais de Gestão.

Como conclusão desta secção, pode-se afirmar que é indispensável a presença de um misto de Competências Técnicas e de Gestão. Para os Auditores de SI, existe um nível médio desejável, por comparação com outras funções relacionadas. Situando-se na Auditoria de SI esse nível pode variar consoante o grau de especialização do Auditor de SI, implicando diferentes combinações de Competências Técnicas e de Gestão. Certamente continuará a ser necessária a existência de Auditores de SI com Competências Técnicas sobre SI muito fortes (porque, por exemplo, são especializados em Auditorias de Segurança aos SI e TIC). No entanto, as Competências de Gestão são (ou devem ser) cada vez mais valorizadas nos Auditores de SI (porque, por exemplo, contribuem para um melhor desempenho do trabalho de cada Auditor).

4.2 O MODELO DE IDENTIFICAÇÃO DE COMPETÊNCIAS DO AUDITOR DE SI

Nesta secção é efectuada a descrição de um Modelo de Competências que é proposto pelo autor do presente trabalho: "MICASI - Modelo de Identificação de Competências do Auditor de SI". Sentiu-se necessidade de construir este modelo dado que na bibliografia académica e profissional não foi identificado nenhum Modelo de Competências abrangente, aplicado à realidade da Auditoria de SI. Para além disso, nas pesquisas efectuadas, identificaram-se maior número de referências às Competências de Gestão, sendo mais raras as obras sobre Competências Técnicas relacionadas com Auditoria de SI.

De seguida descrever-se-á o processo de investigação e de construção do modelo, onde se terá a oportunidade de compreender que o modelo resultou da utilização adaptada de dois referenciais distintos, um sobre Competências de Gestão e outro sobre Competências Técnicas. Posteriormente será efectuada uma descrição das funcionalidades da ferramenta que foi desenvolvida para suportar o modelo, encerrando-se a presente secção com uma apresentação sucinta de diversas hipóteses de aplicação do modelo em contexto de investigação académica e em contexto empresarial.

4.2.1 O PROCESSO DE INVESTIGAÇÃO E CONSTRUÇÃO DO MODELO

O principal objectivo deste sub-processo de investigação foi construir um modelo que permita identificar quais as competências necessárias e mais importantes para a função Auditoria de SI. O modelo construído foi designado de "MICASI - Modelo de Identificação de Competências do Auditor de SI", justificando-se a escolha desta designação pelos objectivos do modelo acima indicados. O carácter de "Identificação" que a designação do modelo anuncia tornar-se-á mais explícito posteriormente (na secção 4.2.3) quando se apresentarem os possíveis contextos e variantes de aplicação do modelo.

O modelo MICASI está estruturado de acordo com os dois principais tipos de competências apresentados e descritos anteriormente (nas secções 4.1.3 e 4.1.4), subdividindo-se em:

- Competências de Gestão (*soft skills* ou *non-technical skills*)
- Competências Técnicas (*hard skills* ou *technical skills*)

O processo de investigação iniciou-se com a tarefa de identificar referenciais ou modelos de competências que se adequassem aos dois grandes tipos de competências acima referidos (Gestão e Técnicas), bem como fossem compatíveis com as ideias sobre Auditoria de SI defendidas ao longo dos Capítulos 2 e 3. Da pesquisa efectuada na literatura académica e profissional, não foi identificado um modelo ou referencial que respondesse na globalidade aos requisitos anteriores mas identificaram-se dois modelos separados que se consideram adequados para cada um dos tipos de competências:

- Competências de Gestão → Modelo de Quantificação de Competências de Gestão para Gestores de Projectos (*SSQ - Soft Skills Quantification for Project Manager Competencies*) da autoria de (Muzio, Fisher, Thomas and Peters, 2007).
- Competências Técnicas → Modelo Curricular para Auditoria e Controlo de SI (*Model Curriculum for IS Audit and Control*) da autoria da (ISACA, 2004).

Relativamente à escolha do Modelo de Quantificação de Competências de Gestão para Gestores de Projectos (SSQ), justifica-se por estar alinhada com a visão de que uma Auditoria de SI pode ser gerida à semelhança de uma Gestão de Projecto (ver nas secções 3.5.3 a 3.5.5). Adicionalmente justifica-se por ser um modelo muito recente, adaptado às exigências actuais das organizações em termos de Competências de Gestão. Segundo os autores do modelo (Muzio, Fisher, Thomas and Peters, 2007), existe muita investigação e literatura que reconhece a necessidade da existência das Competências de Gestão (*soft skills, micro-social skills*, etc.), mas não existem obras que detalhem formas de identificar e avaliar/quantificar essas competências, nem que as relacionem com a Gestão de Projectos.

Aliás, também não foram encontradas obras que permitam identificar e avaliar as Competências de Gestão no contexto específico da Auditoria de SI. No entanto, no contexto da Auditoria em

geral (não específica de SI), num dos domínios da certificação CIA (referidos na secção 4.1.3), podemos encontrar algumas referências úteis às Competências de Gestão (*Business Management Skills*). Estas, apesar de estarem bem desenvolvidas ao nível dos Conhecimentos Gerais de Gestão, não estão tão abrangentes ao nível das Capacidades Interpessoais, quando comparadas com o modelo SSQ. Tendo em conta o exposto, considera-se que a adaptação para a Auditoria de SI do modelo SSQ originalmente desenvolvido para a Gestão de Projectos é uma opção adequada.

Relativamente à escolha do Modelo Curricular para Auditoria e Controlo de SI da ISACA, justifica-se por ser um modelo desenvolvido especificamente para explicitar as competências que um Auditor de SI deverá possuir. Este modelo está alinhado com as necessidades e as expectativas dos profissionais de Auditoria de SI pois baseia-se em investigação efectuada com a colaboração de académicos, profissionais de Auditoria, empresas de Auditoria e associações profissionais de Auditoria. Este modelo está também alinhado com a estrutura do CobiT (ver na secção 3.4.2) e com os domínios da certificação CISA (ver na secção 4.1.3).

O Modelo Curricular da ISACA é claramente orientado para as Competências Técnicas, embora num apêndice do modelo se possa encontrar uma breve referência a um conjunto de competências que a ISACA não detalha, pois considera não estarem directamente consideradas no perfil que é específico do Auditor de SI e, também, por serem comuns a outras profissões. A ISACA designa estas competências como "sugestão de competências complementares" e pelos exemplos que fornece, conclui-se que se tratam de Competências de Gestão (exemplos: capacidades de comunicação, entrevista, negociação, escrita, psicologia organizacional, comportamento, gestão de projecto, gestão de equipas, etc.).

Segundo a (ISACA, 2004), existe uma elevada procura pela profissão de Auditor de SI que muitas vezes é desempenhada por especialistas em SI ou por profissionais de outras áreas de negócio (exemplo: financeira, comercial, etc.). Este possuem algumas competências relacionadas com SI, mas nem sempre possuem as Competências Técnicas relacionadas com a Auditoria que sejam adequadas para o exercício da função. Verifica-se também que estes profissionais nem sempre conseguem manter actualizadas as suas Competências Técnicas

sobre SI devido ao elevado ritmo de desenvolvimento das tecnologias. Estes profissionais que não estão suficientemente preparados para a função, para colmatar as suas lacunas de formação recorrem geralmente aos seguintes três tipos de soluções: participação em formação interna ministrada pela organização em conjunto com formação por aprendizagem no próprio posto de trabalho; participação em eventos e seminários promovidos por associações profissionais ou por fornecedores; e obtenção de licenciaturas ou pós-graduações na área de Auditoria de SI ou obtenção de certificações profissionais. A última das três hipóteses, na qual se inclui a certificação CISA, é a que proporciona o conhecimento e as Competência Técnicas mais aprofundadas para o exercício da função. Deste modo, torna-se necessária a existência de um Modelo Curricular, como o da ISACA, que defina e regule quais deverão ser essas competências e que possa ser usado como referência por aqueles três grandes tipos de formação. Neste contexto, o Modelo Curricular do ISACA parece ser a opção mais conveniente para ser utilizado como referencial para as Competências Técnicas.

Assim, o modelo MICASI foi construído através da utilização dos conteúdos presentes nos dois referenciais atrás apresentados (Modelo SSQ e Modelo Curricular ISACA). O produto final da adaptação pode ser consultado no **Anexo 2: Modelo de Identificação de Competências do Auditor de SI (MICASI)**. Desta adaptação, resultou a identificação do seguinte número de competências:

- Competências de Gestão → 23 competências identificadas → consultar as competências e sua respectiva descrição no **Anexo 2** na grelha "Competências de Gestão (*soft skills*)"
- Competências Técnicas → 27 competências identificadas, agrupadas em 7 domínios → consultar as competências e sua respectiva descrição no **Anexo 2** na grelha "Competências Técnicas (*hard skills*)"

Relativamente à adaptação do Modelo de Quantificação de Competências de Gestão (SSQ), não foram utilizados todos os conceitos e mecanismos de análise que este modelo originalmente prevê. O SSQ permite auxiliar os Gestores de Projectos a identificarem as 6 Competências de Gestão que consideram mais importantes para um desempenho de sucesso dos elementos das suas equipas, a partir de uma listagem de 23 Competências de Gestão que o modelo descreve. O modelo também permite que os Gestores de Projecto o utilizem como base para efectuar uma

avaliação real das suas equipas quanto às 6 competências pré-determinadas como mais importantes (atribuindo para cada um dos elementos da equipa uma classificação e indicando qual a competência mais forte e qual a mais fraca). Na adaptação efectuada do SSQ para o modelo MICASI, estes mecanismos de análise não foram utilizados (não se seleccionou *a priori* um conjunto de 6 competências pré-determinadas para a análise). A adaptação efectuada consistiu apenas na utilização das 23 competências (nome e respectivas descrições) que modelo original de (Muzio, Fisher, Thomas and Peters, 2007) define.

Relativamente à adaptação do Modelo Curricular da ISACA, este não foi utilizado com o seu propósito original que é ser um referencial curricular para cursos de formação de Auditoria de SI. A adaptação efectuada consistiu na utilização do modelo da ISACA como uma fonte para a identificação das Competências Técnicas para o modelo MICASI. Relativamente ao modelo original da ISACA, mantiveram-se as competências divididas em 7 agrupamentos, correspondentes aos domínios de conhecimento necessários para a profissão de Auditor de SI. O primeiro domínio, relativo aos "Processo de Auditoria", equivale à área de Conhecimentos de Auditoria. Os restantes domínios, a partir do segundo, equivalem à área de Conhecimentos de SI.

Os nomes e respectivas descrições das 27 Competências Técnicas que foram consideradas resultaram dum exercício de resumir os tópicos e sub-tópicos dos conteúdos de formação que a (ISACA, 2004) define para cada um dos já referidos 7 domínios de conhecimento:

- 1 – Processo de Auditoria
- 2 – Gestão, Planeamento e Organização dos SI
- 3 – Infraestruturas Técnicas e Práticas Operacionais de SI
- 4 – Protecção dos Activos de Informação
- 5 – Recuperação de Desastres e Continuidade de Negócio
- 6 – Desenvolvimento, Aquisição, Implementação e Manutenção de Aplicações de Negócio
- 7 – Avaliação de Processos de Negócio e Gestão do Risco

Uma vez descrito o processo de investigação e construção do modelo MICASI, na próxima secção serão descritas e apresentadas visualmente as funcionalidades da ferramenta que foi desenvolvida para suportar o modelo MICASI.

4.2.2 A Descrição das Funcionalidades da Ferramenta de Suporte ao Modelo

Com o objectivo operacionalizar o modelo MICASI, ou seja, dotá-lo de funcionalidades que o tornem aplicável na prática, procedeu-se ao desenvolvimento duma ferramenta de suporte.

Através da figura seguinte é possível visualizar um resumo das funcionalidades da ferramenta de suporte ao modelo. A descrição e compreensão das funcionalidades deve ser acompanhada com a consulta do **Anexo 2: Modelo de Identificação de Competências do Auditor de SI (MICASI)**.

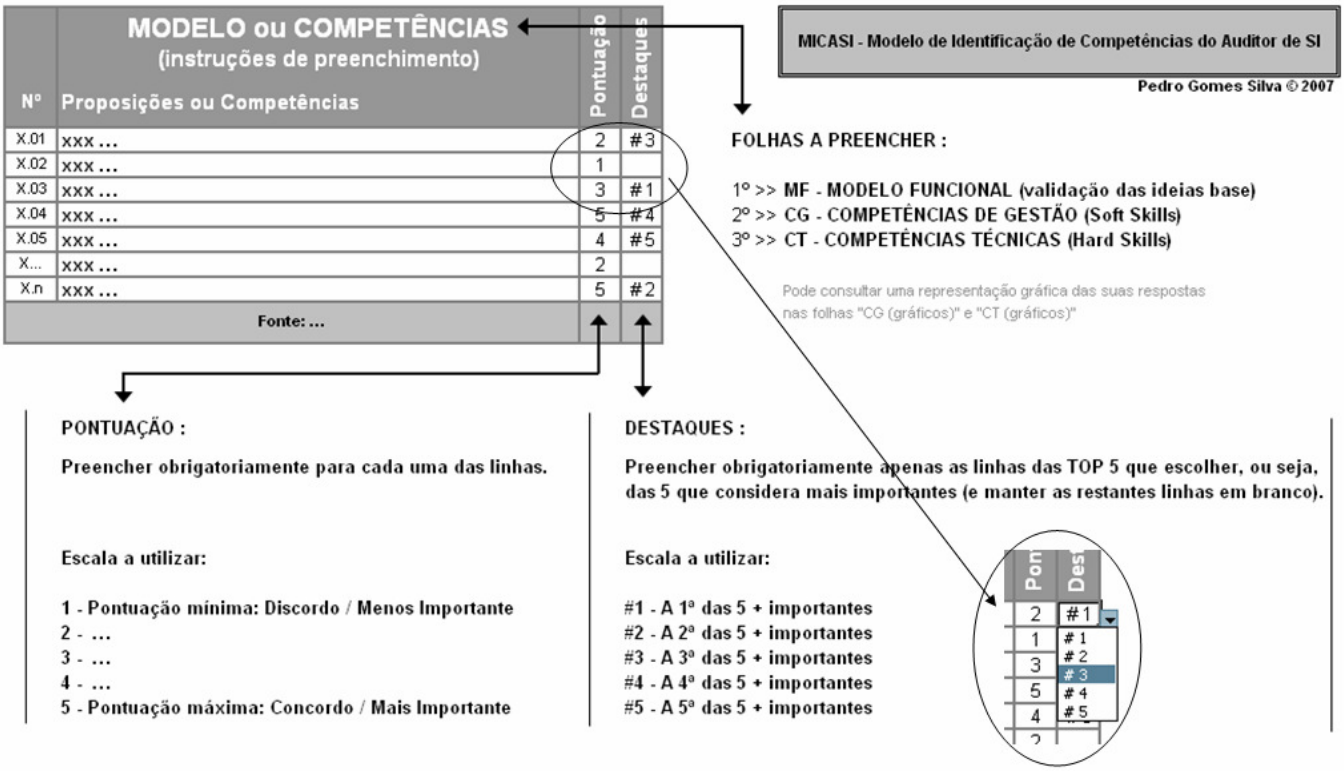


Figura 4.6 - Funcionalidades de Preenchimento da Ferramenta de Suporte ao MICASI

Fonte: Elaborado pelo autor

A ferramenta é composta por 3 grelhas/folhas para preenchimento, designadamente:

- 1ª – MF → "Modelo Funcional (validação das ideias base)"
- 2ª – CG → "Competências de Gestão (*Soft Skills*)"
- 3ª – CT → "Competências Técnicas (*Hard Skills*)"

Adicionalmente, a ferramenta possui ainda uma folha inicial de "Instruções" de preenchimento (que corresponde à figura anterior apresentada). As folhas seguintes da ferramenta, as 3 acima indicadas, são as que se destinam ao preenchimento por parte dos utilizadores da ferramenta.

A ferramenta foi desenvolvida na aplicação MS Excel por esta possuir um conjunto de vantagens adequadas às tarefas de desenvolvimento da ferramenta e, posteriormente, às de análise de resultados (exemplos: flexibilidade de estruturação, validação de dados, ordenação e tratamento de resultados, representação gráfica dos resultados, etc.).

Procedeu-se ao desenvolvimento da ferramenta tendo em conta os objectivos e as utilizações pretendidas no âmbito da investigação, nomeadamente:

- Garantir, em todos os passos de desenvolvimento, uma coerência da ferramenta com o modelo MICASI (definido na secção 4.2.1) e com as ideias defendidas para a função Auditoria de SI (apresentadas ao longo dos Capítulo 2. e 3.).
- Possibilitar a aplicação prática do modelo MICASI nas entrevistas semi-estruturadas a profissionais de Auditoria de SI, a partir das quais se efectua a avaliação qualitativa dos resultados (ver secções 4.3.1 e 4.3.2).
- Elaborar uma listagem que identifique as competências relevantes, com a respectiva descrição de cada uma delas, arrumadas em duas grelhas "Competências de Gestão" e "Competências Técnicas" que representam os dois grandes tipos de competências (de acordo com o modelo MICASI definido na secção 4.2.1).
- Construir um mecanismo de classificação das competências, contendo uma funcionalidade de "Pontuação" de cada uma das competências e uma componente de "Destaque" das competências consideradas mais importantes.

Tendo em conta estes objectivos e utilizações pretendidas, em especial os dois primeiros (garantir coerência com as ideias defendidas para a função Auditoria de SI e a aplicação em entrevistas semi-estruturadas), chegou-se à conclusão que era necessário introduzir na ferramenta um mecanismo, inicialmente não previsto, que permitisse alinhar os profissionais de Auditoria de SI que iriam utilizar a ferramenta com as ideias defendidas para a função Auditoria de SI. Este mecanismo justifica-se e será também útil nos casos em que a ferramenta é utilizada fora do contexto da presente Tese, ou seja, por um indivíduo que não tem conhecimento das ideias defendidas neste texto para a Auditoria de SI.

Optou-se então por elaborar uma grelha adicional (1ª grelha/folha de preenchimento) designada "Modelo Funcional". Esta contém um conjunto de proposições que resumem essas ideias, servindo assim como um mecanismo de validação das ideias base, a utilizar antes das grelhas das "Competências de Gestão" e das "Competências Técnicas". Relativamente às proposições do Modelo Funcional que estão na 1ª grelha/folha de preenchimento, foram elaboradas pelo autor do presente trabalho, sendo originais ou compiladas a partir de diversas fontes indicadas na bibliografia.

De seguida, serão referidas algumas das funcionalidades de preenchimento da ferramenta e, posteriormente, serão apresentadas as funcionalidades de análise da ferramenta.

No sentido de facilitar as tarefas de preenchimento (e, também posteriormente, as de análise), a cada uma das proposições e das competências foi atribuída uma numeração de acordo com a seguinte nomenclatura:

- Proposições do Modelo Funcional → MF.nn , sendo "MF" = Modelo Funcional e "nn" a numeração sequencial das 16 proposições apresentadas.
- Competências de Gestão → CG.nn , sendo "CG" = Competências de Gestão e "nn" a numeração sequencial das 23 competências apresentadas.
- Competências Técnicas → CT.dn , sendo "CT" = Competências Técnicas, "d" a numeração dos 7 domínios de conhecimento apresentados, e "nn" a numeração sequencial das competências apresentadas dentro de cada domínio.

Em cada uma das três grelhas/folhas, existem duas colunas para classificação das proposições ou das competências, com obrigatoriedade de preenchimento de acordo com as seguintes regras:

- "Pontuação" → O utilizador da ferramenta tem de preencher obrigatoriamente para cada uma das proposições ou competências em causa. A escala a utilizar vai desde " 1 - Pontuação mínima: Discordo / Menos Importante" até " 5 - Pontuação máxima: Concordo / Mais Importante ".
- "Destaques" → O utilizador da ferramenta tem preencher obrigatoriamente apenas as linhas das *TOP 5* que escolher, ou seja, das 5 que considera mais importantes (e manter as restantes linhas em branco). O objectivo da coluna "Destaques" é precisamente "obrigar" o utilizador da ferramenta a optar e escolher, por exemplo, de entre dois valores "5" qual o que considera mais importante e efectuar, sucessivamente o mesmo exercício para os valores "4", "3", "2", "1" até obter um máximo de 5 destaques no total da grelha/folha em causa.

Note-se que a ferramenta possui um mecanismo de restrição/validação dos valores que o utilizador da ferramenta pode introduzir nas grelhas de resposta (ver o destaque na última figura apresentada). Estes dois conceitos de "Pontuação" (classificação das competências) e "Destaques" (destacar quais as competências mais fortes) foram inspirados em conceitos semelhantes previstos no Modelo SSQ (referido na secção 4.2.1).

Foram também desenvolvidos na ferramenta mecanismos que permitem uma rápida análise e interpretação dos resultados após preenchimento, nomeadamente:

- A ordenação das classificações por ordem decrescente de "Pontuação" e por ordem crescente de "Destaques", tanto para as Competências de Gestão, como para as Competência Técnicas para que, após o entrevistado tenha efectuado a suas classificações nas grelhas, seja possível identificar de forma rápida as competências com melhor classificação e com pior classificação.
- A visualização através de gráficos das "Pontuações" e dos "Destaques", para cada uma das competências, agrupadas também em Competências de Gestão e Competência Técnicas, para permitir igualmente uma rápida análise aquando das entrevistas semi-estruturadas.

A próxima figura expõe alguns exemplos das funcionalidades gráficas de análise que a ferramenta possui para os dois principais tipos de competências:

- Competências de Gestão → 1 gráfico de barras (horizontal) + 1 gráfico circular (radar)
- Competências Técnicas → 1 gráfico de barras (horizontal) + 2 gráficos circulares (radar), sendo um destes últimos relativo à totalidade das Competências Técnicas e outro relativo ao valor médio das Competências Técnicas em cada um dos 7 domínios de conhecimento.

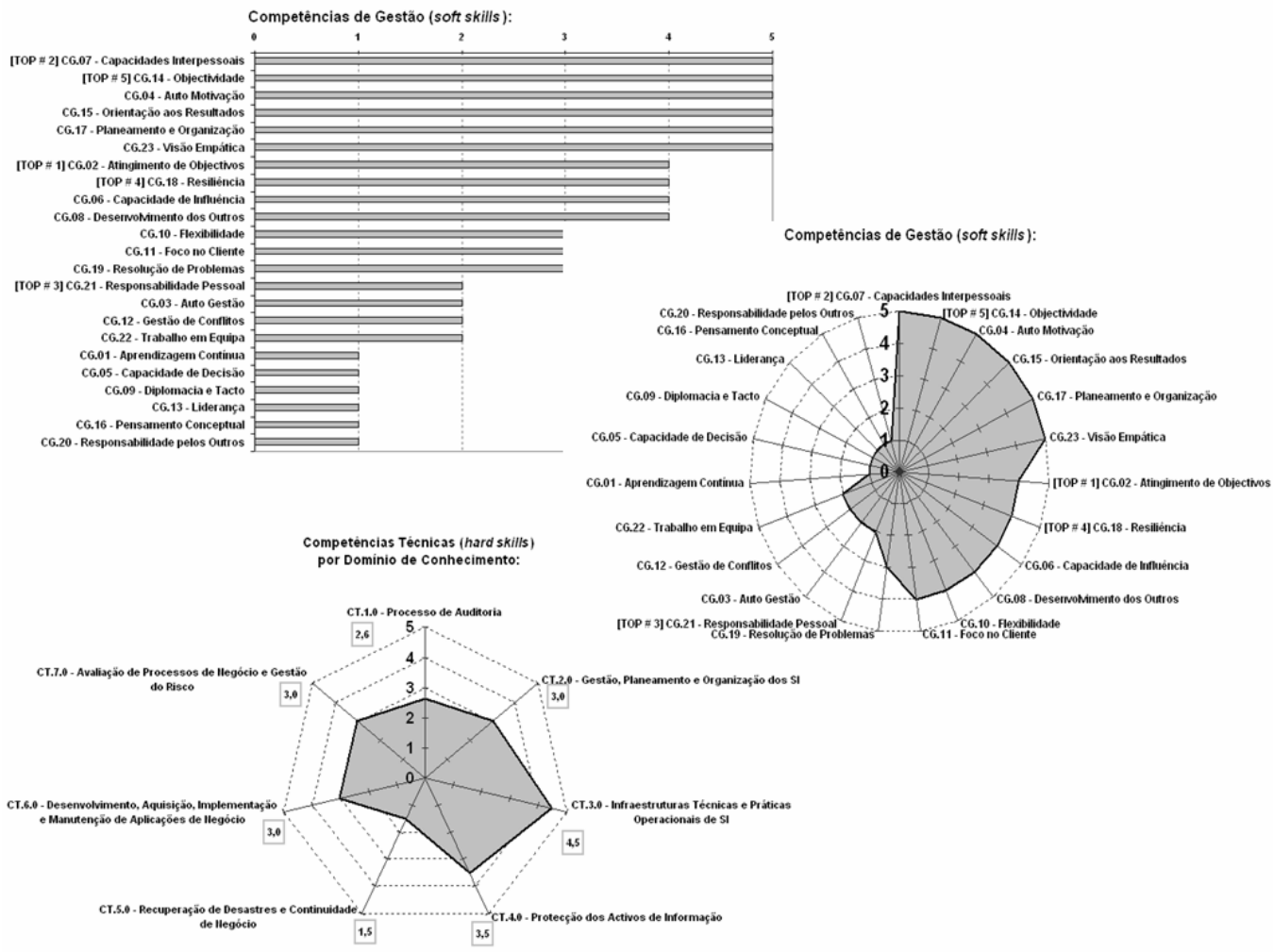


Figura 4.7 - Funcionalidades de Análise da Ferramenta de Suporte ao MICASI

Fonte: Elaborado pelo autor

Note-se que os valores/resultados apresentados nos 3 gráficos da figura são meramente exemplificativos. Os gráficos tanto podem ser apresentados com as competências na sua ordenação original (correspondente à numeração sequencial), como por ordenação decrescente de "Pontuação" (tal como nos exemplos apresentados na figura). A primeira hipótese permite efectuar comparações entre respostas de diferentes utilizadores, enquanto que a segunda hipótese é mais adequada para analisar as ordens de importância atribuídas por um só determinado utilizador da ferramenta. Os gráficos indicam também os "Destaques" através da aposição da indicação "TOP #n" a preceder a numeração e o nome da competência, caso esta tenha sido alvo de destaque.

4.2.3 A Aplicabilidade do Modelo em Contexto de Investigação e Empresarial

Existem dois principais contextos para possíveis aplicações do Modelo MICASI, para os quais se concretizam de seguida algumas hipóteses.

- Contexto de Investigação → Aplicar o modelo para investigação académica na área das Competências de Auditoria de SI, a partir do qual se possa efectuar:
  - Identificação de Competências → Utilização como um dicionário de competências. Serve como um denominador comum para grupos de trabalho na mesma área de investigação em Auditoria de SI pois cada competência possui uma designação única e uma respectiva descrição.
  - Classificação de Competências → Utilização como base para a realização de inquéritos ou para a realização de entrevistas semi-estruturadas. Estes podem ser realizados a académicos ou profissionais da área de Auditoria de SI com vista à classificação das competências que considerem como mais importantes num Auditor de SI.
- Contexto Empresarial → Aplicar o modelo como instrumento de gestão dos recursos humanos da Equipa de Auditoria de SI, podendo ser utilizado como:
  - Referencial de Competências → Utilização para pré-definir níveis de competências desejáveis num Auditor de SI (na escala de 1 a 5). O modelo pode ter diferentes níveis pré-definidos para cada uma das competências, dependendo do nível de carreira do

Auditor de SI em causa (exemplos: Auditor Júnior de SI, Auditor Sénior de SI, Gestor de Auditoria de SI, Director de Auditoria de SI, etc.).

- Identificação de Competências → Utilização como instrumento de diagnóstico de competências aquando do recrutamento de Auditores de SI. A informação recolhida no processo de recrutamento (entrevistas, currículos, referências de terceiros, etc.) pode ser analisada e registada de forma estruturada na ferramenta, servindo para identificar pontos fortes ou fracos dos candidatos e permitindo também efectuar comparações entre candidatos.
- Avaliação de Competências → Utilização no âmbito do processo de avaliação anual dos Auditores de SI. Pode ser efectuada uma comparação entre o nível real de cada uma das competências observadas no Auditor de SI e o nível pré-definido como desejável em cada competência.

Adicionalmente, o modelo poderá ser utilizado em contexto empresarial também para a função de Controlo Interno de SI, quer na vertente de Competências de Gestão, quer na vertente de Competências Técnicas. Esta hipótese é justificável pois as Competências Técnicas previstas no modelo são baseadas no Modelo Curricular da ISACA que foi desenvolvido não só para a função de Auditoria de SI, mas também para a função de Controlo de SI.

Ainda em contexto empresarial, o modelo poderá ser aplicado a outras funções duma organização, embora de forma não tão abrangente. A vertente relativa às Competências de Gestão poderia ser aplicada a funções que, tal como defendemos para a Auditoria de SI, também deverão possuir competências semelhantes às das Gestão de Projectos (exemplos: Auditoria de Processos de Negócio, Gestores de Projectos de SI, etc.). A vertente relativa às Competências Técnicas poderia ser aplicada a funções de SI (exemplos: Responsável de Segurança de SI, Responsável de Qualidade de SI, etc.).

No que se refere ao contexto de investigação, na próxima secção serão mostrados os resultados duma possível aplicação do modelo neste contexto, nomeadamente utilizando-o para classificação de competências.

4.3 Os Resultados da Aplicação do Modelo de Competências

Nas próximas secções apresentam-se os resultados da aplicação prática do modelo MICASI descrito anteriormente. O modelo foi aplicado em contexto de investigação, designadamente como base para a realização de três entrevistas semi-estruturadas a profissionais da área de Auditoria de SI. O objectivo das entrevistas foi a classificação das competências que estes profissionais consideram como mais importantes para um Auditor de SI.

Assim, após um breve enquadramento do processo de realização das entrevistas, será efectuada a análise qualitativa dos resultados das entrevistas. Esta análise incluirá, para cada um dos grandes tipos de competências (Gestão e Técnicas), os seguintes pontos: uma representação gráfica da análise das classificações; a identificação das competências com maior importância atribuída; a apresentação das ideias fundamentais sobre as competências que cada um dos entrevistados destacou na entrevista; e a prioritização das 10 competências que foram consideradas como mais importantes para a função Auditoria de SI

4.3.1 As Entrevistas Semi-Estruturadas

O propósito desta secção é enquadrar o processo de realização das entrevistas. As entrevistas efectuadas consideram-se como sendo semi-estruturadas dado que foram baseadas na estrutura do modelo MICASI. Este serviu de guia para a análise/discussão com o entrevistado sobre as competências que este considera como mais importantes para a função Auditoria de SI. Neste contexto, a entrevista semi-estruturada não é uma entrevista livre sobre determinado tema, sendo os comentários dos entrevistados obtidos sempre dentro dos limites definidos.

Neste caso, os limites encontram-se definidos pela estrutura do Modelo MICASI, nomeadamente as descrições das Competências de Gestão e as descrições das Competências Técnicas (complementadas por um instrumento de validação que são as proposições do Modelo Funcional).

No entanto, não se pode afirmar que se tratam de entrevistas totalmente estruturadas (no sentido de entrevistas fechadas) pois para além de terem como referência o modelo MICASI, não existe uma listagem de questões pré-definidas e comuns para serem utilizadas na discussão dos resultados com cada um dos entrevistados.

A figura seguinte resume as ideias apresentadas anteriormente, traduzindo o modo como as entrevistas foram estruturadas.

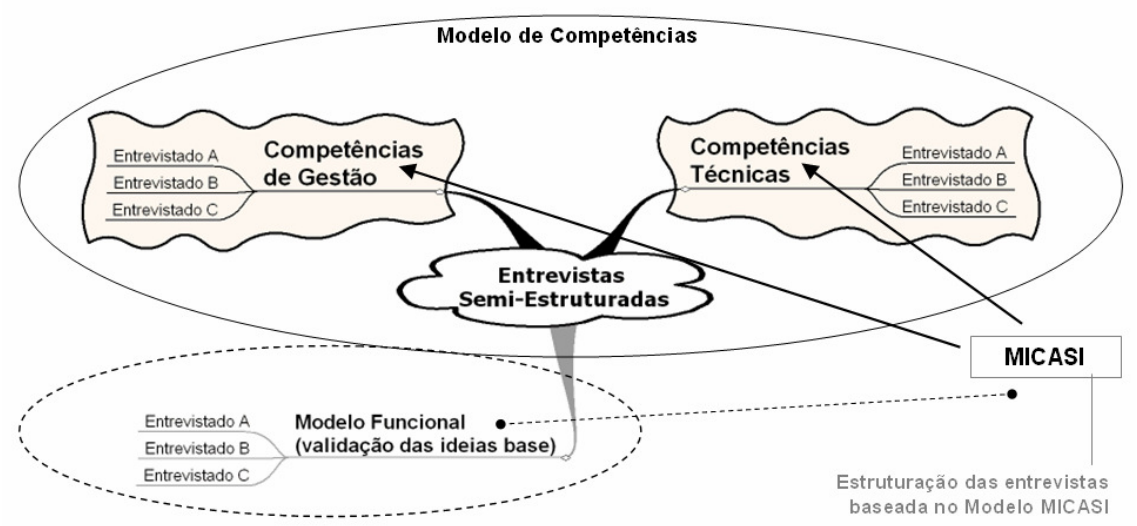


Figura 4.8 - Estruturação das Entrevistas

Fonte: Elaborado pelo autor

Na interpretação da figura, é relevante distinguir os seguintes elementos:

- Modelo conceptual estruturador da entrevista → Modelo MICASI (Competências de Gestão e Competências Técnicas), complementado por um instrumento que não faz parte integrante do Modelo de Competências mas que permite a validação das ideias base da tese (Modelo Funcional).
- Ferramentas de suporte às entrevistas → Ferramenta de suporte ao MICASI (grelhas/folhas de preenchimento e gráficos de análise).
- Ferramenta de análise das entrevistas → Ferramenta *Mind Manager* (mapas conceptuais que estruturam as ideias discutidas na entrevista).

De acordo com as boas práticas deste tipo de investigação, foram efectuados registos sistematizados das três entrevistas realizadas e dos respectivos resultados obtidos, para cada uma das vertentes de análise (Competências de Gestão, Competências Técnicas e Modelo Funcional). Estes registos podem ser encontrados nos anexos abaixo indicados.

- **Anexo 3: Detalhe dos Resultados das Entrevistas** → Contém três grelhas/folhas com o detalhe de todas as classificações efectuadas por cada um dos entrevistados (ver exemplo na figura abaixo).

			A		B		C		Média	
	COMPETÊNCIAS DE GESTÃO (*Soft Skills*)									
Nº	Competências	Descrição	Pontuação	Destaques	Pontuação	Destaques	Pontuação	Destaques	Pontuação	Destaques
CG.01	Aprendizagem Contínua	Competência para desenvolver responsabilidade pessoal e acção para aprender e implementar novas ideias, métodos, tecnologias, etc.	5	# 1	5	# 2	5		5	# 2
CG.02	Atingimento de Objectivos	Competência para definir, perseguir e alcançar objectivos atingíveis, independentemente dos obstáculos ou das circunstâncias.	3		3		5	# 4	4	# 4
CG.03	Auto Gestão	Competência para prioritizar e completar tarefas para disponibilizar resultados desejáveis em períodos de tempo predefinidos.	3		3		4		3	
CG.04	Auto Motivação	Competência para encetar e manter de forma sustentada o ímpeto/motivação sem estímulos externos.	5	# 4	3		4		4	# 4
CG.05	Capacidade de Decisão	Competência para analisar todos os aspectos de uma situação para obter uma visão completa que permita tomar a decisão.	4		5	# 1	5	# 2	5	# 2
CG.06	Capacidade de Influência	Competência para afectar as acções, as decisões, as opiniões ou as ideias dos outros.	4		4		5	# 1	4	# 1
CG.07	Capacidades Interpessoais	Competência para interagir com os outros de um modo positivo.	4		4		4		4	
CG.08	Desenvolvimento dos Outros	Competência de contribuir para o crescimento e desenvolvimento dos outros								

Figura 4.9 - Representação do Detalhe dos Resultados das Entrevistas

Fonte: Elaborado pelo autor

- **Anexo 4: Análise dos Resultados das Entrevistas** → Contém um conjunto de três mapas conceptuais (ver exemplo na figura abaixo) que foram elaborados com um duplo propósito:
  - Resumir as ideias discutidas durante a entrevista.
  - Suportar o exercício de análise qualitativa.

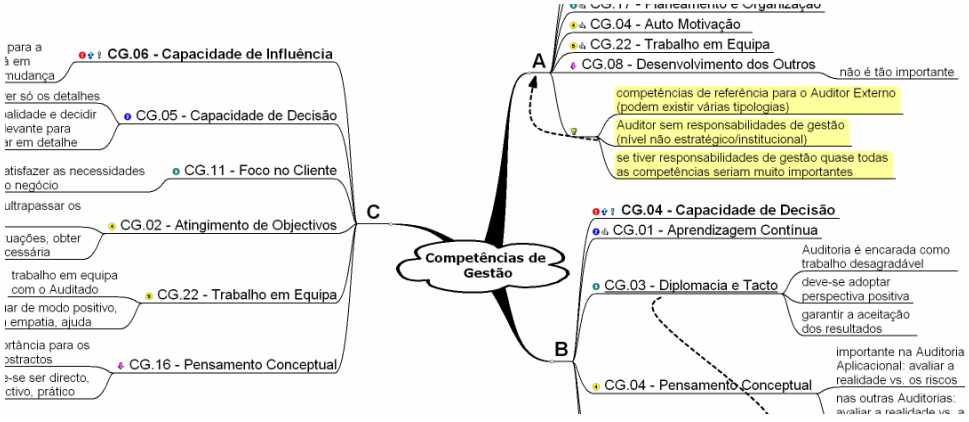


Figura 4.10 - Representação da Análise dos Resultados das Entrevistas

Fonte: Elaborado pelo autor

Para entrevistados, seleccionaram-se três profissionais responsáveis por Auditoria de SI, com uma experiência muito significativa na área e com percursos académicos e profissionais distintos, permitindo assim obter diferentes visões. Os entrevistados, doravante designados pela respectiva letra que os identificam, são:

ENTREVISTADO	NOME	ÁREA PROFISSIONAL	TIPO DE AUDITORIA DE SI
Entrevistado A	Prof. Doutor Alberto Carneiro	Universidade Autónoma de Lisboa - Professor no Departamento de Ciências e Tecnologias	visão de ensino/académica e visão de profissional Auditor de SI externo
Entrevistado B	Dr. Rui Gomes	KPMG – *Partner IT Advisory*	visão de profissional Auditor de SI externo
Entrevistado C	Dr. Paulo Gomes	Sonae SGPS – Director de Auditoria de SI	visão de profissional Auditor de SI interno

Tabela 4.1 - Identificação dos Entrevistados

Fonte: Elaborado pelo autor

O processo de entrevistas iniciou-se no princípio do 2º semestre de 2007, com o primeiro contacto por e-mail a cada um dos três entrevistados, contendo uma breve contextualização do tema da tese. Posteriormente, enviou-se a ferramenta de suporte ao modelo MICASI para os entrevistados procederem à classificação das competências, através da utilização das funcionalidades de "Pontuação" e "Destaques" que a ferramenta possui. Enviou-se igualmente um índice dos conteúdos da tese (índice de capítulos, lista de tabelas e lista de figuras) para uma contextualização mais pormenorizada do trabalho em curso. As grelhas/folhas da ferramenta foram preenchidas pelos entrevistados previamente à realização da entrevista, de modo a que o autor/entrevistador a pudesse preparar convenientemente com uma pré-análise dos resultados. Efectuou-se o tratamento dos dados e a análise gráfica dos resultados. Procedeu-se à identificação de questões específicas a colocar durante a entrevista, em função das classificações atribuídas pelos entrevistados para cada uma das competências em análise. As entrevistas foram realizadas presencialmente, com excepção do entrevistado A em que foi recebido um conjunto de comentários através de e-mail. Os esclarecimentos/comentários dos entrevistados permitiram a validação das classificações atribuídas e constituíram a base para a elaboração dos mapas conceptuais que sistematizam e resumem as ideias discutidas durante a entrevista (estes mapas encontram-se no **Anexo 4**).

4.3.2 A Análise Qualitativa dos Resultados

A análise dos resultados será efectuada de acordo com o definido no capítulo introdutório deste trabalho de investigação (secções 1.1.1 – Vértices da Metodologia Utilizada e 1.1.2 – Vantagens e Limitações). Assim, a análise será de natureza qualitativa, incluindo-se nesta análise as tarefas de recolha e tratamento dos dados das entrevistas semi-estruturadas.

Antes de prosseguir, uma nota sobre a natureza da análise. A análise designa-se de qualitativa pois baseia-se na interpretação das classificações atribuídas pelos entrevistados, tendo estas sido obtidas através da utilização da ferramenta de suporte ao MICASI. Apesar desta ferramenta possuir uma funcionalidade de classificação que pode considerada de quantitativa ("Pontuação"), ela é apenas um meio para identificar quais as competências que cada um dos entrevistados considera como mais importantes para um Auditor de SI. Para além disso, a funcionalidade de "Destaques", também existente na ferramenta, é claramente uma forma de hierarquizar ideias. Assim, com base nestas pontuações e destaques será efectuada uma análise qualitativa das diferentes classificações atribuídas pelos entrevistados. Daqui espera-se verificar a existência de diferentes visões sobre o perfil do Auditor de SI.

A leitura das seguintes análises deverá ser acompanhada da consulta do **Anexo 3** e **Anexo 4**.

Começar-se-á por apresentar as principais conclusões sobre a validação das ideias base do Modelo Funcional. Recorde-se que esta validação de ideias tinha por objectivo alinhar as classificações atribuídas pelos entrevistados com os conceitos e as ideias defendidas para a função Auditoria de SI ao longo deste trabalho de investigação.

Os entrevistados atribuem, em média, uma importância máxima e um destaque elevado às seguintes três proposições que definem, a alto nível, a função de Auditoria de SI:

- [MF.08] A Auditoria e a Gestão dos Riscos são instrumentos de Governo das Sociedades.
- [MF.03] A Auditoria de SI tem por missão avaliar e potenciar a melhoria contínua dos níveis de controlo dos SI e a adequada gestão dos seus riscos por parte da organização.
- [MF.02] Três dos principais factores caracterizadores do paradigma actual da função são:
  - Visão holística da Auditoria, ao definir um carácter multi-dimensional quanto ao seu âmbito (visão COSO);
  - Auditoria baseada no risco (de passiva, reactiva e baseada em controlos, passou para activa, proactiva e baseada em riscos);
  - Auditoria contribui para a implementação de soluções de melhoria contínua (no sentido de melhorias preventivas e não apenas soluções correctivas).

É relevante salientar que os três entrevistados também atribuíram, em média, elevada importância à proposição [MF.13] relativa à comparação dos três referenciais (CobiT, ITIL e ISO 17799), embora esta não tenha sido merecedora de nenhum destaque específico durante a entrevista no contexto do Modelo Funcional.

Apresenta-se de seguida uma análise às ideias fundamentais sobre o Modelo Funcional que cada um dos entrevistados fez questão de realçar na entrevista:

- Entrevistado **A** → Considera que muitas das proposições referem-se em específico apenas à Auditoria de SI, mas algumas são referentes e aplicáveis à função Auditoria em geral (não SI).
- Entrevistado **B** → De acordo com a lógica da proposição [MF.05], considera que a Auditoria de SI deve ser encarada como uma actividade de aconselhamento (*advisory*), cuja missão fundamental deverá ser trazer valor à organização, através da gestão dos riscos e da melhoria contínua [MF.01]. No entanto, constata-se que o principal motivo da Auditoria continua a ser a conformidade. O entrevistado atribui ainda destaque à independência da função [MF.07], defendo que a forma como uma função é avaliada (performance, atingimento de objectivos, etc.) é que determina a sua importância e a sua independência na organização.
- Entrevistado **C** → Considera que o maior valor da Auditoria de SI está em influenciar a mudança para resolver os problemas [MF.04]. Para o conseguir, a Auditoria de SI deverá alavancar a relação existente com a Gestão/Administração das organizações [MF.08].

De um modo global, constatou-se que não foram manifestadas discordâncias relevantes pelos entrevistados quanto à validação das ideias base do Modelo Funcional (a média da pontuação nunca é inferior a 3 em 5), tendo-se verificado um alinhamento geral com as ideias defendidas neste trabalho de investigação.

Relativamente às Competências de Gestão, o gráfico seguinte apresenta a análise das classificações (média dos 3 entrevistados).

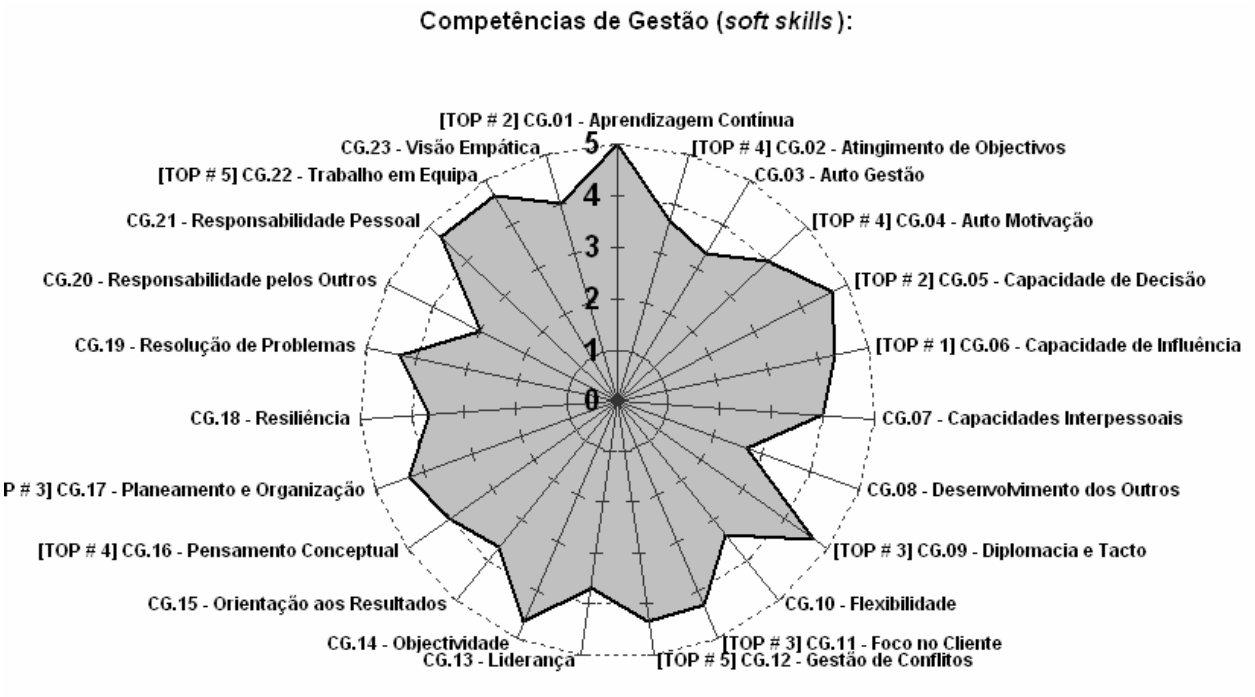


Figura 4.11 - Análise Gráfica de Resultados: Competências de Gestão

Fonte: Elaborado pelo autor

Da análise do gráfico, conclui-se que as duas competências com maior importância atribuída e, simultaneamente, com maior destaque atribuído pelo conjunto dos três entrevistados são a aprendizagem contínua [CG.01] e a capacidade de decisão [CG.05]. Existem outras competências que são igualmente consideradas de maior importância pelos três entrevistados, embora com destaque inferior ou sem destaque: a diplomacia e tacto [CG.09], a objectividade [CG.14], a responsabilidade pessoal [CG.21] e o trabalho em equipa [CG.22].

Salienta-se o facto do entrevistado **C** ter atribuído o máximo destaque à capacidade de influência [CG.06] que não foi destacada pelos restantes (embora tenha sido altamente pontuada). Trata-se de um resultado interessante pois, nas posições mais conservadoras sobre o papel do Auditor, a capacidade de influenciar o Auditado é habitualmente encarada como indesejável uma vez que poderia colocar em causa a independência do Auditor. Não obstante, conclui-se que uma das competências directamente relacionadas com a independência da função – a objectividade (no sentido de imparcialidade) [CG.14] – consta entre as competências classificadas como mais importantes pelos entrevistados, coexistido com a capacidade de influência [CG.06].

As ideias fundamentais sobre as Competências de Gestão que cada um dos entrevistados entendeu realçar na entrevista foram analisadas do seguinte modo:

- Entrevistado **A** → Considera que nem todas as competências que o modelo prevê devem ser encaradas como importantes ou muito importantes para um perfil de Auditor de SI sem responsabilidades de gestão (ou seja, nível não estratégico/institucional). Caso se considere um perfil de Auditor de SI com essas responsabilidades de gestão, então quase todas as competências previstas pelo modelo seriam muito importantes.
- Entrevistado **B** → Para além da capacidade de decisão [CG.05] que destaca em primeiro lugar, o entrevistado destaca a relação que se deve estabelecer entre a competência de diplomacia e tacto [CG.09] e a competência de gestão de conflitos [CG.12]. Neste contexto, o entrevistado considera que a Auditoria é, por natureza, encarada como uma actividade desagradável, pelo que o Auditor deverá diplomaticamente adoptar uma perspectiva positiva perante o Auditado e garantir que este aceita os resultados. Assim, o tacto do Auditor é fundamental para gerir possíveis situações de conflito.
- Entrevistado **C** → Adicionalmente à já referida capacidade de influência [CG.06] destacada em primeiro lugar pelo entrevistado, este também destaca a capacidade de decisão [CG.05] para explicitar que o Auditor de SI não se deve focar demasiado nos detalhes no trabalho de Auditoria. O Auditor de SI deverá possuir as competências que lhe permitam ter uma visão global sobre os pontos da Auditoria e a consequente capacidade de decidir quais são os pontos mais críticos ou relevantes que deverão ser aprofundados em detalhe.

Como resumo, na tabela seguinte apresenta-se uma prioritização das 10 Competências de Gestão que foram consideradas como mais importantes para a função Auditoria de SI (de entre as 23 que o modelo prevê). A tabela foi construída conjugando três factores de análise: a pontuação dada às competências mais importantes, os respectivos destaques atribuídos e as ideias fundamentais sobre as competências que foram referidas pelos entrevistados.

#01. Capacidade de Decisão	**#06.** Objectividade
#02. Aprendizagem Contínua	**#07.** Capacidade de Influência
#03. Diplomacia e Tacto	**#08.** Foco no Cliente
#04. Trabalho em Equipa	**#09.** Planeamento e Organização
#05. Responsabilidade Pessoal	**#10.** Atingimento de Objectivos

Tabela 4.2 - As 10 Competências de Gestão mais Importantes no Auditor de SI

Fonte: Elaborado pelo autor

O próximo gráfico representa as classificações (média dos 3 entrevistados) relativas aos 7 domínios de conhecimento previstos pelo modelo para as Competências Técnicas.

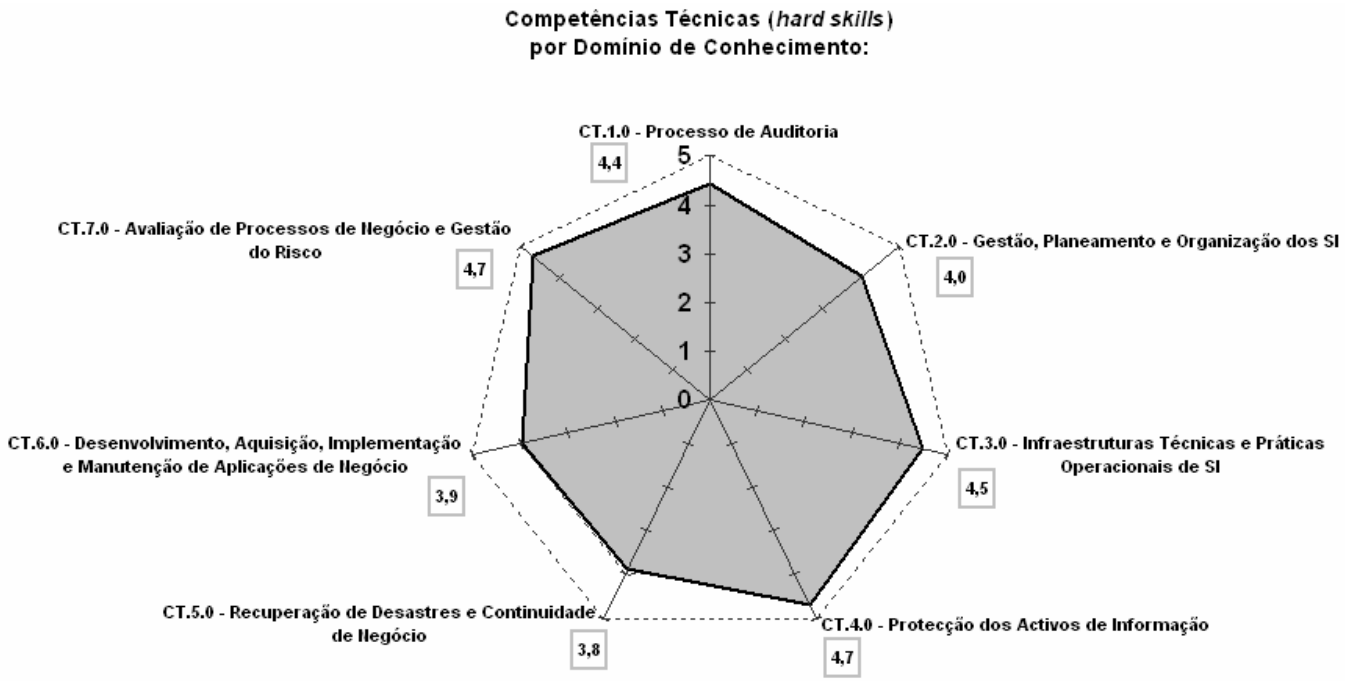


Figura 4.12 - Análise Gráfica de Resultados: Competências Técnicas por Domínio

Fonte: Elaborado pelo autor

Tendo apenas em conta as pontuações atribuídas (e não considerando os destaques individuais efectuados pelos entrevistados), consta-se que os domínios de conhecimento que, em média, são mais valorizados para os Auditores de SI são a protecção dos activos de informação [CT.4.0] e a avaliação de processos de negócio e gestão do risco [CT.7.0]. Esta classificação justifica-se pelo facto do primeiro ser composto na totalidade por 4 competências relacionadas com a segurança da informação e o segundo por estar relacionado com as auditorias aplicacionais. O domínio globalmente menos valorizado é o da recuperação de desastres e continuidade de negócio [CT.05], fundamentalmente pelo facto de uma das duas competências que o compõem – seguros [CT.5.2] – ter sido considerada como menos importante pelos entrevistados.

O gráfico seguinte apresenta as classificações (média dos 3 entrevistados) relativas a cada uma das Competências Técnicas.

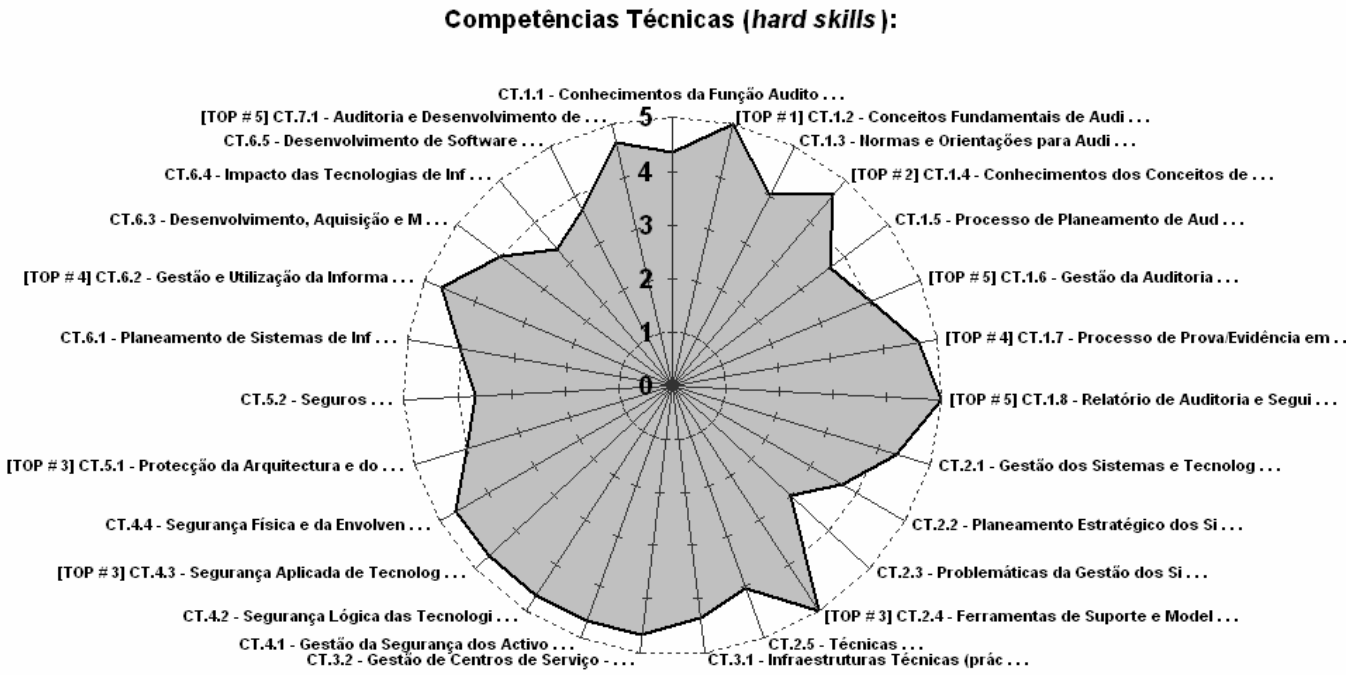


Figura 4.13 - Análise Gráfica de Resultados: Competências Técnicas

Fonte: Elaborado pelo autor

Efectuando a análise para cada uma das Competências Técnicas individualmente, as conclusões são ligeiramente diferentes da análise por domínio de conhecimento. Assim, as três competências com maior importância atribuída e, simultaneamente, com destaque relevante atribuído pelo conjunto dos entrevistados são os "conceitos fundamentais de Auditoria" [CT.1.2], os "conceitos de controlo interno" [CT.1.4] e os "modelos estruturados (ex: CobiT, ITIL, ISO 17799)" [CT.2.4]. Como se constata, os dois domínios de conhecimentos onde estas competências se inserem não foram globalmente apuradas como sendo dos mais importantes, apesar destas três competências serem individualmente as mais importantes.

A análise às ideias fundamentais sobre as Competências Técnicas que cada um dos entrevistados salientou na entrevista é a seguinte:

- Entrevistado **A** → Considera que se pode concordar muito com determinada competência mas esta pode não ser importante em determinada situação (coerência entre "concordância" e " importância"). Neste contexto, a importância das competências depende também do nível do Auditor de SI que se considerar (exemplo: depende do Auditor ter ou não responsabilidades de gestão).
- Entrevistado **B** → Sobressai o facto das três primeiras competências destacadas por este entrevistado coincidirem com as já referidas três primeiras que foram apuradas no conjunto dos entrevistados. O entrevistado defende que a maior ou menor importância das Competências Técnicas nos diversos domínios de conhecimento em análise depende do tipo de Auditoria de SI a realizar. Por exemplo, para uma Auditoria aos controlos gerais de SI é importante a competência relativa aos "modelos estruturados (ex: CobiT, ITIL, ISO 17799)" [CT.2.4]. Já para uma Auditoria à segurança, é relevante o domínio da "protecção dos activos de informação" [CT.4.0]. Para uma Auditoria às aplicações de negócio, torna-se fundamental o domínio "Auditoria controlos aplicacionais" [CT.7.1].
- Entrevistado **C** → Neste caso, as duas primeiras competências destacadas coincidem com o resultado do conjunto dos entrevistados. O seu terceiro destaque vai para uma competência que mais nenhum entrevistado assinalou: o "Planeamento da recuperação de desastres" [CT.5.1]. O entrevistado também atribui grande ênfase ao domínio do "Desenvolvimento de aplicações de negócio" [CT.6.0] porque considera-o bastante específico e de natureza diferente dos restantes domínios (está muito relacionado com o tipo de negócio) Assim, a maior ou menor importância das competências deste ou doutro domínio depende do tipo de negócio, da organização, dos produtos, das preocupações com a informação, etc. Este

entrevistado considera que existem 4 grandes tendências em termos de Competências Técnicas que o Auditor de SI deverá dominar:

- 1ª - Aplicações de negócio
- 2ª - Segurança (confidencialidade)
- 3ª - Continuidade de negócio (recuperação de desastres)
- 4ª - Governo dos SI (*IT Governance*)

À semelhança do efectuado anteriormente para as Competências de Gestão, e seguindo os mesmos factores de análise, apresenta-se na tabela seguinte um resumo com a prioritização das 10 Competências Técnicas que foram consideradas como mais importantes para a função Auditoria de SI (de entre as 27 que o modelo prevê).

#01. "Conceitos Fundamentais de Auditoria"	**#06.** "Processo de Evidência em Auditoria"
#02. "Conceitos de Controlo Interno"	**#07.** "Relatório de Auditoria e Seguimento/Acompanhamento"
#03. "Modelos Estruturados (ex: CobiT, ITIL, ISO 17799)"	**#08.** "Auditoria a Controlos Aplicacionais"
#04. "Segurança Aplicada de Tecnologias de Informação"	**#09.** "Gestão de Centros de Serviço"
#05. "Gestão e Utilização da Informação"	**#10.** "Planeamento de Recuperação de Desastres"

Tabela 4.3 - As 10 Competências Técnicas mais Importantes no Auditor de SI

Fonte: Elaborado pelo autor

Como conclusão, na tabela podem-se identificar três grandes agrupamentos correspondentes às Competências Técnicas que deverão ser mais importantes para um Auditor de SI:

- 1º - Conhecimentos de Auditoria → Correspondem maioritariamente às competências do domínio "Processo de Auditoria" [CT.1.0].
- 2º - Conhecimentos de referenciais de SI → Correspondem à competência "modelos estruturados (ex: CobiT, ITIL, ISO 17799)" [CT.2.4].
- 3º - Conhecimentos específicos da área/processo/sistema auditado → São variáveis de acordo com as restantes Competências Técnicas.

§ § §

Encerra-se este capítulo, que pretende ser um complemento, constatando que as competências classificadas como mais importantes são coerentes com os três principais determinantes do Desempenho do Auditor (Capacidade, Experiência e Conhecimento - ver secção 4.1.2) e também com as quatro áreas de conhecimento identificadas (Capacidades Interpessoais, Conhecimentos Gerais de Gestão, Conhecimentos de Auditoria e Conhecimentos de SI - ver secção 4.1.3).

Assim, por um lado, verifica-se que a Capacidade do próprio Auditor é predominantemente determinada pelas suas Competências de Gestão. De facto, as 10 Competências de Gestão identificadas como mais importantes estão associadas aos mecanismos de gestão do próprio indivíduo (exemplos: Capacidades Interpessoais - Diplomacia e Tacto, Capacidade de Influência, etc.) e aos conhecimentos gerais que o indivíduo possui que são relevantes para as suas actividades profissionais (exemplos: Conhecimentos Gerais de Gestão - Planeamento e Organização, Foco no Cliente, etc.). Por outro lado, verifica-se que a Experiência profissional do Auditor e o Conhecimento especializado que ele possui são predominantemente determinados pelas suas Competências Técnicas. De facto, as 10 Competências Técnicas identificadas como mais importantes estão associadas ao processo de Auditoria (exemplo: Conhecimentos de Auditoria - "Conceitos Fundamentais de Auditoria") e aos conhecimentos que o indivíduo possui sobre SI (exemplo: Conhecimentos de SI - "Segurança Aplicada de Tecnologias de Informação"). Estas conclusões não invalidam naturalmente a existência de Competências Técnicas que sejam determinantes da Capacidade do indivíduo ou a existência de Competências de Gestão que sejam determinantes da sua Experiência e Conhecimento profissionais.

Consta-se igualmente um alinhamento com as ideias defendidas ao longo deste trabalho de investigação, nomeadamente no Modelo Funcional. Assim, entre as competências que foram identificadas como mais importantes, encontram-se algumas que foram merecedoras de grande relevo no Modelo Funcional. Destas, destaca-se o facto do Auditor de SI dever possuir competências semelhantes às das Gestão de Projectos (exemplos: Competências de Gestão - Trabalho em Equipa, Atingimento de Objectivos, etc.) e possuir conhecimentos de referenciais de SI (exemplo: Competências Técnicas - "Modelos Estruturados CobiT, ITIL, ISO 17799").

5 CONCLUSÕES E DESENVOLVIMENTOS FUTUROS

O último capítulo tem como propósito apresentar, de forma sistematizada, as principais conclusões deste trabalho relativas ao Modelo Funcional e de Competências da Auditoria de SI. Adicionalmente, são sugeridas linhas de investigação futura, algumas das quais resultam de aspectos identificados ao longo do trabalho e que o autor considera merecedores de desenvolvimento mais aprofundado.

5.1 O MODELO FUNCIONAL DE AUDITORIA DE SI

O Modelo Funcional é um conjunto de ideias estruturadas e sequenciadas sobre a função Auditoria de SI. Este modelo integra as diversas dimensões que compõem a Auditoria de SI. Resultou do somatório de vários contributos, sendo uns originais (propostos pelo autor) e outros adaptados (a partir das referências utilizadas na revisão bibliográfica).

Neste contexto, apresenta-se de seguida um conjunto de proposições que resumem as principais conclusões obtidas sobre as diversas dimensões que, em conjunto, constituem um modelo para a função Auditoria de SI (o papel, a missão/objectivos, a organização, o âmbito, os referenciais metodológicos, os processos da função, etc.).

- O papel do Auditor tem evoluído e de forma positiva ao longo de 4 Eras. Partindo de um Auditor preocupado com "o passado" (Era da Inspecção), passou-se para um Auditor preocupado com "o presente" (Era do Controlo), agora preocupado com "o futuro" (Era do Risco) e, cada vez mais, preocupado de "forma permanente" (Era da Auditoria Contínua).
- Três dos principais factores caracterizadores do paradigma actual da função são:
  - Visão holística da Auditoria, ao definir um carácter multi-dimensional quanto ao seu âmbito (visão COSO);
  - Auditoria baseada no risco (de passiva, reactiva e baseada em controlos, passou para activa, proactiva e baseada em riscos);
  - Auditoria contribui para a implementação de soluções de melhoria contínua (no sentido de melhorias preventivas e não apenas soluções correctivas).

- A Auditoria de SI tem por missão avaliar e potenciar a melhoria contínua dos níveis de controlo dos SI e a adequada gestão dos seus riscos por parte da organização.
- O verdadeiro valor acrescentado da função surge quando os problemas (findings) são resolvidos, sendo o relatório de Auditoria apenas um meio para atingir um fim que é a melhoria do estado dos controlos dos SI da organização.
- O desempenho de actividades secundárias pelo Auditor de SI (exemplo: consultoria interna) é um importante contributo para promover uma cultura de controlo na organização e é um modo de aumentar o conhecimento especializado e prático em SI pelo Auditor.
- A Auditoria de SI é uma função especializada que deve estar inserida num departamento de Auditoria e Gestão de Risco, coexistindo com a função de Auditoria de Processos de Negócio (função semelhante mas mais abrangente e generalista) e com a função de Gestão de Risco (função complementar pois ajuda os Gestores de SI a identificar e a gerir os seus riscos).
- Para garantir independência, o departamento de Auditoria e Gestão de Risco deverá reportar ao Comité de Auditoria e Gestão de Risco e, por via deste, ao CEO (*Chief Executive Officer*) no âmbito das suas responsabilidades de supervisão.
- A Auditoria e a Gestão dos Riscos são instrumentos de Governo das Sociedades (*Corporate Governance*).
- A gestão dos recursos associados à Informação, tais como os SI e as TIC, deve ser encarada como um processo de negócio. Em consequência, os processos de SI devem ser alvo de Auditoria, à semelhança dos restantes processos de negócio.
- São três os principais factores da equação que determina o universo da Auditoria de SI: os Processos de Negócio (entre os quais os de Gestão dos SI); os Recursos de SI (incluindo pessoas, aplicações, tecnologias, etc.); e a Informação (critérios de confidencialidade, integridade, disponibilidade, etc.).
- Devem fazer parte do âmbito da Auditoria de SI todos os níveis de controlo de SI: controlos de Governo, de Gestão e Técnicos.
- É importante não executar a Auditoria de SI de um modo *ad-hoc*, mas sim adoptar e adaptar um ou uma combinação de referenciais metodológicos (exemplos: CobiT; ITIL, ISO 17799) que mais se adequem e que sejam úteis para o trabalho do Auditor.
- O CobiT é o referencial que possui mais actividades directamente relacionadas e específicas para Auditoria de SI. O ITIL é, dos 3 referenciais, o menos direccionado para as actividades de Auditoria de SI, enquanto que o ISO 17799 está mais vocacionado para actividades de Auditoria de SI relacionadas com a conformidade da segurança da informação.

- O planeamento anual da Auditoria de SI deve ser elaborado a partir de uma prioritização de Auditorias a efectuar. Estas são determinadas com base nos contributos (*inputs*) da Gestão de Risco (riscos críticos com impacto nos SI) e com base num conhecimento do planeamento estratégico e operacional dos SI (alinhamento com o negócio).
- É desejável a integração de metodologias entre diferentes tipos de Auditorias Internas, pelo que as fases sequenciais que constituem uma Auditoria de SI não são muito diferentes das fases de outros tipos de Auditoria Interna que também se baseiam numa abordagem ao risco (exemplo: Auditoria de Processos de Negócio).
- Cada Auditoria de SI pode ser gerida como se tratasse de uma Gestão de Projecto, com as inerentes técnicas de gestão de cada um dos parâmetros que definem e estruturam uma Auditoria (objectivos, âmbito, tempo, recursos, comunicação, qualidade, riscos, produtos resultantes, etc.).

5.2 O MODELO DE COMPETÊNCIAS DE AUDITORIA DE SI

O Modelo de Competências é o conjunto das competências que o Auditor de SI deve possuir, agrupadas em dois grandes tipos: as Competências de Gestão e as Competências Técnicas. Este modelo, proposto pelo autor, foi designado de "MICASI - Modelo de Identificação de Competências do Auditor de SI". A sua construção resultou da combinação e adaptação de dois referenciais distintos. As Competências de Gestão basearam-se num modelo de competências de Gestão de Projectos (*SSQ - Soft Skills Quantification for Project Manager Competencies*) e as Competências Técnicas basearam-se no modelo curricular da ISACA (*Model Curriculum for IS Audit and Control*).

Apresenta-se de seguida um conjunto de pontos que resumem as principais conclusões obtidas sobre o estudo das competências do Auditor de SI. Alguns destes pontos também ajudam a contextualizar a necessidade da construção de um Modelo de Competências, bem como a sua estruturação e caracterização.

- Dado que não foi identificado nenhum Modelo de Competências abrangente, aplicado à realidade da Auditoria de SI, justifica-se a necessidade de construção de um que identifique as competências de forma adequada, devidamente arrumadas e classificadas.
- Grande parte das competências desejáveis no contexto da Auditoria em geral são também aplicáveis especificamente aos Auditores de SI.
- A Equipa de Auditoria de SI deverá dominar, no seu conjunto, a área de conhecimento em Auditoria de SI, estando o conhecimento distribuído pelas diversas competências que cada Auditor de SI que constitui essa equipa possui.
- O ambiente de execução da Auditoria é também um determinante relevante das competências dos Auditores de SI. São três os elementos que o constituem: a Auditoria (as metodologias), os SI (os alvos da Auditoria) e o Negócio (o contexto no qual se executa a Auditoria).
- As competências do Auditor para conhecer o negócio e para se relacionar com a restante organização são essenciais para não se colocar em risco o próprio processo de Auditoria.
- A Experiência profissional do Auditor e a sua Capacidade individual determinam o seu Conhecimento que, por sua vez, determina o Desempenho em contexto de Auditoria. Para além disso, o Desempenho é também directamente determinado pela Capacidade do indivíduo.
- A área de conhecimento em Auditoria de SI diz respeito ao conjunto dos conhecimentos necessários ao adequado desempenho da função. E constituída pela intersecção de várias áreas de conhecimento: Capacidades Interpessoais, Conhecimentos Gerais de Gestão, Conhecimentos de Auditoria e Conhecimentos de SI.
- As Capacidades Interpessoais e os Conhecimentos Gerais de Gestão aproximam-se mais das Competências de Gestão. Os Conhecimentos de Auditoria e os Conhecimentos de SI aproximam-se mais das Competências Técnicas.
- As Competências de Gestão são as inerentes aos mecanismos de gestão do próprio indivíduo e aos conhecimentos gerais que o indivíduo possui que são relevantes para a sua profissão.
- As Competências Técnicas são as competências relacionadas com o processo de Auditoria de SI e com os conhecimentos que o indivíduo possui neste domínio.
- É indispensável a combinação de Competências de Gestão e Técnicas, podendo o nível variar consoante o grau de especialização do Auditor de SI.

- A dimensão da organização onde o Auditor de SI se encontra inserido, a variedade dos SI e TIC e ainda o tipo de negócio poderão justificar a especialização ou, pelo contrário, a diversificação de conhecimentos em Auditoria de SI.
- Quanto mais especializado for o Auditor de SI em determinados SI ou TIC, mais críticas se tornam as Competências Técnicas. Quanto menos especializado for o Auditor, mais necessárias se tornam as Competências de Gestão.
- O desafio de transformar conceitos técnicos de SI em informação de gestão útil para a restante organização só é atingível utilizando as Competências de Gestão.
- Um modelo misto de áreas de conhecimento, tanto em Auditoria, como em SI, são essenciais para formar um corpo de Competências Técnicas adequado.

O trabalho de investigação foi concluído com a aplicação prática do modelo MICASI. Para tal, efectuaram-se entrevistas a profissionais de Auditoria de SI com o objectivo de classificarem quais as competências mais importantes para um Auditor de SI, tendo por base as competências previstas no modelo MICASI. As principais conclusões foram as seguintes:

- As três Competências de Gestão consideradas como mais importantes são: a aprendizagem contínua, a capacidade de decisão e diplomacia e tacto.
- As três Competências Técnicas consideradas como mais importantes são: os "conceitos fundamentais de Auditoria", os "conceitos de controlo interno" e os "modelos estruturados (ex: CobiT, ITIL, ISO 17799)".
- Do conjunto das Competências de Gestão, identificou-se uma pouco usual no perfil habitualmente desejável do Auditor de SI: a capacidade de influência.
- Do conjunto das Competências Técnicas, identificaram-se dois domínios de conhecimento que são mais valorizados nos Auditores de SI: a "protecção dos activos de informação" e a "avaliação de processos de negócio e gestão do risco".
- Do conjunto das Competências Técnicas, identificaram-se três grandes agrupamentos de competências obrigatórias nos Auditores de SI: 1º - Conhecimentos de Auditoria; 2º - Conhecimentos de referenciais de SI; 3º - Conhecimentos específicos da área/processo/sistema auditado.

5.3 AS LINHAS DE INVESTIGAÇÃO FUTURA

Para o final deste texto, deixa-se um conjunto de linhas de investigação futura que são fruto da reflexão do autor efectuada durante e no final do trabalho. As sugestões de desenvolvimentos futuros estão agrupadas em três blocos de ideias que se apresentam de seguida.

→ **Modelo Funcional**:

- Centrar a investigação na Auditoria de SI externa, dado que este trabalho focou-se essencialmente em Auditoria de SI interna. A maior parte dos conceitos tratados são aplicados tanto a uma como outra, no entanto poderão existir alguns com diferenças merecedoras de estudo (exemplos: independência, organização, planeamento, etc.).
- Adaptar os conceitos desenvolvidos no contexto da Auditoria de SI para o contexto do Controlo Interno de SI. Embora se tratem de actividades com diferentes papéis na organização, têm processos comuns e possuem também um denominador comum que é o conceito de controlo. A justificar esta ideia está o facto da mais relevante associação de profissionais de Auditoria de SI ser também de profissionais de Controlo Interno de SI (*Information Systems Audit and Control Association*) e o facto das suas normas de Auditoria de SI serem também normas de Controlo Interno de SI (*IS Standards, Guidelines and Procedures for Auditing and Control Professionals*).
- Alargar o estudo para incluir outros referenciais de SI que sejam também aplicáveis às actividades de Auditoria de SI, para além dos estudados (CobiT, ITIL e ISO 17799). Por outro lado, actualizar o estudo dos referenciais de SI recorrendo a versões mais recentes face às utilizadas neste trabalho. Esta sugestão torna-se mais pertinente dado que o período de conclusão deste trabalho coincidiu com o lançamento da versão 3 do ITIL e com a passagem da ISO 17799 para ISO 27002.
- Autonomizar o estudo do Planeamento de Auditoria de SI, enquanto plano anual de Auditorias de SI (em alinhamento com o planeamento estratégico do negócio e dos SI) e consequente definição do planeamento das Auditorias de SI individuais (em alinhamento com o planeamento dos restantes tipos de Auditorias da organização). O estudo deste processo pode ser relevante ao ponto de merecer uma autonomização, à semelhança do que acontece com o estudo do Planeamento de SI dentro dos diversos domínios que constituem o estudo dos SI.

→ **Modelo de Competências**:

- Explorar mais aprofundadamente a relação entre Conhecimento e Competências. Esta linha de investigação justifica-se pois durante o trabalho sobressaiu a importância do Conhecimento, aquando do estudo dos determinantes do desempenho do Auditor (secção 4.1.2). Para além disso, as competências do Auditor de SI foram estruturadas em quatro áreas de conhecimento que, cada uma delas por si só, poderão ser merecedoras de maior desenvolvimento no contexto dos SI (Capacidades Interpessoais, Conhecimentos Gerais de Gestão, Conhecimentos de Auditoria e Conhecimentos de SI).
- Desdobrar o modelo MICASI em diversos sub-modelos de competências, variando o nível de conhecimentos exigíveis ao Auditor de SI consoante o seu nível de maturidade/experiência em Auditoria de SI (exemplos: Auditor Júnior de SI, Auditor Sénior de SI, Gestor de Auditoria de SI, Director de Auditoria de SI, etc.).
- Alargar a amostra de entrevistas a realizar com base no modelo MICASI, de modo a consolidar os resultados obtidos nesta primeira aplicação do modelo. Permitiria igualmente obter e combinar mais visões sobre as competências do Auditor de SI, para além das já apresentadas (visão de Auditor de SI interno, visão de Auditor de SI externo, visão académica/ensino de Auditoria de SI).
- Utilizar o modelo MICASI noutras situações em contexto de trabalho de investigação ou em contexto empresarial. Estas possíveis aplicações estão indicadas na secção relativa à aplicabilidade do modelo (secção 4.2.3).

→ **Integração do Modelo Funcional e de Competências**:

- Articular o modelo defendido para a função Auditoria de SI com as competências previstas para o Auditor de SI. Numa primeira etapa, este estudo poderia verificar a coerência dos diversos processos de gestão operacional da função Auditoria de SI (secções 3.5.2 a 3.5.5) com as diversas áreas de conhecimento exigíveis ao Auditor de SI (secção 4.1.3) e com as diversas Competências de Gestão e Competências Técnicas (secções 4.1.4, 4.2.1 e 4.3.2.). Numa segunda etapa, o estudo poderia ser alargado para os processos de gestão estratégica da função Auditoria de SI, ou seja, verificar a coerência daquelas competências com os objectivos, a organização, o âmbito, os referenciais e o planeamento da função (secções 3.1 a 3.5.1).
- Estender os conceitos analisados no contexto da Auditoria de SI para o contexto de outros tipos de Auditorias, integrando quer o modelo da função, quer as competências do Auditor. A

Auditoria de SI desenvolveu-se a partir de outros tipos de Auditorias mais generalistas como a Auditoria Interna pelo que continua a basear-se nos principais fundamentos desta. Assim, seria interessante validar a aplicabilidade dos conceitos defendidos, por exemplo, à Auditoria de Processos de Negócio. A alegação desta linha de investigação fica reforçada com a opinião segundo a qual é desejável a integração de metodologias entre diferentes tipos de Auditorias Internas (secção 2.4.1).

- Elaborar uma Metodologia de Auditoria de SI, contendo os processos de execução da Auditoria e as respectivas competências necessárias. A utilização sistemática dum documento de Definição de Auditoria, bem como dos respectivos conteúdos que foram descritos e discutidos sob a forma de técnicas de Gestão de Auditorias de SI (secção 3.5.5), poderá ser um ponto de partida para o desenvolvimento de uma metodologia formal e detalhada para cada uma das fases que constituem uma Auditoria de SI. Esta metodologia poderia estar articulada com as inerentes competências, necessárias consoante as fases e o tipo de actividades, nomeadamente com as Competências de Gestão e Competências Técnicas que foram identificadas como mais importantes para o Auditor de SI (secção 4.3.2).
- Elaborar uma Política de Auditoria de SI de modo a enquadrar a metodologia atrás sugerida. A metodologia constituiria uma visão Táctica-Operacional de como executar e gerir as diversas fases de uma Auditoria de SI, com as respectivas competências adequadas. A referida metodologia deveria estar enquadrada e articulada com uma visão mais Política-Estratégica para a função Auditoria de SI, o que constituiria a Política de Auditoria de SI. Dado que o tema do presente trabalho é a "Auditoria de SI: Modelo Funcional e de Competências", este seria um bom ponto de partida a partir do qual se podem derivar os dois documentos: a Política de Auditoria de SI (conceptualmente situada acima) e a Metodologia de SI (conceptualmente situada abaixo).

§ § §

Apesar dos desenvolvimentos futuros sugeridos e dos possíveis caminhos ainda para percorrer com base nas conclusões obtidas, espera-se que este trabalho de investigação tenha contribuído para aumentar o conhecimento da função e potenciar a excelência profissional nas áreas dos SI e da Auditoria em geral e, em particular, na Auditoria de SI.

Referências Bibliográficas

Amaral, L. e Varajão, J., *Planeamento de Sistemas de Informação*, FCA, Lisboa, Portugal, 2000.

APQC - American Productivity & Quality Center and AA - Arthur Andersen, *Process Classification Framework*, in www.apqc.org, 1996.

Asthon, B., "A View of International IT Security Standards", *The EDP Audit, Control and Security Newsletter* (29:6), December 2001.

Baskerville, R.L. and Myers, M. D., "Information Systems as a Reference Discipline", *MIS Quarterly* (26:1), March 2002.

Braga, A., "A Gestão da Informação", *Revista Millenium* (19), Instituto Superior Politécnico de Viseu, Junho 2000.

BSI - British Standards Institute, *BS ISO/IEC 17799:2005 - Information technology. Security techniques. Code of practice for information security management.*, British Standards Institute, London, UK, June 2005.

BSI - British Standards Institute Brasil, *BSI Brasil - Raising Standards Everywhere*, in www.bsibrasil.com.br, Março 2006.

Cangemi, M.P., *Managing the Audit Function: A Corporate Audit Department Procedure*, John Wiley & Sons, New York, USA, 2003.

Carneiro, A., *Auditoria de Sistemas de Informação*, FCA, Lisboa, Portugal, 2004.

Carvalho, J.A., "Information System? Which One Do You Mean?", in Falkenberg, E., K. Lyytinen and A. Verrijn-Stuart (Eds.), *Information Systems Concepts: An Integrated Discipline Emerging*, Kluwer Academic Publishers, 2000.

Carvalho, J.A., *Using the Viable System Model to Describe the Role of Computer-Based Systems in Organization*, Universidade do Minho - Escola de Engenharia, Guimarães, Portugal, 1998.

Davis, C., Schillerand, M. and Wheeler, M., *IT Auditing - Using Controls to Protect Information Assets*, McGraw-Hill, New York, USA, 2007.

Dhillon, G., *Principles of Information Systems Security: Texts and Cases*, John Wiley & Sons, New York, USA, 2006.

Díaz, M. C. M. y Vera, I. A, "Orígenes y classificación de la auditoria de la información", *Acimed* (14:5), 2006.

Fretwell, P.Z., *The Changing Role of the Internal Auditor*, Protiviti - Independent Risk Consulting, in www.knowledgeleader.com, August 2004.

Gallegos, F., "IT Audit Career Development Plan", *Information Systems Control Journal* (2), 2003.

Geada, F., "Auditoria: Fundamentação Histórica da Profissão", *Auditoria Interna*, Instituto Português de Auditoria Interna, Outubro/Novembro 2005.

IIA - The Institute of Internal Auditors, *Certified Internal Auditor Exam Content*, in www.theiia.org, 2007a.

IIA - The Institute of Internal Auditors, *Code of Ethics*, The Institute of Internal Auditors, Florida, USA, June 2000.

IIA - The Institute of Internal Auditors, *GTAG - Global Technology Audit Guide: Information Technology Controls*, The Institute of Internal Auditors, Florida, USA, 2005a.

IIA - The Institute of Internal Auditors, *GTAG - Global Technology Audit Guide: Continuous Auditing - Implications for Assurance, Monitoring, and Risk Assessment*, The Institute of Internal Auditors, Florida, USA, 2005b.

IIA - The Institute of Internal Auditors, *GTAG - Global Technology Audit Guide: Management of IT Auditing*, The Institute of Internal Auditors, Florida, USA, 2006.

IIA - The Institute of Internal Auditors, *The Audit Committee: A Holistic View of Risk*, in www.theiia.org, 2007b.

IIA - The Institute of Internal Auditors, *The GAIT Methodology: A risk-based approach to assessing the scope of IT General Controls*, in www.theiia.org, 2007c.

IIA - The Institute of Internal Auditors, *The Role of Internal Auditing in Enterprise-wide Risk Management,*, The Institute of Internal Auditors, Florida, USA, September 2004.

ISACA - Information Systems Audit and Control Association, *CISA Job Practice Areas*, in www.isaca.org, 2006.

ISACA - Information Systems Audit and Control Association, *Glossary of Terms*, in www.isaca.org, 2007.

ISACA - Information Systems Audit and Control Association, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, Information Systems Audit and Control Association, Illinois, USA, September 2005.

ISACA - Information Systems Audit and Control Association, *ISACA Model Curriculum for IS Audit and Control*, Information Systems Audit and Control Association, Illinois, USA, 2004.

ISCJ - Information Systems Control Journal editors, "What Recruiters and Staffing Agencies Say about Trends in IS Auditing", Editors compendium of readers contributions, *Information Systems Control Journal* (5), 2000.

ITGI - IT Governance Institute, *CobiT - Control Objectives for Information and related Technology*, *3rd Edition*, IT Governance Institute, Illinois, USA, 2000.

ITGI - IT Governance Institute, *CobiT Mapping*, in www.itgi.org, 2004.

ITGI - IT Governance Institute and OGC - Office of Government Commerce, *Aligning CobiT, ITIL and ISO 17799 for Business Benefit*, in www.itgi.org and www.ogc.gov.uk, 2005.

Jacka, J. M., "I Am the Very Model of a Modern Audit Manager", *Internal Auditor*, The Institute of Internal Auditors, February 2006.

Kaplan, B. and Duchon, D., "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study", *MIS Quarterly* (2:4), December 1998.

Karapetrovic, S. and Willborn, W., "Audit System: concepts and practices", *Total Quality Management* (12:1), January 2001.

LeBlanc, K., "The Big Picture: ITIL as an Integrated Framework", ITIL & ITSM Knowledge Base, in www.itilworx.com, August 2004.

Libby, R. and Luft, J., "Determinants of judgment performance in accounting settings: Ability, knowledge, motivation, and environment", *Accounting, Organizations and Society* (18:5), 1993.

Marchand, D.A., *Competing with Information: A Manager's Guide to Creating Business Value with Information Content*, John Wiley & Sons, New York, USA, 2000.

McNamee, D. and Selim, G.M., *Risk Management: Changing the Internal Auditor's Paradigm*, The Institute of Internal Auditors Research Foundation, Florida, USA, 1998.

Moody, D.L., *Building Links between IS Research and the Professional Practice: Improving the Relevance and Impact of IS Research*, University of Melbourne and Simsion Bowles & Associates, Australia, 2000.

Muzio, E., Fisher, D. J., Thomas, E. R. and Peters, V., "Soft Skills Quantification (SSQ) for Project Manager Competencies", *Project Management Journal* (38:2), June 2007.

Nascimento, J.C., *A Virtualização da Gestão de Sistemas de Informação: Impactos na sua Organização e nos seus Recursos Humanos*, Tese de Doutoramento, Universidade do Minho - Escola de Engenharia, Guimarães, Portugal, 2002.

OGC - Office of Government Commerce, *An Introduction to ITIL*, in www.ogc.gov.uk, 2004.

Oliveira, A., "A importância dos Sistemas de Informação para a indústria", *Revista Estudos de Gestão* (4:3), 1998/9.

Oliveira, A., "Concepção e Implementação de Sistemas de Informação e Apoio à Gestão e ao Negócio", *Galileu - Revista de Economia e Direito* (2:2), 1997.

PMI - Project Management Institute, *PMBOK Guide - A Guide to the Project Management Body of Knowledge* , *3rd Edition*, Project Management Institute, Pennsylvania, USA, 2004.

Porto Editora, *Dicionário da Língua Portuguesa 2008*, in www.portoeditora.pt, Maio 2007.

Power, D. and Terziovski, M., "The process, practice and outcomes of non-financial auditing: five Australian case studies", *Int. J. Manufacturing Technology and Management* (7:1), 2005.

Prakarsa, S., *IS Auditing in 21st Century*, MSBA Research Project, Pomona California State Polytechnic University, California, USA, 1996.

Sadowski, G.P., *The Skills Needed by Sucessful Entry Level Auditors in the next Millennium*, MSBA Research Project, Pomona California State Polytechnic University, California, USA, 1997.

Santos, C., Vasconcelos, A., e Tribolet, J., "Da Framework CEO à Auditoria de Sistemas de Informação", *Actas da V Conferência da Associação Portuguesa de Sistemas de Informação*, Lisboa, Portugal, Novembro 2004.

Sayana, S. A., "The IS Audit Process", *Information Systems Control Journal* (1), 2002.

Shapiro, C., and Varian, H. R., *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business Scholl Press, Massachusetts, USA, 1999.

Silva, P.G., *Análise da Aplicação Informática AutoAudit*, Relatório de Tecnologias dos Sistemas de Informação, MBI - Master on Business Information, Universidade do Minho - Escola de Engenharia, Guimarães, Portugal, Fevereiro 2004a.

Silva, P.G., *Gestão de Projectos aplicada à Definição de Âmbito de Auditorias de Sistemas de Informação*, Relatório de Gestão de Projectos, MBI - Master on Business Information, Universidade do Minho - Escola de Engenharia, Guimarães, Portugal, Março 2004b.

Spafford, G., "The Benefits of Standard IT Governance Frameworks", IT Process Institute, in www.itpi.org, April 1998.

Touquet, M.D., *Best Practices of IS Audit Management*, MSBA Research Project, Pomona California State Polytechnic University, California, USA, 1996.

Anexos

Anexo 1: Actividades de Auditoria de SI previstas no CobiT, ITIL e ISO 17799

Este Anexo faz parte integrante da secção "3.4.3 - As Actividades de Auditoria de SI previstas nos Referenciais", na qual se descreve a metodologia de análise utilizada na produção dos resultados abaixo.

LEGENDA INTERPRETATIVA :	
xxx	Actividades indirectamente aplicáveis à Auditoria de SI previstas em um ou mais dos 3 referenciais
xxx	Actividades directamente relacionadas com Auditoria de SI previstas em um ou mais dos 3 referenciais
xxx	Actividades específicas de Auditoria de SI ou de Gestão de Risco de SI previstas no referencial CobiT

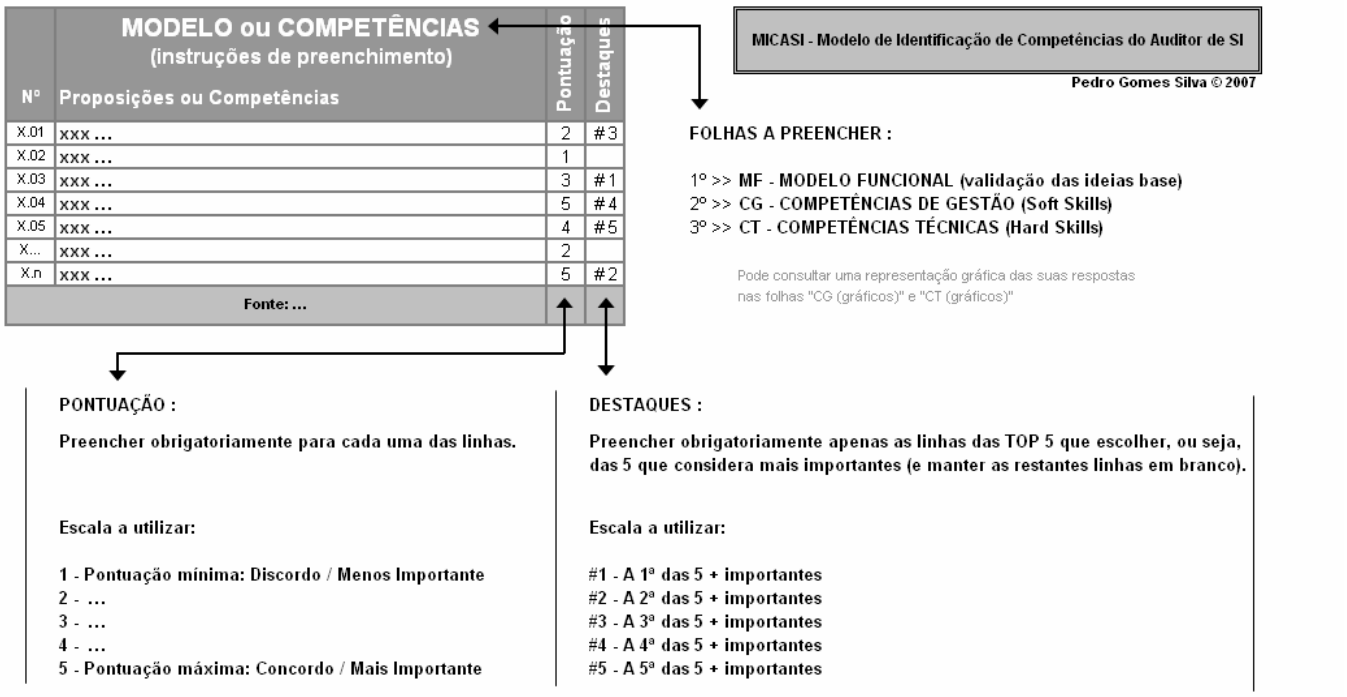
CobiT			ITIL			ISO 17799	
Level 1	Level 2	Level 3	Level 1	Level 2	Level 3	Level 1	Level 2
PO - Plan and Organise	PO1 - Define a Strategic IT Plan	PO1.7 - Monitoring and evaluating of IT Plans	Planning to Implement Service Management	How Do We Keep the Momentum Going	7.4 - Ongoing monitoring and process reviews	-	-
	PO4 - Define the IT Organisation and Relationships	PO4.6 - Responsability for logical and physical security	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
	PO6 - Communicate Management Aims and Direction	PO6.4 - Policy implementation resources	Security Management	Security Management Measures	4.3 - Audit and Evaluate	12 - Compliance	12.2 - Reviews of security policy and technical compliance
		PO6.5 - Maintenance of policies	-	-	-	12 - Compliance	12.2 - Reviews of security policy and technical compliance
		PO6.6 - Compliance with policies, procedures and standards	Security Management; Planning to Implement Service Management; Service Support; Service Delivery	Security Management Measures; How Do We Keep the Momentum Going; Change Management; Financial Management for IT Services	4.3 - Audit and Evaluate 7.4 - Ongoing monitoring and process reviews 8.7.1 - Auditing for compliance 5.7.11 - Auditing the systems	12 - Compliance	12.2 - Reviews of security policy and technical compliance
		PO6.8 - Security and internal control framework policy	-	-	-	12 - Compliance	12.2 - Reviews of security policy and technical compliance
		PO6.9 - Intellectual property rights	-	-	-	12 - Compliance	12.2 - Reviews of security policy and technical compliance
	PO8 - Ensure Compliance With External Requirements	PO8.1 - External requirements review	-	-	-	4 - Organizational Security 12 - Compliance	4.1 - Information security infrastructure 12.2 - Reviews of security policy and technical compliance 12.1 - Compliance with legal requirements
		PO8.2 - Practices and procedures for complying with external requirements	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		PO8.3 - Safety and ergonomic compliance	-	-	-	5 - Asset Classification and Control 7 - Physical and Environmental Security 8 - Communications and Operations Management	5.1 - Accountability for assets 7.1 - Secure areas 8.1 - Operational procedures and responsibilities
		PO8.4 - Privacy, intellectual property and data flow	-	-	-	8 - Communications and Operations Management 10 - Systems Development and Maintenance 12 - Compliance	8.7 - Exchanges of information and software 10.3 - Cryptographic controls 12.1 - Compliance with legal requirements
		PO8.5 - Electronic commerce	-	-	-	8 - Communications and Operations Management	8.7 - Exchanges of information and software
		PO8.6 - Compliance with insurance contracts	-	-	-	5 - Asset Classification and Control 7 - Physical and Environmental Security	5.1 - Accountability for assets 7.2 - Equipment security

CobiT			ITIL			ISO 17799	
Level 1	Level 2	Level 3	Level 1	Level 2	Level 3	Level 1	Level 2
	PO9 - Assess Risks	PO9.1 - Business Risk Assessment	ICT Infrastructure Management; Service Delivery	Annex 3B; Availability Management	3.B - Risk Management Plan 8.9.3 - Central Computer and Telecommunications Agency Risk Analysis and Management Method 7.3.2 - Requirements analysis and strategy definition	-	-
		PO9.2 - Risk Assessment Approach	ICT Infrastructure Management; Service Delivery	Annex 3B; Availability Management; IT Service Continuity Management	3.B - Risk Management Plan 8.9.3 - Central Computer and Telecommunications Agency Risk Analysis and Management Method 7.5 - Risk Assessment Model	3 - Security Policy 4 - Organizational Security	3.1 - Information security policy 4.1 - Information security infrastructure
		PO9.3 - Risk Identification	Service Delivery	Availability Management	8.9.3 - Central Computer and Telecommunications Agency Risk Analysis and Management Method	4 - Organizational Security 5 - Asset Classification and Control 7 - Physical and Environmental Security 9 - Access Control 10 - Systems Development and Maintenance	4.2 - Security of third-party acess 5.2 - Information classification 7.1 - Secure areas 7.2 - Equipment security 9.2 - User acess management 9.4 - Network access control 10.3 - Cryptographic controls
		PO9.4 - Risk Measurement	Service Delivery	Availability Management	8.9.3 - Central Computer and Telecommunications Agency Risk Analysis and Management Method	-	-
		PO9.5 - Risk Plan Action	Service Delivery	IT Service Continuity Management	7.3.2 - Risk reduction measures 7.3.3 - Implement risk reduction measures	10 - Systems Development and Maintenance	10.1 - Security requirements of systems
		PO9.6 - Risk Acceptance	The Business Perspective	Understanding the Business Viewpoint	5.1.1 - Business view on risk	-	-
		PO9.7 - Safeguard Selection	-	-	-	4 - Organizational Security	4.2 - Security of third-party acess
		PO9.8 - Risk Assessment Commitment	-	-	-	3 - Security Policy	3.1 - Information security policy
AI - Acquire and Implement	AI1 - Identify Automated Solutions	AI1.10 - Audit trails design	-	-	-	9 - Access Control 10 - Systems Development and Maintenance 12 - Compliance	9.7 - Monitor system access and use 10.2 - Security in application systems 12.1 - Compliance with legal requirements 12.3 - System audit considerations
	AI2 - Acquire and Maintain Application Software	AI2.12 - Controllability	Appplication Management	-	7. Control Methods and Techniques	4 - Organizational Security 9 - Access Control 10 - Systems Development and Maintenance	4.1 - Information security infrastructure 9.7 - Monitor system access and use 10.2 - Security in application systems
	AI3 - Acquire and Maintain Technology Infrastructure	AI3.7 - Use and monitoring of system utilities	ICT Infrastructure Management	Design and Planning; Operations	2.7.2 - The tools 4.4.1 - Management of all ICT infrastructure events	12 - Compliance	12.3 - System audit considerations
DS - Deliver and Support	DS5 - Ensure Systems Security	DS5.5 - Management review of user accounts	Security Management	Security Management Measures	4.3 - Audit and evaluate security reviews of IT systems	-	-
		DS5.7 - Security Surveillance	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		DS5.8 - Data Classification	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		DS5.10 - Violation and security activity reports	-	-	-	12 - Compliance	12.2 - Reviews of security policy and technical
		DS5.12 - Reacreditation	Security Management	Security Management Measures	4.3 - Audit and evaluate security reviews of IT	12 - Compliance	12.2 - Reviews of security policy and technical
	DS7 - Educate and Train Users	DS7.3 - Security principles and awareness training	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
	DS11 - Manage Data	DS11.5 - Source document retention	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		DS11.20 - Retention periods and storage terms	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		DS11.25 - Backup storage	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		DS11.26 - Archiving	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
		DS11.30 - Continued integrity of stored data	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements
	DS13 - Manage Operations	DS13.7 - Safeguard special forms and output devices	-	-	-	12 - Compliance	12.1 - Compliance with legal requirements

CobiT			ITIL			ISO 17799	
Level 1	Level 2	Level 3	Level 1	Level 2	Level 3	Level 1	Level 2
M - Monitor	M1 - Monitor the Processes	M1.1 - Collecting monitoring data benchmarks, proprietary nature and integrity of data	ICT Infrastructure Management; Service Delivery	Operations; Service Level Management	4.6.1 - The techniques (relevant performance indicators) 4.4.7 - Establish monitoring capabilities	12 - Compliance	12.1 - Compliance with legal requirements
		M1.2 - Assessing performance targets, continual assessment basis	ICT Infrastructure Management; The Business Perspective; Planning to Implement Service Management; Servifce Delivery	Operations; Business/IS alignment; How Do We Check our Milestones Have Been Reached; How Do We Keep the Momentum Going; Service Level Management	4.6.1 - The techniques (KPIs, CSFs) 4.5.2 - Benchmarking 6.1 - Critical sucess factors and key performance indicators 7.4 - Ongoing monitoring and process reviews 4.3.3 - Estabilish initial perception of the services	-	-
		M1.3 - Assessing customer satisfaction service shortfalls identified	Service Support; Service Delivery	The Service Desk; Service Level Management	4.4.8 - Customer satisfaction analysis and surveys 4.5.2 - Service review meetings	-	-
		M1.4 - Management reporting reports, risk mitigation	The Business Perspective; Service Delivery	Managing progress toward goals; Service Level Management	6.3 - Service reporting (status the provision of service) 4.4.9 - Define reporting and review procedures 4.5.1 - Monitoring and reporting	-	-
	M2 - Assess Internal Control Adequacy	M2.1 - Internal control monitoring	-	-	-	8 - Communications and Operations Management 12 - Compliance	8.1 - Operational procedures 8.5 - Network management 12.1 - Compliance with legal requirements
		M2.2 - Timely operation of internal controls	-	-	-	3 - Security Policy 4 - Organizational Security 6 - Personnel Security 8 - Communications and Operations Management	3.1 - Information security policy 4.1 - Information security infrastructure 6.3 - Responding to security incidents and malfunctions 8.1 - Operational procedures and responsabilities 8.5 - Network management
		M2.3 - Internal control level reporting	-	-	-	4 - Organizational Security 6 - Personnel Security 8 - Communications and Operations Management	4.1 - Information security infrastructure 6.3 - Responding to security incidents and malfunctions 8.1 - Operational procedures and responsabilities 8.4 - Housekeeping
		M2.4 - Operational security and internal control assurance	-	-	-	3 - Security Policy 4 - Organizational Security 6 - Personnel Security 8 - Communications and Operations Management 12 - Compliance	3.1 - Information security policy 4.1 - Information security infrastructure 6.3 - Responding to security incidents and malfunctions 8.1 - Operational procedures and responsabilities 8.4 - Housekeeping 12.2 - Reviews of security policy and technical compliance
	M3 - Obtain Independent Assurance	M3.1 - Independent security and internal control (certification / accreditation of IT services)	-	-	-	4 - Organizational Security 12 - Compliance	4.1 - Information security infrastructure 12.2 - Reviews of security policy and technical compliance 12.1 - Compliance with legal requirements
		M3.2 - Independent security and internal control (certification / accreditation of third-party providers)	-	-	-	-	-
		M3.3 - Independent effectiveness evaluation of IT services	-	-	-	-	-
		M3.5 - Independent assurance of compliance with laws and regulatory requirements and contractual commitments	-	-	-	4 - Organizational Security	4.1 - Information security infrastructure
		M3.6 - Independent assurance of compliance with laws and regulatory requirements and contractual commitments by third-party service providers	-	-	-	-	-
		M3.7 - Competence of independent assurance function	-	-	-	4 - Organizational Security 12 - Compliance	4.1 - Information security infrastructure 12.2 - Reviews of security policy and technical
		M3.8 - Proactive audit involvement	-	-	-	-	-
	M4 - Provide for Independent Audit	M4.1 - Audit Charter	-	-	-	12 - Compliance	12.3 - System audit considerations
		M4.2 - Independence	-	-	-	-	-
		M4.3 - Professional ethics and standards	-	-	-	-	-
		M4.4 - Competence	-	Includes: Technical competence, skills and knowledge		-	-
		M4.5 - Planning	-	-	-	-	-
		M4.6 - Performance of audit work	-	-	-	-	-
		M4.7 - Reporting	-	-	-	-	-
		M4.8 - Follow-up activities	-	-	-	-	-

Anexo 2: Modelo de Identificação de Competências do Auditor de SI (MICASI)

Este Anexo faz parte integrante da secção "4.2 - O Modelo de Identificação de Competências do Auditor de SI", na qual se apresenta o processo de construção do modelo e se descrevem as funcionalidades da ferramenta que suporta o modelo.



Nº	MODELO FUNCIONAL (validação das ideias base) Proposições	Pontuação	Destaques
MF.01	O papel do Auditor tem evoluído e de forma positiva ao longo de 4 Eras. Partindo de um Auditor preocupado com "o passado" (Era da Inspecção), passou-se para um Auditor preocupado com "o presente" (Era do Controlo), agora preocupado com "o futuro" (Era do Risco) e, cada vez mais, preocupado de "forma permanente" (Era da Auditoria Contínua).		
MF.02	Três dos principais factores caracterizadores do paradigma actual da função são: 1º - Visão holística da Auditoria, ao definir um carácter multi-dimensional quanto ao seu âmbito (visão COSO); 2º - Auditoria baseada no risco (de passiva, reactiva e baseada em controlos, passou para activa, proactiva e baseada em riscos); 3º - Auditoria contribui para a implementação de soluções de melhoria contínua (no sentido de melhorias preventivas e não apenas soluções correctivas).		
MF.03	A Auditoria de SI tem por missão avaliar e potenciar a melhoria contínua dos níveis de controlo dos SI e a adequada gestão dos seus riscos por parte da organização.		
MF.04	O verdadeiro valor acrescentado da função surge quando os problemas (*findings*) são resolvidos, sendo o relatório de Auditoria apenas um meio para atingir um fim que é a melhoria do estado dos controlos dos SI da organização.		
MF.05	O desempenho de actividades secundárias pelo Auditor de SI (exemplo: consultoria interna) é um importante contributo para promover uma cultura de controlo na organização e é um modo de aumentar o conhecimento especializado e prático em SI pelo Auditor.		
MF.06	A Auditoria de SI é uma função especializada que deve estar inserida num departamento de Auditoria e Gestão de Risco, coexistindo com a função de Auditoria de Processos de Negócio (função semelhante mas mais abrangente e generalista) e com a função de Gestão de Risco (função complementar pois ajuda os Gestores de SI a identificar e a gerir os seus riscos).		
MF.07	Para garantir independência, o departamento de Auditoria e Gestão de Risco deverá reportar ao Comité de Auditoria e Gestão de Risco e, por via deste, ao CEO (*Chief Executive Officer*) no âmbito das suas responsabilidades de supervisão.		
MF.08	A Auditoria e a Gestão dos Riscos são instrumentos de Governo das Sociedades (*Corporate Governance*).		
MF.09	A gestão dos recursos associados à Informação, tais como os SI e as TIC, deve ser encarada como um processo de negócio. Em consequência, os processos de SI devem ser alvo de Auditoria, à semelhança dos restantes processos de negócio.		
MF.10	São três os principais factores da equação que determina o universo da Auditoria de SI: os Processos de Negócio (entre os quais os de Gestão dos SI); os Recursos de SI (incluindo pessoas, aplicações, tecnologias, etc.); e a Informação (critérios de confidencialidade, integridade, disponibilidade, etc.).		
MF.11	Devem fazer parte do âmbito da Auditoria de SI todos os níveis de controlo de SI: controlos de Governo, de Gestão e Técnicos.		
MF.12	É importante não executar a Auditoria de SI de um modo *ad-hoc*, mas sim adoptar e adaptar um ou uma combinação de referenciais metodológicos (exemplos: CobiT; ITIL, ISO 17799) que mais se adequem e que sejam úteis para o trabalho do Auditor.		
MF.13	O CobiT é o referencial que possui mais actividades directamente relacionadas e específicas para Auditoria de SI. O ITIL é, dos 3 referenciais, o menos direccionado para as actividades de Auditoria de SI, enquanto que o ISO 17799 está mais vocacionado para actividades de Auditoria de SI relacionadas com a conformidade da segurança da informação.		
MF.14	O planeamento anual da Auditoria de SI deve ser elaborado a partir de uma prioritização de Auditorias a efectuar. Estas são determinadas com base nos contributos (*inputs*) da Gestão de Risco (riscos críticos com impacto nos SI) e com base num conhecimento do planeamento estratégico e operacional dos SI (alinhamento com o negócio).		
MF.15	É desejável a integração de metodologias entre diferentes tipos de Auditorias Internas, pelo que as fases sequênciais que constituem uma Auditoria de SI não são muito diferentes das fases de outros tipos de Auditoria Interna que também se baseam numa abordagem ao risco (exemplo: Auditoria de Processos de Negócio).		
MF.16	Cada Auditoria de SI pode ser gerida como se tratasse de uma Gestão de Projecto, com as inerentes técnicas de gestão de cada um dos parâmetros que definem e estruturam uma Auditoria (objectivos, âmbito, tempo, recursos, comunicação, qualidade, riscos, produtos resultantes, etc.).		
Fonte: Preposições elaboradas pelo Autor (originais ou compiladas a partir de diversas fontes indicadas na bibliografia)			

Nº	COMPETÊNCIAS DE GESTÃO (*Soft Skills*) Competências	Descrição	Pontuação	Destaques
CG.01	**Aprendizagem Contínua**	Competência para desenvolver responsabilidade pessoal e acção para aprender e implementar novas ideias, métodos, tecnologias, etc.		
CG.02	**Atingimento de Objectivos**	Competência para definir, perseguir e alcançar objectivos atingíveis, independentemente dos obstáculos ou das circunstâncias.		
CG.03	**Auto Gestão**	Competência para prioritizar e completar tarefas para disponibilizar resultados desejáveis em períodos de tempo predefinidos.		
CG.04	**Auto Motivação**	Competência para encentar e manter de forma sustentada o ímpeto/motivação sem estímulos externos.		
CG.05	**Capacidade de Decisão**	Competência para analisar todos os aspectos de uma situação para obter uma visão completa que permita tomar a decisão.		
CG.06	**Capacidade de Influência**	Competência para afectar as acções, as decisões, as opiniões ou as ideias dos outros.		
CG.07	**Capacidades Interpessoais**	Competência para interagir com os outros de um modo positivo.		
CG.08	**Desenvolvimento dos Outros**	Competência de contribuir para o crescimento e desenvolvimento dos outros.		
CG.09	**Diplomacia e Tacto**	Competência para tratar os outros com razoabilidade/justiça, independentemente de pontos de vista parciais ou pessoais.		
CG.10	**Flexibilidade**	Competência para prontamente modificar, responder e incorporar mudança com um mínimo de resistência pessoal.		
CG.11	**Foco no Cliente**	Competência para o compromisso de satisfazer as necessidades do cliente.		
CG.12	**Gestão de Conflitos**	Competência para conciliar diferentes pontos de vista de modo construtivo.		
CG.13	**Liderança**	Competência de organizar e motivar as pessoas para alcançar objectivos, criando uma lógica organizada e direccionada.		
CG.14	**Objectividade**	Competência de ter em atenção os diversos pontos de vista de forma imparcial.		
CG.15	**Orientação aos Resultados**	Competência para identificar as acções necessárias para completar tarefas e obter resultados.		
CG.16	**Pensamento Conceptual**	Competência para analisar situações hipotéticas ou conceitos abstractos para avistar resultados.		
CG.17	**Planeamento e Organização**	Competência para implementar um processo de actividades para sistematizar, procedimentar e produzir resultados.		
CG.18	**Resiliência**	Competência para recuperar rapidamente das adversidades.		
CG.19	**Resolução de Problemas**	Competência para identificar componentes chave de um problema para formular as soluções.		
CG.20	**Responsabilidade pelos Outros**	Competência de assumir responsabilidade pelas acções dos outros.		
CG.21	**Responsabilidade Pessoal**	Competência de responder pelas próprias acções.		
CG.22	**Trabalho em Equipa**	Competência para cooperar com outros para atingir objectivos.		
CG.23	**Visão Empática**	Competência para antever e compreender os pensamentos e as atitudes dos outros.		
Fonte: SSQ - *Soft Skills Quantification for Project Manager Competencies - Project Management Institute Journal* Adaptado e traduzido de (Muzio, Fisher, Thomas and Peters, 2007)				

Nº	COMPETÊNCIAS TÉCNICAS (*Hard Skills*) Competências	Tópicos	Pontuação	Destaques
CT.1.0	**Domínio de Conhecimento: Processo de Auditoria**			
CT.1.1	**Conhecimentos da Função Auditoria de SI**	Leis e regulamentos; Natureza e origem das auditoria (teoria da agência, seguros, etc.); Necessidade de controlo dos SI; Tipos de auditoria (externa, interna, de gestão, etc.); Responsabilidade e autoridade do Auditor (carta de auditoria, sub-contratação, etc.); Regulação da profissão de Auditor de SI (Código de Conduta, normas, etc.)		
CT.1.2	**Conceitos Fundamentais de Auditoria**	Materialidade; Prova/Evidência; Relevância; Independência; Risco; Fraude; Conformidade; etc.		
CT.1.3	**Normas e Orientações para Auditoria de SI**	Conhecimento dos Códigos de Ética Profissional (ex: ISACA); Normas e Orientações para Auditoria de SI; Técnicas e práticas de Auditoria de SI.		
CT.1.4	**Conhecimentos dos Conceitos de Controlo Interno**	Estrutura e indicadores de Governo dos SI; Objectivos de Controlo Interno; Classificação de Controlos (preventivos, detectivos, correctivos); Controlos Gerais (organização, segurança, desenvolvimento, documentação, etc.); Controlos Aplicacionais (entrada, processamento, saída, etc.); Estruturas de Controlo (ex: CobiT)		
CT.1.5	**Processo de Planeamento de Auditorias**	Planeamento estratégico e táctico de Auditorias; Carta de Auditoria; Métodos de avaliação de riscos; Técnicas de recolha de informação e avaliação de controlos; Plano, programa e âmbito da Auditoria; Cassificação e tipos de Auditorias (operacional, geral, aplicacional, física, lógica, etc.)		
CT.1.6	**Gestão da Auditoria**	Alocação e priorização de recursos; Avaliação da qualidade da Auditoria; Identificação de melhores prácticas; Planeamento da carreira; Desenvolvimento profissional; etc.		
CT.1.7	**Processo de Prova/Evidência em Auditoria**	Provas/evidências suficientes, relevantes e úteis; Técnicas de recolha de prova/evidência; Natureza e tipos de teste de conformidade vs. substantivos; Amostragem estatística e não estatística; Sistemas/aplicações de apoio à Auditoria; Regras sobre documentação; Materialidade das excepções/conclusões; Revisão do trabalho e alcance dos objectivos.		
CT.1.8	**Relatório de Auditoria e Seguimento/Acompanhamento**	Relatórios de Auditoria (forma, estrutura, conteúdos, linguagem, destinatários, etc.); Seguimento/acompanhamento da implementação das recomendações.		
CT.2.0	**Domínio de Conhecimento: Gestão, Planeamento e Organização dos SI**			
CT.2.1	**Gestão dos Sistemas e Tecnologias de Informação**	Gestão de Projectos de Tecnologias de Informação; Gestão do Risco (económico, tecnológico, etc.); Controlo de qualidade do software; Gestão das infraestruturas, das operações e do suporte das Tecnologias de Informação; Indicadores de desempenho das Tecnologias de Informação; Externalização de funções de Sistemas e Tecnologias de Informação.		
CT.2.2	**Planeamento Estratégico dos Sistemas e Tecnologias de Informação**	Estratégias competitiva e ligação com estratégia corporativa; SI Estratégicos; Tipos e classificações de SI; Segregação de funções; Formação em Sistemas e Tecnologias de Informação.		
CT.2.3	**Problemáticas da Gestão dos Sistemas e Tecnologias de Informação**	Aspectos legais; Propriedade intelectual; Aspectos éticos; Privacidade; Governo dos SI; Outras problemáticas actuais.		
CT.2.4	**Ferramentas de Suporte e Modelos Estruturados**	Utilização na Auditoria de ferramentas de suporte e modelos estruturados (ex: CobiT; ITIL, ISO17799, etc.)		
CT.2.5	**Técnicas**	Verificações ao controlo de alterações; Verificações operacionais; Revisões à gestão da qualidade.		
CT.3.0	**Domínio de Conhecimento: Infraestruturas Técnicas e Práticas Operacionais de SI**			
CT.3.1	**Infraestruturas Técnicas (prácticas de Planeamento, Implementação e Operação)**	Arquitectura das Tecnologias de Informação; Hardware; Software; Redes; Segurança; Controlos base; Ferramentas de monitorização do desempenho; Governo dos SI; Gestão dos recursos e das infraestruturas da Informação; Sistemas proprietários vs. abertos.		
CT.3.2	**Gestão de Centros de Serviço - manter a infraestrutura de sistemas e tecnologias de informação através de organizações dedicadas a estas actividades**	Gestão de Centros de Serviço e normas/orientação de operação (ex: CobiT; ITIL, ISO17799, etc.); Gestão da mudança (ex: novas implementações, alterações, ferramentas de controlo); Gestão da segurança; Gestão da configuração; Gestão de incidentes; Gestão da capacidade; Alocação de recursos; Gestão de sistemas distribuídos; Gestão de fornecedores; Gestão de clientes; Gestão de níveis de serviço; Gestão da contingência e da recuperação (ex: backups); Gestão de centros de atendimento; Gestão de redes; Gestão das operações da infraestrutura.		

CT.4.0	**Domínio de Conhecimento: Protecção dos Activos de Informação**			
CT.4.1	**Gestão da Segurança dos Activos de Informação**	Conceitos básicos de segurança das Tecnologias de Informação; Necessidade de segurança dos recursos de Informação; Políticas de segurança; Normas de segurança.		
CT.4.2	**Segurança Lógica das Tecnologias de Informação**	Componentes da segurança lógica das Tecnologias de Informação; Controlo de acessos lógicos; Procedimentos, ferramentas e software de controlo de acessos.		
CT.4.3	**Segurança Aplicada de Tecnologias de Informação - Recursos de Alta Tecnologia**	Segurança das comunicações e das redes (ex: cliente-servidor, serviços baseados na rede; firewalls, encriptação, etc.) Segurança dos centros de processamento de dados; Segurança das bases de dados; Segurança dos sistemas de desenvolvimento e dos processos de manutenção.		
CT.4.4	**Segurança Física e da Envolvente**	Conceitos de segurança física das Tecnologias de Informação; Controlo dos acessos físicos; Questões da envolvente.		
CT.5.0	**Domínio de Conhecimento: Recuperação de Desastres e Continuidade de Negócio**			
CT.5.1	**Protecção da Arquitectura e dos Activos das Tecnologias de Informação - Planeamento de Recuperação de Desastres**	Avaliação de impactos no negócio; Comprometimento e suporte por parte da Gestão; Documentação, preparação, aprovação e distribuição do plano de continuidade de negócio. Manutenção, formação, teste e verificação do plano de continuidade de negócio; O papel do auditor.		
CT.5.2	**Seguros**	Valoração dos activos (ex: equipamentos, sistemas, pessoas, etc.); Recursos que podem ser segurados; Tipos e descrição de seguros.		
CT.6.0	**Domínio de Conhecimento: Desenvolvimento, Aquisição, Implementação e Manutenção de Aplicações de Negócio**			
CT.6.1	**Planeamento de Sistemas de Informação**	Componentes da gestão dos SI (ex: processos de dados, tecnologias, organização, etc.); Entender as partes interessadas e as suas necessidades; Métodos de planeamento de SI (investigação de sistemas, oportunidades de integração e reengenharia de processos; avaliações de risco e de custo-benefício, análise de sistemas orientados a objectos, etc.); Integração com o software de planeamento de recursos da organização.		
CT.6.2	**Gestão e Utilização da Informação**	Monitorização de desempenho de níveis de serviço face aos acordados; Qualidade, disponibilidade, integridade, privacidade; Dados e informação; Análise, avaliação e desenho da arquitectura da Informação (ex: o papel das bases de dados e dos sistemas de gestão e armazenamento de dados); Arquitectura das aplicações (ex: modelação de SI; processos e soluções, etc.); Análise, avaliação e desenho de entidades, seus processos de negócio e modelos de negócio; Gestão da Informação (ex: administração de dados e de bases de dados, papeis e responsabilidades de administração, etc.); Tecnologias de bases de dados como ferramentas para o auditor; Estruturas de dados e linguagens de interrogação de dados.		
CT.6.3	**Desenvolvimento, Aquisição e Manutenção de Sistemas de Informação**	Gestão de Projectos de SI (ex: planeamento, organização, desenvolvimento, controlo, execução, etc.); Métodos para o ciclo de vida de desenvolvimento de software (fases e tarefas, análise, avaliação, desenho, etc.); Abordagens ao desenvolvimento de sistemas (ex: pacotes standard, prototipagem, reengenharia de processos, engenharia assistida por computador, etc.); Procedimentos de manutenção e de controlo de alterações em sistemas; Análise, avaliação e controlo dos riscos e das características dos projectos.		
CT.6.4	**Impacto das Tecnologias de Informação nos Processos e Soluções de Negócio**	Externalização de processos de negócio; Tendências e problemáticas de aplicações de comércio electrónico.		
CT.6.5	**Desenvolvimento de Software**	Segregação da especificação e da implementação na programação; Metologias para especificação de requisitos; Desenho de algoritmos; Tratamento de ficheiros; Indexação; Criação e manipulação de bases de dados; Bons princípios de desenho de ecrán e de relatórios.		
CT.7.0	**Domínio de Conhecimento: Avaliação de Processos de Negócio e Gestão do Risco**			
CT.7.1	**Auditoria e Desenvolvimento de Controlos Aplicacionais**	Procedimentos e controlos de entrada, processamento e saída; Documentação dos sistemas e aplicações; Rotinas de Auditoria.		
Fonte: *ISACA Model Curriculum for IS Audit and Control* **Adaptado e traduzido de (ISACA, 2004)**				

Anexo 3: Detalhe dos Resultados das Entrevistas

Este Anexo faz parte integrante das secções "4.3.1 - As Entrevistas Semi-Estruturadas" e "4.3.2 - A Análise Qualitativa dos Resultados".

		A		B		C		Média	
	MODELO FUNCIONAL (validação das ideias base)	Pontuação	Destaques	Pontuação	Destaques	Pontuação	Destaques	Pontuação	Destaques
Nº	Proposições								
MF.01	O papel do Auditor tem evoluído e de forma positiva ao longo de 4 Eras. Partindo de um Auditor preocupado com "o passado" (Era da Inspecção), passou-se para um Auditor preocupado com "o presente" (Era do Controlo), agora preocupado com "o futuro" (Era do Risco) e, cada vez mais, preocupado de "forma permanente" (Era da Auditoria Contínua).	4		3		4		4	
MF.02	Três dos principais factores caracterizadores do paradigma actual da função são: 1º - Visão holística da Auditoria, ao definir um carácter multi-dimensional quanto ao seu âmbito (visão COSO); 2º - Auditoria baseada no risco (de passiva, reactiva e baseada em controlos, passou para activa, proactiva e baseada em riscos); 3º - Auditoria contribui para a implementação de soluções de melhoria contínua (no sentido de melhorias preventivas e não apenas soluções correctivas).	5	# 1	5		5	# 3	5	# 2
MF.03	A Auditoria de SI tem por missão avaliar e potenciar a melhoria contínua dos níveis de controlo dos SI e a adequada gestão dos seus riscos por parte da organização.	4	# 3	5	# 1	5		5	# 2
MF.04	O verdadeiro valor acrescentado da função surge quando os problemas (*findings*) são resolvidos, sendo o relatório de Auditoria apenas um meio para atingir um fim que é a melhoria do estado dos controlos dos SI da organização.	2		3		5	# 2	3	# 2
MF.05	O desempenho de actividades secundárias pelo Auditor de SI (exemplo: consultoria interna) é um importante contributo para promover uma cultura de controlo na organização e é um modo de aumentar o conhecimento especializado e prático em SI pelo Auditor.	4		4	# 4	4		4	# 4
MF.06	A Auditoria de SI é uma função especializada que deve estar inserida num departamento de Auditoria e Gestão de Risco, coexistindo com a função de Auditoria de Processos de Negócio (função semelhante mas mais abrangente e generalista) e com a função de Gestão de Risco (função complementar pois ajuda os Gestores de SI a identificar e a gerir os seus riscos).	1		4		4		3	
MF.07	Para garantir independência, o departamento de Auditoria e Gestão de Risco deverá reportar ao Comité de Auditoria e Gestão de Risco e, por via deste, ao CEO (*Chief Executive Officer*) no âmbito das suas responsabilidades de supervisão.	1		5	# 3	4		3	# 3
MF.08	A Auditoria e a Gestão dos Riscos são instrumentos de Governo das Sociedades (*Corporate Governance*).	5	# 2	5		5	# 1	5	# 2
MF.09	A gestão dos recursos associados à Informação, tais como os SI e as TIC, deve ser encarada como um processo de negócio. Em consequência, os processos de SI devem ser alvo de Auditoria, à semelhança dos restantes processos de negócio.	3		4		5	# 4	4	# 4
MF.10	São três os principais factores da equação que determina o universo da Auditoria de SI: os Processos de Negócio (entre os quais os de Gestão dos SI); os Recursos de SI (incluindo pessoas, aplicações, tecnologias, etc.); e a Informação (critérios de confidencialidade, integridade, disponibilidade, etc.).	3		5	# 2	5	# 5	4	# 4
MF.11	Devem fazer parte do âmbito da Auditoria de SI todos os níveis de controlo de SI: controlos de Governo, de Gestão e Técnicos.	1		5		4		3	
MF.12	É importante não executar a Auditoria de SI de um modo *ad-hoc*, mas sim adoptar e adaptar um ou uma combinação de referenciais metodológicos (exemplos: CobiT; ITIL, ISO 17799) que mais se adequem e que sejam úteis para o trabalho do Auditor.	4	# 4	5	# 5	4		4	# 5
MF.13	O CobiT é o referencial que possui mais actividades directamente relacionadas e específicas para Auditoria de SI. O ITIL é, dos 3 referenciais, o menos direccionado para as actividades de Auditoria de SI, enquanto que o ISO 17799 está mais vocacionado para actividades de Auditoria de SI relacionadas com a conformidade da segurança da informação.	4		5		5		5	
MF.14	O planeamento anual da Auditoria de SI deve ser elaborado a partir de uma prioritização de Auditorias a efectuar. Estas são determinadas com base nos contributos (*inputs*) da Gestão de Risco (riscos críticos com impacto nos SI) e com base num conhecimento do planeamento estratégico e operacional dos SI (alinhamento com o negócio).	2		5		4		4	
MF.15	É desejável a integração de metodologias entre diferentes tipos de Auditorias Internas, pelo que as fases sequênciais que constituem uma Auditoria de SI não são muito diferentes das fases de outros tipos de Auditoria Interna que também se baseam numa abordagem ao risco (exemplo: Auditoria de Processos de Negócio).	4	# 5	4		4		4	# 5
MF.16	Cada Auditoria de SI pode ser gerida como se tratasse de uma Gestão de Projecto, com as inerentes técnicas de gestão de cada um dos parâmetros que definem e estruturam uma Auditoria (objectivos, âmbito, tempo, recursos, comunicação, qualidade, riscos, produtos resultantes, etc.).	4		3		5		4	
Fonte: Preposições elaboradas pelo Autor (originais ou compiladas a partir de diversas fontes indicadas na bibliografia)									

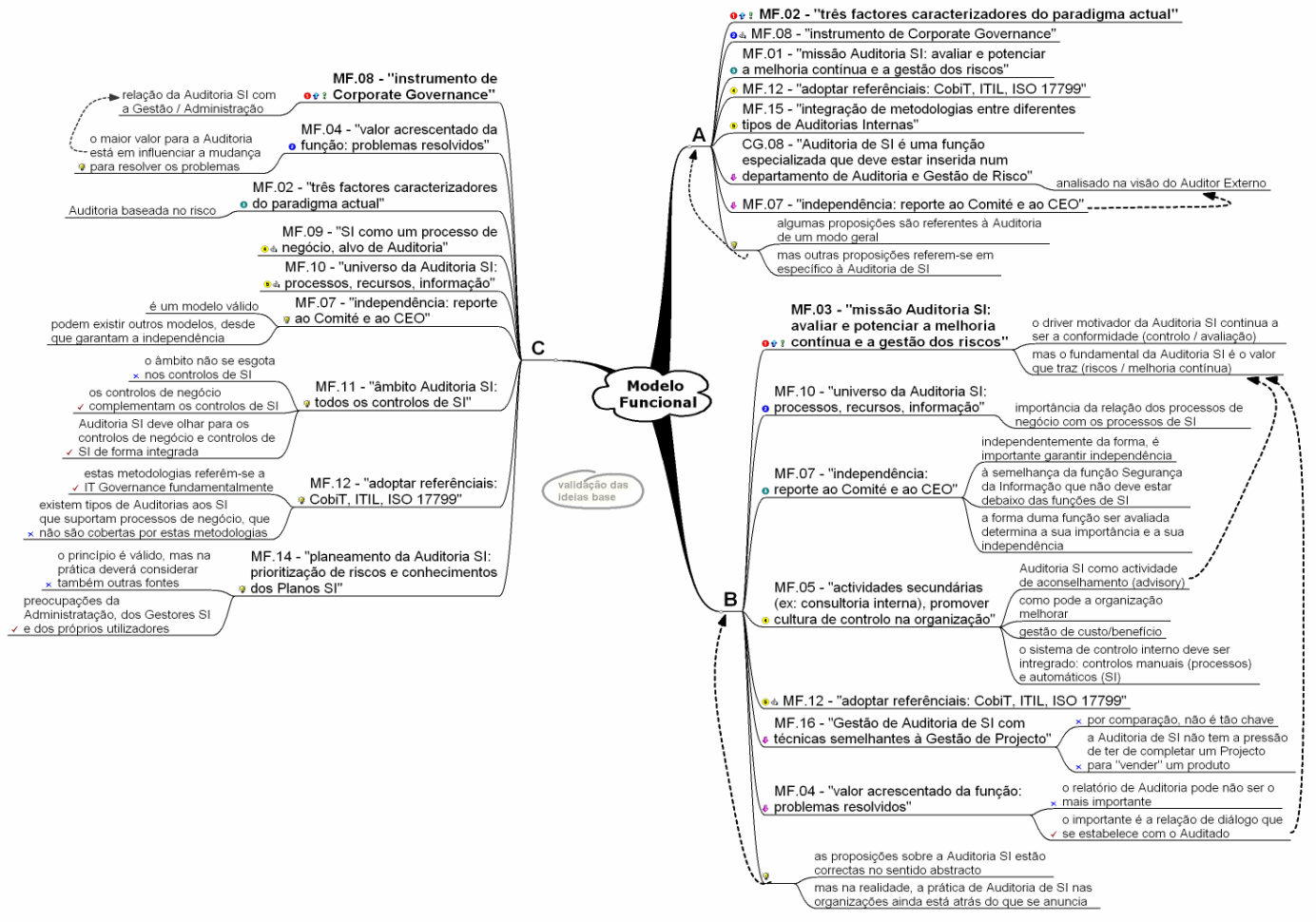
			A		B		C		Média	
	COMPETÊNCIAS DE GESTÃO (*Soft Skills*)									
Nº	**Competências**	**Descrição**	**Pontuação**	**Destaques**	**Pontuação**	**Destaques**	**Pontuação**	**Destaques**	**Pontuação**	**Destaques**
CG.01	**Aprendizagem Contínua**	Competência para desenvolver responsabilidade pessoal e acção para aprender e implementar novas ideias, métodos, tecnologias, etc.	5	# 1	5	# 2	5		5	# 2
CG.02	**Atingimento de Objectivos**	Competência para definir, perseguir e alcançar objectivos atingíveis, independentemente dos obstáculos ou das circunstâncias.	3		3		5	# 4	4	# 4
CG.03	**Auto Gestão**	Competência para prioritizar e completar tarefas para disponibilizar resultados desejáveis em períodos de tempo predefinidos.	3		3		4		3	
CG.04	**Auto Motivação**	Competência para encetar e manter de forma sustentada o ímpeto/motivação sem estímulos externos.	5	# 4	3		4		4	# 4
CG.05	**Capacidade de Decisão**	Competência para analisar todos os aspectos de uma situação para obter uma visão completa que permita tomar a decisão.	4		5	# 1	5	# 2	5	# 2
CG.06	**Capacidade de Influência**	Competência para afectar as acções, as decisões, as opiniões ou as ideias dos outros.	4		4		5	# 1	4	# 1
CG.07	**Capacidades Interpessoais**	Competência para interagir com os outros de um modo positivo.	4		4		4		4	
CG.08	**Desenvolvimento dos Outros**	Competência de contribuir para o crescimento e desenvolvimento dos outros.	2		3		3		3	
CG.09	**Diplomacia e Tacto**	Competência para tratar os outros com razoabilidade/justiça, independentemente de pontos de vista parciais ou pessoais.	5		5	# 3	4		5	# 3
CG.10	**Flexibilidade**	Competência para prontamente modificar, responder e incorporar mudança com um mínimo de resistência pessoal.	3		3		4		3	
CG.11	**Foco no Cliente**	Competência para o compromisso de satisfazer as necessidades do cliente.	5	# 2	3		5	# 3	4	# 3
CG.12	**Gestão de Conflitos**	Competência para conciliar diferentes pontos de vista de modo construtivo.	4		5	# 5	4		4	# 5
CG.13	**Liderança**	Competência de organizar e motivar as pessoas para alcançar objectivos, criando uma lógica organizada e direccionada.	3		3		5		4	
CG.14	**Objectividade**	Competência de ter em atenção os diversos pontos de vista de forma imparcial.	4		5		5		5	
CG.15	**Orientação aos Resultados**	Competência para identificar as acções necessárias para completar tarefas e obter resultados.	4		3		4		4	
CG.16	**Pensamento Conceptual**	Competência para analisar situações hipotéticas ou conceitos abstractos para avistar resultados.	4		5	# 4	3		4	# 4
CG.17	**Planeamento e Organização**	Competência para implementar um processo de actividades para sistematizar, procedimentar e produzir resultados.	5	# 3	4		4		4	# 3
CG.18	**Resiliência**	Competência para recuperar rapidamente das adversidades.	3		4		4		4	
CG.19	**Resolução de Problemas**	Competência para identificar componentes chave de um problema para formular as soluções.	4		4		5		4	
CG.20	**Responsabilidade pelos Outros**	Competência de assumir responsabilidade pelas acções dos outros.	3		2		4		3	
CG.21	**Responsabilidade Pessoal**	Competência de responder pelas próprias acções.	5		4		5		5	
CG.22	**Trabalho em Equipa**	Competência para cooperar com outros para atingir objectivos.	5	# 5	4		5	# 5	5	# 5
CG.23	**Visão Empática**	Competência para antever e compreender os pensamentos e as atitudes dos outros.	4		4		4		4	
Fonte: SSQ - *Soft Skills Quantification for Project Manager Competencies - Project Management Institute Journal* Adaptado e traduzido de (Muzio, Fisher, Thomas and Peters, 2007)										

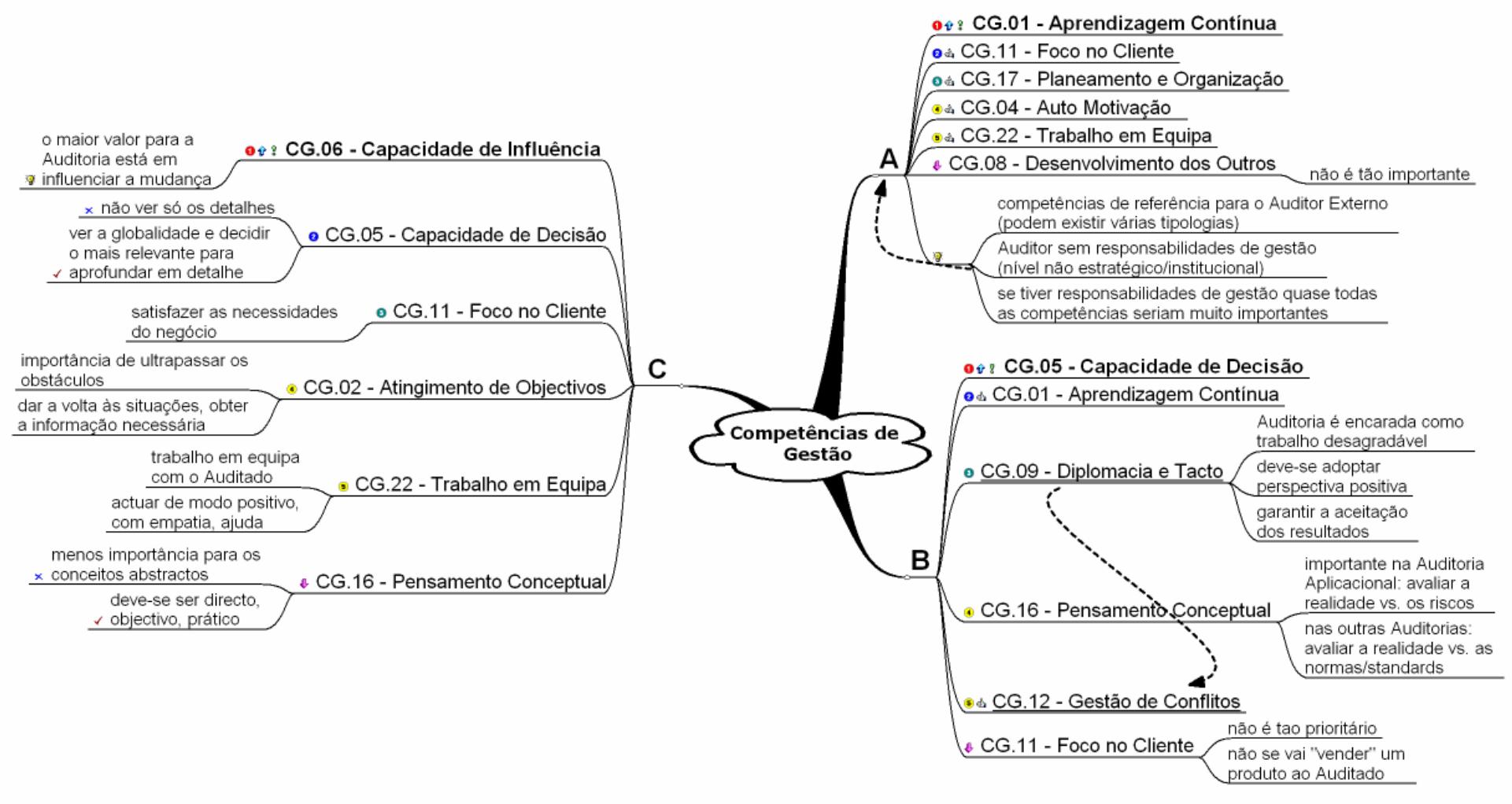
			A		B		C		Média	
	COMPETÊNCIAS TÉCNICAS (*Hard Skills*)									
Nº	**Competências**	**Tópicos**	**Pontuação**	**Destaques**	**Pontuação**	**Destaques**	**Pontuação**	**Destaques**	**Pontuação**	**Destaques**
CT.1.0	**Domínio de Conhecimento: Processo de Auditoria**									
CT.1.1	**Conhecimentos da Função Auditoria de SI**	Leis e regulamentos; Natureza e origem das auditoria (teoria da agência, seguros, etc.); Necessidade de controlo dos SI; Tipos de auditoria (externa, interna, de gestão, etc.); Responsabilidade e autoridade do Auditor (carta de auditoria, sub-contratação, etc.); Regulação da profissão de Auditor de SI (Código de Conduta, normas, etc.)	5		4		4		4	
CT.1.2	**Conceitos Fundamentais de Auditoria**	Materialidade; Prova/Evidência; Relevância; Independência; Risco; Fraude; Conformidade; etc.	5	# 1	5	# 1	5		5	# 1
CT.1.3	**Normas e Orientações para Auditoria de SI**	Conhecimento dos Códigos de Ética Profissional (ex: ISACA); Normas e Orientações para Auditoria de SI; Técnicas e práticas de Auditoria de SI.	3		5		4		4	
CT.1.4	**Conhecimentos dos Conceitos de Controlo Interno**	Estrutura e indicadores de Governo dos SI; Objectivos de Controlo Interno; Classificação de Controlos (preventivos, detectivos, correctivos); Controlos Gerais (organização, segurança, desenvolvimento, documentação, etc.); Controlos Aplicacionais (entrada, processamento, saída, etc.); Estruturas de Controlo (ex: CobiT)	4		5	# 2	5	# 1	5	# 2
CT.1.5	**Processo de Planeamento de Auditorias**	Planeamento estratégico e táctico de Auditorias; Carta de Auditoria; Métodos de avaliação de riscos; Técnicas de recolha de informação e avaliação de controlos; Plano, programa e âmbito da Auditoria; Cassificação e tipos de Auditorias (operacional, geral, aplicacional, física, lógica, etc.)	3		4		4		4	
CT.1.6	**Gestão da Auditoria**	Alocação e prioritização de recursos; Avaliação da qualidade da Auditoria; Identificação de melhores prácticas; Planeamento da carreira; Desenvolvimento profissional; etc.	4		4	# 5	4		4	# 5
CT.1.7	**Processo de Prova/Evidência em Auditoria**	Provas/evidências suficientes, relevantes e úteis; Técnicas de recolha de prova/evidência; Natureza e tipos de teste de conformidade vs. substantivos; Amostragem estatística e não estatística; Sistemas/aplicações de apoio à Auditoria; Regras sobre documentação; Materialidade das excepções/conclusões; Revisão do trabalho e alcance dos objectivos.	4		5	# 4	5		5	# 4
CT.1.8	**Relatório de Auditoria e Seguimento/Acompanhamento**	Relatórios de Auditoria (forma, estrutura, conteúdos, linguagem, destinatários, etc.); Seguimento/acompanhamento da implementação das recomendações.	5	# 5	5		5		5	# 5
CT.2.0	**Domínio de Conhecimento: Gestão, Planeamento e Organização dos SI**									
CT.2.1	**Gestão dos Sistemas e Tecnologias de Informação**	Gestão de Projectos de Tecnologias de Informação; Gestão do Risco (económico, tecnológico, etc.); Controlo de qualidade do software; Gestão das infraestruturas, das operações e do suporte das Tecnologias de Informação; Indicadores de desempenho das Tecnologias de Informação; Externalização de funções de Sistemas e Tecnologias de Informação.	4		4		5		4	
CT.2.2	**Planeamento Estratégico dos Sistemas e Tecnologias de Informação**	Estratégias competitiva e ligação com estratégia corporativa; SI Estratégicos; Tipos e classificações de SI; Segregação de funções; Formação em Sistemas e Tecnologias de Informação.	3		4		4		4	
CT.2.3	**Problemáticas da Gestão dos Sistemas e Tecnologias de Informação**	Aspectos legais; Propriedade intelectual; Aspectos éticos; Privacidade; Governo dos SI; Outras problemáticas actuais.	2		4		3		3	
CT.2.4	**Ferramentas de Suporte e Modelos Estruturados**	Utilização na Auditoria de ferramentas de suporte e modelos estruturados (ex: CobiT; ITIL, ISO17799, etc.)	5		5	# 3	5	# 2	5	# 3
CT.2.5	**Técnicas**	Verificações ao controlo de alterações; Verificações operacionais; Revisões à gestão da qualidade.	4		4		4		4	
CT.3.0	**Domínio de Conhecimento: Infraestruturas Técnicas e Práticas Operacionais de SI**									
CT.3.1	**Infraestruturas Técnicas (prácticas de Planeamento, Implementação e Operação)**	Arquitectura das Tecnologias de Informação; Hardware; Software; Redes; Segurança; Controlos base; Ferramentas de monitorização do desempenho; Governo dos SI; Gestão dos recursos e das infraestruturas da Informação; Sistemas proprietários vs. abertos.	4		4		5		4	
CT.3.2	**Gestão de Centros de Serviço - manter a infraestrutura de sistemas e tecnologias de informação através de organizações dedicadas a estas actividades**	Gestão de Centros de Serviço e normas/orientação de operação (ex: CobiT; ITIL, ISO17799, etc.); Gestão da mudança (ex: novas implementações, alterações, ferramentas de controlo); Gestão da segurança; Gestão da configuração; Gestão de incidentes; Gestão da capacidade; Alocação de recursos; Gestão de sistemas distribuídos; Gestão de fornecedores; Gestão de clientes; Gestão de níveis de serviço; Gestão da contingência e da recuperação (ex: backups); Gestão de centros de atendimento; Gestão de redes; Gestão das operações da infraestrutura.	5	# 2	4		5		5	

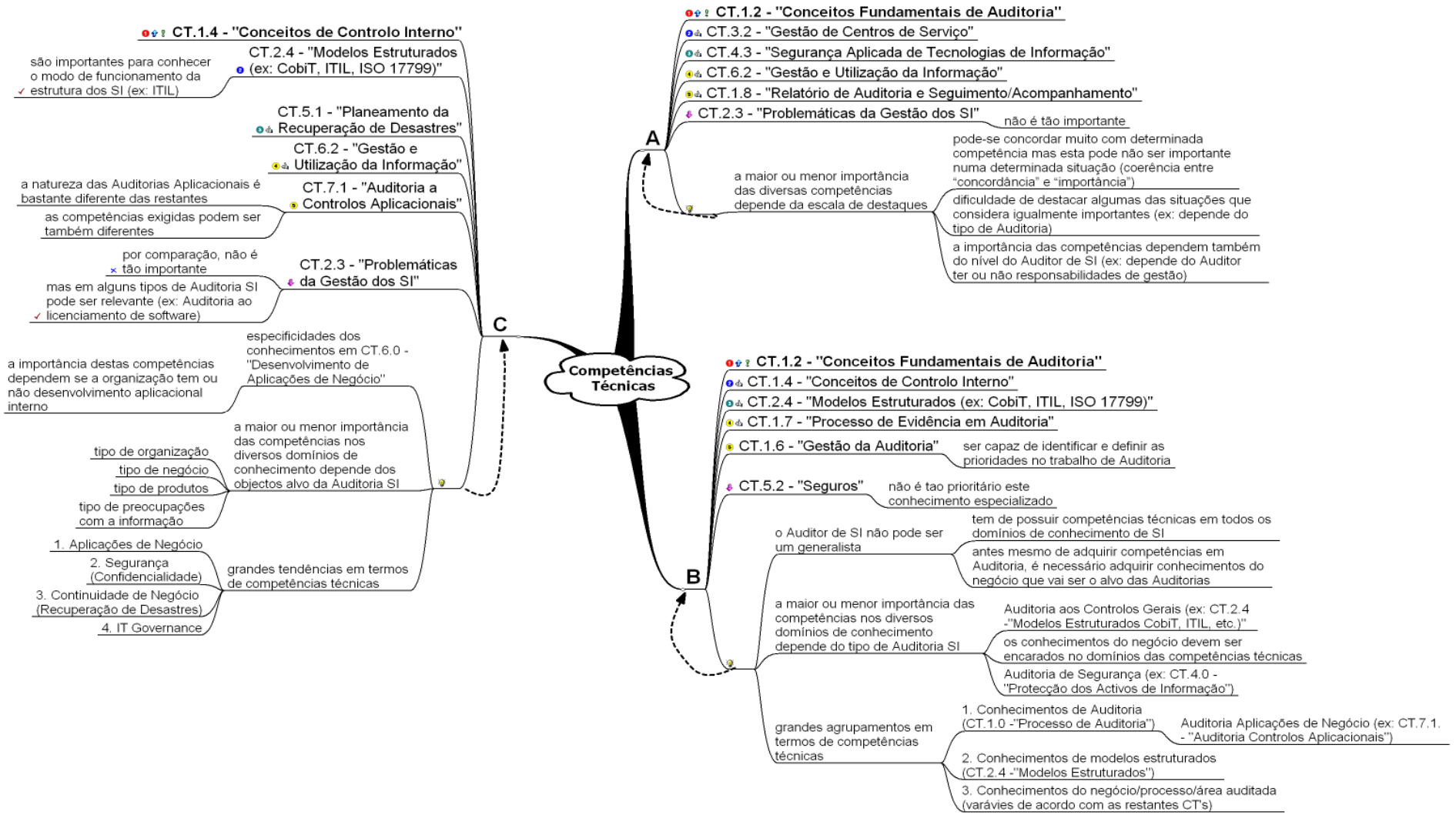
CT.4.0	**Domínio de Conhecimento: Protecção dos Activos de Informação**										
CT.4.1	**Gestão da Segurança dos Activos de Informação**	Conceitos básicos de segurança das Tecnologias de Informação; Necessidade de segurança dos recursos de Informação; Políticas de segurança; Normas de segurança.	5		4		5		5	
CT.4.2	**Segurança Lógica das Tecnologias de Informação**	Componentes da segurança lógica das Tecnologias de Informação; Controlo de acessos lógicos; Procedimentos, ferramentas e software de controlo de acessos.	5		4		5		5	
CT.4.3	**Segurança Aplicada de Tecnologias de Informação - Recursos de Alta Tecnologia**	Segurança das comunicações e das redes (ex: cliente-servidor, serviços baseados na rede; firewalls, encriptação, etc.) Segurança dos centros de processamento de dados; Segurança das bases de dados; Segurança dos sistemas de desenvolvimento e dos processos de manutenção.	5	# 3	4		5		5	# 3
CT.4.4	**Segurança Física e da Envolvente**	Conceitos de segurança física das Tecnologias de Informação; Controlo dos acessos físicos; Questões da envolvente.	5		4		5		5	
CT.5.0	**Domínio de Conhecimento: Recuperação de Desastres e Continuidade de Negócio**										
CT.5.1	**Protecção da Arquitectura e dos Activos das Tecnologias de Informação - Planeamento de Recuperação de Desastres**	Avaliação de impactos no negócio; Comprometimento e suporte por parte da Gestão; Documentação, preparação, aprovação e distribuição do plano de continuidade de negócio. Manutenção, formação, teste e verificação do plano de continuidade de negócio; O papel do auditor.	3		4		5	# 3	4	# 3
CT.5.2	**Seguros**	Valoração dos activos (ex: equipamentos, sistemas, pessoas, etc.); Recursos que podem ser segurados; Tipos e descrição de seguros.	4		3		4		4	
CT.6.0	**Domínio de Conhecimento: Desenvolvimento, Aquisição, Implementação e Manutenção de Aplicações de Negócio**										
CT.6.1	**Planeamento de Sistemas de Informação**	Componentes da gestão dos SI (ex: processos de dados, tecnologias, organização, etc.); Entender as partes interessadas e as suas necessidades; Métodos de planeamento de SI (investigação de sistemas, oportunidades de integração e reengenharia de processos; avaliações de risco e de custo-benefício, análise de sistemas orientados a objectos, etc.); Integração com o software de planeamento de recursos da organização.	4		4		4		4	
CT.6.2	**Gestão e Utilização da Informação**	Monitorização de desempenho de níveis de serviço face aos acordados; Qualidade, disponibilidade, integridade, privacidade; Dados e informação; Análise, avaliação e desenho da arquitectura da Informação (ex: o papel das bases de dados e dos sistemas de gestão e armazenamento de dados); Arquitectura das aplicações (ex: modelação de SI; processos e soluções, etc.); Análise, avaliação e desenho de entidades, seus processos de negócio e modelos de negócio; Gestão da Informação (ex: administração de dados e de bases de dados, papeis e responsabilidades de administração, etc.); Tecnologias de bases de dados como ferramentas para o auditor; Estruturas de dados e linguagens de interrogação de dados.	5	# 4	4		5	# 4	5	# 4
CT.6.3	**Desenvolvimento, Aquisição e Manutenção de Sistemas de Informação**	Gestão de Projectos de SI (ex: planeamento, organização, desenvolvimento, controlo, execução, etc.); Métodos para o ciclo de vida de desenvolvimento de software (fases e tarefas, análise, avaliação, desenho, etc.); Abordagens ao desenvolvimento de sistemas (ex: pacotes standard, prototipagem, reengenharia de processos, engenharia assistida por computador, etc.); Procedimentos de manutenção e de controlo de alterações em sistemas; Análise, avaliação e controlo dos riscos e das características dos projectos.	4		4		4		4	
CT.6.4	**Impacto das Tecnologias de Informação nos Processos e Soluções de Negócio**	Externalização de processos de negócio; Tendências e problemáticas de aplicações de comércio electrónico.	2		4		4		3	
CT.6.5	**Desenvolvimento de Software**	Segregação da especificação e da implementação na programação; Metologias para especificação de requisitos; Desenho de algoritmos; Tratamento de ficheiros; Indexação; Criação e manipulação de bases de dados; Bons princípios de desenho de ecrán e de relatórios.	3		4		4		4	
CT.7.0	**Domínio de Conhecimento: Avaliação de Processos de Negócio e Gestão do Risco**										
CT.7.1	**Auditoria e Desenvolvimento de Controlos Aplicacionais**	Procedimentos e controlos de entrada, processamento e saída; Documentação dos sistemas e aplicações; Rotinas de Auditoria.	4		5		5	# 5	5	# 5
Fonte: *ISACA Model Curriculum for IS Audit and Control* Adaptado e traduzido de (ISACA, 2004)											

Anexo 4: Análise dos Resultados das Entrevistas

Este Anexo faz parte integrante da secção "4.3.2 - A Análise Qualitativa dos Resultados".




Competências de Gestão
A
CG.01 - Aprendizagem Contínua
CG.11 - Foco no Cliente
CG.17 - Planeamento e Organização
CG.04 - Auto Motivação
CG.22 - Trabalho em Equipa
CG.08 - Desenvolvimento dos Outros
não é tão importante
competências de referência para o Auditor Externo (podem existir várias tipologias)
Auditor sem responsabilidades de gestão (nível não estratégico/institucional)
se tiver responsabilidades de gestão quase todas as competências seriam muito importantes
B
CG.05 - Capacidade de Decisão
CG.01 - Aprendizagem Contínua
CG.09 - Diplomacia e Tacto
Auditoria é encarada como trabalho desagradável
deve-se adoptar perspectiva positiva
garantir a aceitação dos resultados
CG.16 - Pensamento Conceptual
importante na Auditoria Aplicacional: avaliar a realidade vs. os riscos
nas outras Auditorias: avaliar a realidade vs. as normas/standards
CG.12 - Gestão de Conflitos
CG.11 - Foco no Cliente
não é tao prioritário
não se vai "vender" um produto ao Auditado
C
CG.06 - Capacidade de Influência
o maior valor para a Auditoria está em influenciar a mudança
CG.05 - Capacidade de Decisão
não ver só os detalhes
ver a globalidade e decidir o mais relevante para
aprofundar em detalhe
CG.11 - Foco no Cliente
satisfazer as necessidades do negócio
CG.02 - Atingimento de Objectivos
importância de ultrapassar os obstáculos
dar a volta às situações, obter a informação necessária
CG.22 - Trabalho em Equipa
trabalho em equipa com o Auditado
actuar de modo positivo, com empatia, ajuda
CG.16 - Pensamento Conceptual
menos importância para os conceitos abstractos
deve-se ser directo, objectivo, prático


Competências Técnicas
A
CT.1.2 - "Conceitos Fundamentais de Auditoria"
CT.3.2 - "Gestão de Centros de Serviço"
CT.4.3 - "Segurança Aplicada de Tecnologias de Informação"
CT.6.2 - "Gestão e Utilização da Informação"
CT.1.8 - "Relatório de Auditoria e Seguimento/Acompanhamento"
CT.2.3 - "Problemáticas da Gestão dos SI"
não é tão importante
a maior ou menor importância das diversas competências depende da escala de destaques
pode-se concordar muito com determinada competência mas esta pode não ser importante numa determinada situação (coerência entre "concordância" e "importância")
dificuldade de destacar algumas das situações que considera igualmente importantes (ex: depende do tipo de Auditoria)
a importância das competências dependem também do nível do Auditor de SI (ex: depende do Auditor ter ou não responsabilidades de gestão)
B
CT.1.2 - "Conceitos Fundamentais de Auditoria"
CT.1.4 - "Conceitos de Controlo Interno"
CT.2.4 - "Modelos Estruturados (ex: CobiT, ITIL, ISO 17799)"
CT.1.7 - "Processo de Evidência em Auditoria"
CT.1.6 - "Gestão da Auditoria"
ser capaz de identificar e definir as prioridades no trabalho de Auditoria
CT.5.2 - "Seguros"
não é tao prioritário este conhecimento especializado
o Auditor de SI não pode ser um generalista
tem de possuir competências técnicas em todos os domínios de conhecimento de SI
antes mesmo de adquirir competências em Auditoria, é necessário adquirir conhecimentos do negócio que vai ser o alvo das Auditorias
a maior ou menor importância das competências nos diversos domínios de conhecimento depende do tipo de Auditoria SI
Auditoria aos Controlos Gerais (ex: CT.2.4 -"Modelos Estruturados CobiT, ITIL, etc.)"
os conhecimentos do negócio devem ser encarados no domínios das competências técnicas
Auditoria de Segurança (ex: CT.4.0 - "Protecção dos Activos de Informação")
grandes agrupamentos em termos de competências técnicas
1. Conhecimentos de Auditoria (CT.1.0 -"Processo de Auditoria")
Auditoria Aplicações de Negócio (ex: CT.7.1. - "Auditoria Controlos Aplicacionais")
2. Conhecimentos de modelos estruturados (CT.2.4 -"Modelos Estruturados")
3. Conhecimentos do negócio/processo/área auditada (varávies de acordo com as restantes CT's)
C
CT.1.4 - "Conceitos de Controlo Interno"
CT.2.4 - "Modelos Estruturados (ex: CobiT, ITIL, ISO 17799)"
são importantes para conhecer o modo de funcionamento da estrutura dos SI (ex: ITIL)
CT.5.1 - "Planeamento da Recuperação de Desastres"
CT.6.2 - "Gestão e Utilização da Informação"
CT.7.1 - "Auditoria a Controlos Aplicacionais"
a natureza das Auditorias Aplicacionais é bastante diferente das restantes
as competências exigidas podem ser também diferentes
CT.2.3 - "Problemáticas da Gestão dos SI"
por comparação, não é tão importante
mas em alguns tipos de Auditoria SI pode ser relevante (ex: Auditoria ao licenciamento de software)
especificidades dos conhecimentos em CT.6.0 - "Desenvolvimento de Aplicações de Negócio"
a importância destas competências dependem se a organização tem ou não desenvolvimento aplicacional interno
a maior ou menor importância das competências nos diversos domínios de conhecimento depende dos objectos alvo da Auditoria SI
tipo de organização
tipo de negócio
tipo de produtos
tipo de preocupações com a informação
grandes tendências em termos de competências técnicas
1. Aplicações de Negócio
2. Segurança (Confidencialidade)
3. Continuidade de Negócio (Recuperação de Desastres)
4. IT Governance