UNIVERSIDADE TÉCNICA DE LISBOA

INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

MESTRADO: Contabilidade, Fiscalidade e Finanças Empresariais

TEMA

O CONTROLO INTERNO NO CONTEXTO DAS NOVAS TECNOLOGIAS DE INFORMAÇÃO

Mestrando: Célia Maria Pereira de Sousa

Orientador: Carlos Fernando Calhau Trigacheiro
Equiparado a Professor Coordenador

Júri:

Presidente: Mestre António Carlos de Oliveira Samagaio
Vogais: Mestre Pedro Nuno Ramos Roque
Dr. Carlos Fernando Calhau Trigacheiro

ISEG/UTL, Junho 2011

RESUMO

O objectivo do presente trabalho é fazer um ponto da situação actual dos Sistemas de Controlo Interno no contexto da utilização continuamente crescente dos sistemas de informação. Para tal, optou-se por analisar esta realidade em dois horizontes distintos, ao nível do Ensino Universitário e ao nível empresarial.

A metodologia seguida foi, na primeira situação, a recolha da informação disponível online, relativa aos cursos, disciplinas e respectivos planos curriculares. Nos casos em que esta última informação não estava disponível online foi elaborado inquérito directo.

Relativamente ao trabalho realizado ao nível empresarial, foi feito inquérito directo às entidades envolvidas.

Em termos de resultados, foi possível perceber que globalmente ao nível do ensino superior ainda não são muitos os cursos, nos diversos graus de ensino objecto de análise, que no seu plano curricular abrangem a totalidade dos temas considerados chave no estudo.

Ao nível empresarial, e para as entidades estudadas, verifica-se a existência de consciência e trabalho das entidades a este nível.

Palavras-chave: Controlo Interno; Sistemas de Informação; Segurança; Auditoria.

ABSTRACT

The aim of this project work is to analyse the current situation of the Internal Control Systems in the context of the steadily increasing use of the information systems. This way it was decided to examine this reality into two distinct areas, at Higher Education level and business level.

The methodology followed in the first area was to gather the data available online on the courses, academic disciplines and their curriculum. When this information was not available online, a direct survey was carried out.

In what concerns the work achieved at business level, a direct survey was carried out at the entities directly involved.

The results obtained show that at Higher Education level, there are not yet many courses, in the different levels of education subjected to analysis, which cover in their curriculum all the key issues considered in the study.

At Business level, and for the entities studied it is verified the existence of awareness and work being done in this area by those entities.

Keywords: Internal Control; Information Systems; Security; Audit.

LISTA DAS SIGLAS

CISA - Certified Information Systems Auditor

CMVM – Comissão do Mercado de Valores Mobiliários

COBIT - Control Objectives for Information and Related Technology

COSO - Committee of Sponsoring Organizations of Tread way Commission

ECIIA – European Confederation of Institutes of Internal Auditors

FEE - Fédération des Experts Comptables Européens

IAASB - International Auditing and Assurance Standards Board

IFAC - International Federation of Accountants

IIA – Institute of Internal Auditors

INTOSAI – International Organization of Supreme Audit Institutions

ISACA - Information Systems Audit and Control Association

ISO - International Organization for Standardization

ITGI – Information Technology Governance Institute

ITIL - Information Technology Infrastructure Library,

OROC – Ordem dos Revisores Oficiais de Contas

SEC - Securities and Exchange Commission

INDICE GERAL

INDICE DE GRÁFICOS E QUADROS

INDICE DE ANEXOS

Capitulo 1 – Introdução

O **Controlo Interno** é essencial ao funcionamento e à concretização dos objectivos de uma organização.

A vertente de **Controlo interno num contexto de Sistemas de Informação** assume novos contornos, e desperta novos desafios, que se colocam quer ao nível da organização quer no âmbito da auditoria.

Considerámos importante estudar a forma como este assunto é tratado tanto no contexto do ensino superior como no contexto empresarial.

Existem hoje standards internacionais que permitem às organizações orientar a implementação de sistemas de controlo interno no contexto das tecnologias de informação, e ao auditor orientar o seu trabalho neste campo.

O presente trabalho pretende sintetizar os trabalhos teóricos realizados pelos principais organismos internacionais e que constituem referenciais amplamente aceites acerca deste tema. Partimos duma visão mais tradicional do Controlo Interno no seio de uma organização e evoluímos para as abordagens de Controlo Interno no contexto dos Sistemas de Informação.

Explanadas as principais características dos standards teóricos neste âmbito, pretendeu-se perceber até que ponto os cursos ministrados nas Universidades públicas abordam esta vertente. Ou seja, perceber se o Controlo Interno, os Sistemas de Informação no contexto da organização e a Segurança dos Sistemas de Informação são temas abordados nos cursos e nas disciplinas leccionadas.

Por outro lado pretendeu-se perceber até que ponto a realidade empresarial nacional reflecte estas preocupações. Numa primeira fase, perceber se, no âmbito do controlo Interno existe uma preocupação especial com as Novas Tecnologias e os Sistemas de Informação e que referenciais são seguidos. Numa segunda fase, perceber a vertente da auditoria neste contexto.

Capitulo 2 – Revisão da Literatura

2.1 - Standards de Controlo Interno – Abordagem Tradicional

O **Controlo Interno** é essencial ao funcionamento e à concretização dos objetivos de qualquer organização. Ao longo dos últimos anos diversos organismos internacionais definiram e preconizaram modelos de controlo interno.

O Controlo Interno, segundo o Tribunal de Contas *"…é a forma de organização que pressupõe a existência de um plano e de sistemas coordenados destinados a prevenir a ocorrência de erros e irregularidades ou a minimizar as suas consequências e a maximizar o desempenho da entidade no qual se insere."*, visando *"salvaguardar os activos; garantir a legalidade e a regularidade das operações; assegurar a oportunidade, a confiança e a integridade das informações de gestão; promover a economia e a eficiência das operações ou actividades da empresa; assegurar que os resultados correspondem aos objectivos definidos."*

Não esquecendo a especificidade de cada organização, o Tribunal de Contas considera como princípios essenciais de um Sistema de Controlo Interno:

- A segregação de funções;
- O controlo das operações;
- A definição de autoridade e de responsabilidade;
- Qualificação, competência e responsabilidade dos recursos humanos;
- O registo metódico dos factos;

Deve ter-se sempre presente que um sistema de controlo interno poderá facultar segurança razoável mas não integral.

Hayes e Schilder (1998), especificam duas vertentes do controlo interno, os controlos administrativos, que dizem respeito à promoção da eficiência operacional e à sua aderência às políticas de gestão, estas relacionadas com as auditorias operacionais e de conformidade, e os controlos contabilísticos principalmente relacionados com a salvaguarda dos activos e cujo objectivo será conferir fiabilidade às demonstrações financeiras e aos relatórios financeiros.

A INTOSAI apresenta o Controlo Interno como um *"processo integral e dinâmico que se está constantemente a adaptar às alterações com que a organização se depara."*

As normas de Auditoria do INTOSAI, no seu ponto 141 indicam que "*O auditor, ao determinar o âmbito e o domínio da auditoria, deve analisar e avaliar a fiabilidade do controlo interno".*

As linhas diretrizes europeias relativas à aplicação das Normas de Auditoria do INTOSAI, no nº 21, determinam que *"…ao avaliar os procedimentos de controlo o auditor procura determinar a existência de todos os procedimentos necessários e o seu funcionamento eficaz, continuo e coerente."* Esta mesma directriz pretende orientar a avaliação do controlo interno e a execução de testes de controlo neste âmbito.

Na mesma linha, também a IFAC / IAASB no seu normativo técnico consagra uma norma aos aspectos relativos à necessidade do auditor comunicar as deficiências identificadas no Controlo Interno, a ISA 265, que no seu objectivo descreve que *" O objectivo do auditor é comunicar de forma apropriada, aos que estão encarregues da governação e da gestão, as deficiências no controlo interno por ele identificadas no decurso da auditoria, e que no seu julgamento profissional tenham importância suficiente para merecer a atenção destes".*

Nas referências relativas à sua esfera de acção a esta norma refere que *" Ao auditor é exigido que obtenha uma compreensão do controlo interno, relevante para a auditoria…"*

Em 1992, o COSO, organização formada em 1985 e cuja missão é desenvolver trabalhos e guias acerca do risco de gestão empresarial, controlo interno e dissuasão de fraude, no intuito de incrementar a performance empresarial e para reduzir a fraude nas organizações, publicou um relatório intitulado "Internal Control – Integrated Framework". Este trabalho fornece uma definição geral de Controlo Interno, que se deseja adaptável a diferentes entidades, providenciando um standard que pretende permitir a implementação ou o aperfeiçoamento do sistema de Controlo Interno.

No âmbito do COSO, Controlo interno é globalmente definido como *"um processo, levado a cabo pelo Conselho de Administração, Direcção ou outros membros da entidade, com o objectivo de proporcionar um grau de confiança razoável na concretização dos seguintes* ***objectivos:***

1. *- Eficácia e eficiência das operações*
2. *- Fiabilidade da informação financeira*
3. *- Conformidade com as leis e regulamentos aplicáveis."*

Assim, o Controlo Interno é compreendido como um **Processo**, e não como um fim em si mesmo. Será um conjunto de acções, **concebido e aplicado pelas diversas entidades** da Organização, no sentido de proporcionar um nível de **confiança razoável**, minimizando os riscos mas na perfeita consciência de que será impossível a segurança absoluta, isto é, a eliminação total do risco.

Desta forma, o Controlo Interno ajudará a entidade a atingir os seus objectivos específicos desde que consistentes e coerentes entre si. Estes objectivos passam pela

optimização da performance e do lucro e pela prevenção do desperdício de recursos, pela fiabilidade dos relatos financeiros e pelo cumprimento das normas e regulamentos que lhe são aplicáveis, evitando prejuízos na sua reputação e outras consequências.

No entanto há que ter em consideração que o Controlo Interno apenas poderá ajudar uma entidade a atingir os seus objectivos.
A obtenção dos objectivos é afectada pelas limitações inerentes a todos os Sistemas de Controlo Interno. Limitações que poderão ter origem no erro, eventualmente no conluio, mas principalmente nas limitações de recursos que estão adstritas à concepção do Sistema, uma vez que os seus benefícios têm de ser considerados relativamente aos custos da sua implementação e manutenção.

Definido que está o Controlo Interno, nesta óptica, e explanados os seus objectivos principais, será agora importante referir aquelas que são apontadas por este organismo com as **Componentes do Controlo Interno**, formando no fundo a "trama base" de todo o Sistema. Este conjunto de Objectivos e Componentes é muitas vezes esquematizado através de um cubo, com se pode ver de seguida:

Figura 2.1.1: Committee of Sponsoring Organizations of Tread way Commission (COSO), "Internal Control – Integrated Framework".

O Controlo Interno assim representado, consiste na sua génese em cinco componentes inter-relacionados, que derivam da forma como a gestão conduz o negócio e que estão portanto intimamente ligados ao processo de Gestão.

Como alicerce de todo o processo está o ***Control Environment*** (Ambiente de Controlo), que envolve a própria organização, influenciando a consciência de controlo das pessoas. É a génese para todas as outras componentes do controlo interno, proporcionando disciplina à estrutura. Os factores de Ambiente de Controlo incluem a integridade, os valores éticos e competência das pessoas, a filosofia de gestão e a forma destes operarem, a forma como a gestão atribui autoridade e responsabilidade

e organiza e promove as pessoas, e a atenção e orientação proporcionada pela direcção.

A segunda componente apresentada para este processo é o ***Risk Assessment*** (avaliação do risco), uma vez que todas as entidades enfrentam uma variedade de riscos de origem externa e interna, é essencial proceder à sua avaliação. Esta avaliação tem por base a definição dos objectivos a atingir, consistindo no fundo, na identificação e análise dos riscos relevantes para atingir os objectivos. Assim, o primeiro passo para avaliar o risco é proceder a uma definição de objectivos que se pretende consistente internamente.

A terceira componente descrita, as ***Control Activities*** (procedimentos de controlo) são, no essencial, as politicas e os procedimentos que ajudam a garantir que as directivas da Gestão são tomadas em consideração. Estas medidas, ajudam a assegurar que são levados a cabo os procedimentos necessários para que se venham a atingir os objectivos da entidade, tendo em consideração os riscos previamente identificados. Estes procedimentos de controlo são desencadeados e abrangem toda a organização, a todos os níveis e em todas as funções, incluindo actividades tão diversas como, por exemplo, aprovações, autorizações, verificações, reconciliações, revisão da performance operacional, segurança dos activos e segregação dos passivos.

Um quarto elemento - **Information *and Communication*** (Informação e Comunicação), a informação realmente pertinente terá de ser identificada, e divulgada internamente de forma clara e em tempo útil. Toda a organização deve compreender claramente o seu papel no sistema de controlo interno, devendo tal ser informado pela gestão de topo, no intuito de que cada função perceba de que forma as suas actividades estão relacionadas com o trabalho dos outros. É importante que esta informação e a Comunicação sejam efectivas e claras, não apenas a nível interno, mas também para o exterior, para stakeholders e stockholders.

Finalmente, o ultimo nível das componentes do Sistema, ***Monitoring*** (monitorização), todo o sistema de controlo interno carece de ser monitorizado. É necessária a existência de um procedimento de avaliação da qualidade do sistema ao longo do tempo. Este procedimento poderá ser de monitorização “ongoing”, de avaliações esporádicas ou uma combinação das duas. O âmbito e a frequência das avaliações esporádicas dependerão tanto da avaliação do risco como da eficácia dos procedimentos de monitorização correntes. As falhas detectadas ao longo deste procedimento deverão ser sempre reportadas superiormente.

Existe uma ligação e uma sinergia entre estas componentes, formando um sistema integrado que deverá reagir de forma dinâmica á alteração das condições.

No contexto da Organização todos os elementos, a diferentes níveis, têm responsabilidade no controlo Interno. Partindo da Gestão, passando pela Direcção e pelos Auditores Internos, até à generalidade do pessoal da organização, a abordagem do controlo interno do COSO cobre a generalidade das actividades e das operações. É uma abordagem do controlo interno baseada no risco. Ou seja os procedimentos de controlo interno a serem criados /melhorados têm por base o risco interno e externo subjacente à operação específica.

De acordo com Ratcliffe e Landes (2009) *,"o auditor deve obter o entendimento suficiente dos cinco componentes do controlo interno de forma a poder avaliar o risco de uma distorção materialmente relevante nas demonstrações financeiras, devido a erro ou a fraude, e tendo em vista a definição da natureza, duração e extensão dos correspondentes procedimentos de auditoria."*

No inicio do século XXI, o tema Controlo Interno ganhou nova dimensão, como forma de resposta aos escândalos e falências de grandes empresas que surgiram neste inicio de século. Colocaram as atenções sobre estes temas, trazendo ao de cima assuntos como a corporate governance, o risk management e o internal control.

Em 2004, o COSO emitiu uma outra publicação, *COSO* Enterprise Risk Management – Integrated Framework, que vem complementar o trabalho desenvolvido em 1992. Este documento que mantém o enfoque principal ao nível do Risco, aborda o tema no contexto da Estratégia da Organização. Este trabalho, define Controlo Interno como parte integrante da Gestão do Risco - sendo certo que todas as organizações enfrentam a incerteza, esta comporta riscos e oportunidades, a capacidade da organização para gerir o risco é vital, tendo em vista a maximização do valor. O ponto óptimo entre o crescimento da rendibilidade e o risco relacionado maximizará o Valor.

Em suma, a Gestão do Risco empresarial é definido como *"…um processo, levado a cabo pelo Conselho de Administração, pela gestão ou por outros na organização, aplicado no contexto de uma estratégia ao longo de toda a empresa, definido para identificar as potenciais ocorrências que poderão afectar a entidade, e gerir o risco no âmbito da apetência para o risco, de forma a proporcionar segurança razoável tendo em vista atingir os objectivos da entidade."* – COSO 2004. O ERM apoia a criação de valor na organização na medida em que sugere que a gestão considere os potenciais acontecimentos futuros geradores de incerteza, e a eles responda no intuito de reduzir as perdas e potenciar os ganhos que daí poderão advir.

Comparativamente com a definição considerada no trabalho de 1992 mantêm-se os elementos base, definindo o conceito como um processo, levado a cabo por pessoas a todos os níveis da organização, no intuito de obter Segurança Razoável tendo em vista os objectivos da organização. São introduzidos novos elementos, a **estratégia e a visão**

da empresa relativamente ao risco que está disposta a assumir e às **potenciais ocorrências**.

Este trabalho focalizando-se nos objectivos da entidade, classifica-os em quatro categorias:

- Objectivos Estratégicos – De alto nível, alinhado e suportando a estratégia.
- Objectivos Operacionais – De utilização eficiente e eficaz dos recursos.
- Objectivos de Reporte – fiabilidade dos relatórios.
- Objectivos de Cumprimento – das leis e regulamentos aplicáveis.

Em suma, mantendo a abordagem de controlo interno numa óptica de Risco, o COSO mantém que estas capacidades de gestão do Risco Empresarial, ajudarão a gestão a alcançar os objectivos da organização em termos de performance e de rendibilidade e a prevenir perdas de recursos, a assegurar que o relato financeiro é fiel e efectivo e que as normas e regulamentos aplicáveis estão a ser cumpridos. Isto é, o Controlo Interno direccionado para a Gestão do Risco Empresarial, nesta abordagem mais recente, mantém os objectivos definidos para o Sistema de Controlo Interno em 1992.
Tal como transparece do resumo esquemático que se segue, mantém-se a interligação dos elementos, acrescentando uma categoria de Objectivos essêncial a esta nova abordagem, os Objectivos Estratégicos. Torna-se agora mais claro que o Controlo Interno é aplicável no ambito de todas as actividades e a todos os níveis da organização, desde o nível da Empresa, ao da Divisão ou da Subsidiária até ao nível da unidade de negócio.

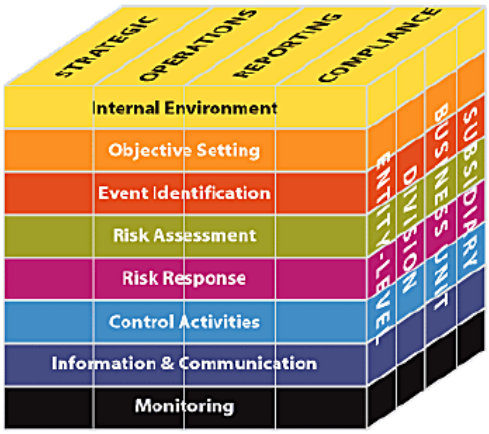


Figura 2.1.2: "COSO ERM Framework – September 2004"

Ao nível das componentes, mantém basicamente a estrutura apresentada em 1992, tendo sido acrescentadas componentes relacionadas directamente com o Risco e com a análise estratégica, mantendo a interligação entre as actuais 8 componentes.

O **ambiente interno**, que estabelece basicamente a filosofia de risco, reconhecendo a possibilidade de existência de ocorrências inesperadas e definindo no fundo a cultura de risco da empresa.

Os dois elementos que se seguem, são inovações na esquematização apresentada.

Estabelecer Objectivos, aplica-se quando a estratégia de risco é tida em consideração na definição dos objectivos. A tolerância ao risco por parte da organização é estabelecida pela variação considerada aceitável para os objectivos definidos, estando também alinhado, obviamente com a apetência para o risco da entidade, isto é, até que nível de risco a organização está disposta a aceitar.

Identificação de Acontecimentos, que poderão surgir, interna ou externamente, e que afectarão a estratégia da organização e a concretização dos seus objectivos. Neste âmbito deverão ser distinguidos os riscos e as oportunidades, ou seja, acontecimentos que podem ter impacto negativo representam riscos, ocorrências que podem ter impacto positivo representam oportunidades.

Avaliação do Risco, permitirá à entidade compreender até que ponto os acontecimentos potenciais poderão ter impacto nos objectivos definidos.

Resposta ao Risco, mais uma componente acrescentada nesta esquematização, será a identificação e avaliação das possibilidades de resposta ao risco, dependendo da apetência para o risco que a organização tem, e feita a análise da relação custo/benefício da resposta a ser dada.

Procedimentos de Controlo, politicas e procedimentos instituídos que asseguram que a resposta ao risco funciona e bem como outras directivas da entidade são seguidas.

Informação e Comunicação, tal como já descrito, a gestão deverá comunicar a informação pertinente de forma clara e atempada, permitindo ao pessoal da organização assumir as suas responsabilidades.

Monitorização da eficácia da Estratégia de Gestão do Risco é levada a cabo através de atividades de monitorização ongoing, avaliações separadas ou mesmo uma combinação de ambas.

Também no contexto da falência de grandes empresas, em particular nos Estados Unidos da América, logo em 2002, surge a US Sarbanes-Oxley Act (SOX), uma lei Federal Norte Americana que define um conjunto de regras a serem cumpridas pelas Empresas de Auditoria, e por todas as empresas (americanas ou não) que se encontrem registadas na Securities and Exchange Commission (SEC), pretendendo desta forma garantir a existência de mecanismos que assegurem a transparência na Gestão dos negócios e a minimização do risco.

A SOX é composta por 11 títulos que descrevem os requisitos do relato financeiro. O título **Quatro - Divulgação da Informação Financeira**, em particular na **Secção 404** é dedicado à Avaliação da Gestão do Controlo Interno. Neste ponto, é exigido que as empresas registadas na SEC reportem o seu controlo interno no relatório financeiro, nomeadamente que declarem a responsabilidade da Gestão de implementar e manter a estrutura adequada de controlo interno e os procedimentos de relato financeiro. E ainda que avaliem no termo do ano fiscal mais recente, a eficácia do Sistema de Controlo Interno e dos procedimento de relato financeiro. Neste contexto, também a empresa de auditoria, na preparação do seu relatório deverá atestar e fazer constar no relatório a avaliação feita pela gestão acerca deste assunto.

A SOX foca um aspecto específico do Controlo Interno, o Controlo Interno no âmbito do relato financeiro, na medida em que se tornou claro que o controlo interno efectivo dentro de uma organização, é essencial para que exista confiança nas demonstrações financeiras publicadas, tornando-se fulcral neste contexto, a independência dos auditores que deverão certificar a existência e adequabilidade do referido controlo interno.

Os procedimentos de Controlo Interno levados a cabo dentro de uma organização, desde que adequados ao nível de risco da entidade e monitorizados adequadamente no sentido de ser possível aferir da sua eficácia são elementos vitais na garantia das Boas Práticas de Gestão e portanto essenciais na relação existente com stockholders na medida em que estas entidades se relacionam com a organização e têm nos relatórios financeiros desta a base da informação que lhes permitirá tomar decisões.

De notar, no entanto, a chamada de atenção feita no "Livro Branco sobre a Corporate Governance em Portugal", *"Em suma, colocando a criação de valor para os accionistas e o tratamento equitativo destes no centro dos objectivos do governo da empresa e do desenho da respectiva estrutura de fiscalização e controlo, crê-se que a gestão e a fiscalização das empresas igualmente deverá ter em conta as responsabilidades sociais da empresa."*

Neste espaço ganha especial relevo o papel do auditor como garante da informação prestada pelas entidades sendo-lhe exigida a apreciação e análise do sistema de controlo interno da entidade objecto de trabalho.

Particularmente a Auditoria Interna, que de acordo com a definição da ECIIA *"É uma garantia objectiva e independente, e uma actividade de consultadoria desenhada para acrescentar valor e incrementar a actividade da organização. Ela ajuda a organização no acompanhamento dos seus objectivos através duma abordagem disciplinada e sistemática que permite avaliar e incrementar a eficácia na gestão do risco, controlo e processos de governação."*

A CMVM no Código de Governo das Sociedades da CMVM - Recomendações, de Janeiro de 2010, expressa claramente a necessidade de criação de sistemas internos de controlo e gestão de riscos. Esses sistemas deverão, ainda de acordo com a referida recomendação, integrar uma série de componentes relativas ao risco.

Nesta mesma publicação é manifesto que cabe ao órgão de administração *"assegurar a criação e funcionamento dos sistemas de controlo interno e de gestão de riscos, cabendo ao órgão de fiscalização a responsabilidade pela avaliação do funcionamento destes sistemas".*

Também é recomendado que as organizações procedam à identificação dos principais riscos a que estão expostas e à descrição dos sistemas de gestão desses riscos, no âmbito do Relatório Anual sobre o Governo das Sociedades.

Existe ainda a clara preocupação de manter a independência dos órgãos de fiscalização, recomendando mesmo, a rotação de auditores ao final de 2 ou 3 mandatos, conforme estes mandatos sejam de 4 ou de 3 anos.

No que concerne ao auditor externo, este deverá verificar, entre outros elementos, *"a eficácia e o funcionamento dos mecanismos de controlo interno e reportar quaisquer deficiências …"*, aliás na linha do que é também recomendado pela ISA 265, supra referida.

Também o Estado Português se preocupa em assegurar que o seu sector empresarial cumpra o que define como os Princípios de Bom Governo. O Decreto-lei nº 300/2007 constitui uma actualização ao regime jurídico do sector empresarial do Estado, alterando a legislação de 1999. O actual decreto-lei, no ponto 3 do seu Artigo 12º determina que as empresas públicas terão de adoptar *"procedimentos de controlo interno adequados a garantir a fiabilidade das contas e demais informação financeira…".*

Refere ainda a supra citada legislação, na alínea l) e n) do Artigo 13º - A, que o relatório anual da empresa deverá referir expressamente a identificação dos auditores externos e deve também conter o relatório por eles elaborado.

A Resolução do Conselho de Ministros nº 49 /2007 assume um papel preponderante nesta área, dando especial destaque ao princípio da transparência, à prevenção de conflitos de interesses e ao controlo do risco. Particularmente no ponto II do Anexo, no parágrafo 16 e seguintes é recomendado que a auditoria nestas organizações observe padrões idênticos aos praticados para as empresas com títulos admitidos à negociação em mercados regulamentados.

A Directriz de Revisão / Auditoria 410 da OROC debruça-se sobre o tema Controlo Interno, remetendo para o trabalho inicialmente apresentado pelo COSO, quando apresenta o controlo interno como um conjunto de cinco componentes interligadas.

A referida Directriz define três grandes objectivos da auditoria/revisão ao sistema de controlo interno:

- Relato financeiro – assegurar que as demonstrações financeiras cumprem os princípios contabilísticos geralmente aceites.
- Conformidade com os Objectivos – naquilo em que as operações e a sua conformidade com os objectivos da organização dizem respeito a informação utilizada pelo auditor.
- Salvaguarda de activos – da utilização ou aquisição não autorizados, normalmente limitado aqueles que se consideram relevantes para o relato financeiro.

Esta Directriz chama ainda a atenção para as limitações inerentes aos sistemas de controlo interno:

- Erro humano por negligência ou má percepção das regras, à possibilidade de conluio que resultará na ilusão do sistema de controlo.
- Os procedimentos de controlo interno serem estabelecidos para as operações de rotina e não para as operações esporádicas.
- O facto de a gestão fazer uma apreciação exclusivamente quantitativa, isto é estabelece uma relação custo/beneficio para a implementação de cada procedimento de controlo.
- O ambiente de controlo pode reduzir a eficácia de outros componentes.
- A alteração de algumas condições, como os titulares do capital, os órgãos de gestão etc. poderá também afectar negativamente o controlo interno da organização.

Ao planear a auditoria, deverá o revisor/auditor compreender os procedimentos de controlo que sejam relevantes para as asserções contidas nas demonstrações financeiras.

Ainda neste caminho, várias outras organizações por todo o mundo publicam trabalhos sobre o tema, entre as quais e ao nível da Europa, a FEE.

Em 2003, no seu “Discussion Paper on the Financial Reporting and Auditing Aspects of Corporate Governance” reconhece o papel fundamental dos sistemas de controlo interno e de gestão do risco, no sucesso de qualquer organização, não apenas ao nível do reporte financeiro mas também nas operações diárias. Defende ainda que um sistema de Controlo Interno difere de acordo com a organização, nomeadamente em

função da sua dimensão, tipo de mercado onde se insere, forma de gestão do risco que adopta e da relação custo/ beneficio dos vários sistemas de controlo.

No fundo corrobora as conclusões dos estudos do COSO.

Em 2005 no seu "Discussion Paper on Risk Management and Internal Control in the EU", a FEE assume-se como não apologista da implementação de legislação equivalente à SOX ao nível da EU, defendendo antes que existem mecanismos mais eficientes, em alternativa à legislação.

Já em 2009, na publicação "Discussion Paper for Auditor's Role Regarding Providing Assurance on Corporate Governance Statements", a FEE sugere aos Estados Membros, que, para além dos elementos impostos no âmbito da Quarta e da Sétima Directiva, no que diz respeito às Declarações da Corporate Governance, venham a recomendar ou mesmo a exigir outro tipo de informações, nomadamente a Declaração do Conselho de Gestão acerca do Controlo Interno.

2.2 – O Controlo Interno num Contexto das Novas Tecnologias de Informação – Standards Internacionais vocacionados para o Controlo Interno neste contexto.

A evolução tecnológica das últimas décadas e o uso generalizado das novas tecnologias de informação abriu um leque de possibilidades e de ameaças a todas as Organizações.

A Informação contida maioritariamente em suporte informático, representa indubitavelmente uma mais-valia para a organização, possibilitando o acesso rápido à informação, facilitando a tomada de decisão em tempo útil, bem como reduzindo o espaço ocupado, facilita o transporte e o acesso à informação.

No entanto, dada a evolução tecnológica e o consequente desenvolvimento do capital humano nesta área, o acesso à documentação é agora fácil, assim como é fácil a sua reprodução. Esta aparente simplificação poderá colocar em causa a sua fiabilidade, passando a ser necessário ter em consideração a própria fiabilidade do suporte da informação.

A autenticidade dos documentos electrónicos é um assunto de grande relevância actualmente, e poderá em última análise ser atestada através da Assinatura Digital a qual tem um papel fundamental para conferir autenticidade e até confidencialidade aos documentos electrónicos. No panorama jurídico nacional existe legislação relativa ao regime jurídico dos documentos electrónicos e da assinatura digital - Decreto-Lei nº 290-D/99, de 2 de Agosto, alterado pelo Decreto-Lei nº 62/2003, de 3 de Abril.

É vital para a organização, conhecer as potencialidades e saber controlar os riscos associados ao uso destes sistemas. Este ambiente de desmaterialização dos

documentos, mas também dos processos operativos dentro da organização, obrigou à transformação dos procedimentos de controlo interno mas também obrigou a que os processos de auditoria conducentes à avaliação dos anteriores sofressem um processo de adaptação a esta nova realidade. Estes sistemas de informação contêm em si mesmos, potencialidades e riscos para a organização, mas também para os auditores, na medida em que configuram a possibilidade de realização de auditorias mais eficazes, apesar de, necessariamente mais complexas, exigindo dos auditores uma maior especialização nesta área. Os auditores de Sistemas de Informação terão de respeitar as regras e exigências da sua profissão e terão de ter a qualificação adequada ao trabalho a realizar.

No âmbito do Controlo Interno no contexto das tecnologias de informação, diversos standards internacionais abordam o tema, traduzindo procedimentos genericamente aceites na implementação e avaliação de sistemas de controlo interno no contexto de Tecnologias de Informação. Numa óptica organizacional, em 1998, foi criado o IT Governance Institute no intuito de promover a reflexão e standards no âmbito da Gestão e controlo das tecnologias de informação empresariais. A ITGI tem como objectivo assegurar que as tecnologias de Informação suportarão os objectivos da organização, optimizam o investimento nesta área e asseguram uma relação equilibrada entre o risco e as oportunidades criadas pelas tecnologias de informação. O ITGI criou e publicou o COBIT, que neste momento vai na sua versão 4.1. e que basicamente funciona como um Guia na área da Gestão das Tecnologias de Informação. De acordo com o próprio ITGI no COBIT 4.1: *" Valor, Risco e Controle constituem o núcleo da IT Governance".*

A implementação desta base de trabalho permite:

- Estabelecer a ligação com as necessidades de negócio.
- Organizar as actividades de Tecnologias de Informação segundo um modelo genericamente aceite.
- Identificar os principais recursos de Tecnologias de Informação a serem alavancados.
- Definir os objectivos de controlo de gestão a serem tidos em consideração.

Assim, o COBIT é uma abordagem essencialmente orientada para o negócio, efectuando a ligação entre os objectivos de negócio e os objectivos das tecnologias de informação, fornecendo métricas e modelos para avaliar a sua realização e identificar as responsabilidades associadas, tanto no campo da gestão como no campo Tecnologias de Informação.

Partindo da gestão dos processos e tendo em vista os objectivos do negócio, foi desenhado no intuito de servir 3 Grupos de potenciais utilizadores:

- A Gestão, que necessita de avaliar o risco e definir os investimentos em TI a realizar.
- O Utilizadores das TI, que necessitam de ter a garantia de que o resultado das suas operações estará assegurado.
- Os Auditores, que poderão utilizar as recomendações do COBIT como standard na avaliação da gestão das TI.

No fundo, o COBIT integra os princípios do COSO, numa visão mais restrita, a das Tecnologias de Informação.

Enquadrado pelos requisitos no âmbito do negócio, Eficácia, Eficiência, Confidencialidade, Integridade, Disponibilidades, Cumprimento, Fiabilidade e pelas fontes dos Sistemas de Informação, Aplicações; Informação, Infra-estruturas e Pessoas. O processo definido no âmbito do COBIT é ilustrado por um modelo que reparte as Tecnologias de Informação em quatro domínios fundamentais, os quais cobrem o ciclo de vida do investimento em Tecnologias de Informação, partindo do **Planeamento e organização**; passando pela sua **Aquisição e implementação;** ao **Fornecimento e suporte** chegando finalmente à **Monitorização e avaliação.** A importância relativa de cada um destes domínios difere de empresa para empresa, dependendo dos seus objectivos e risco.

Os 4 domínios descritos comportam 34 processos, os quais são desmembrados em 316 actividades e tarefas da organização, que gerem os recursos de Tecnologias de Informação de forma a distribuir a informação de acordo com as exigências do negócio e dos órgãos de gestão, tal como descrito na figura abaixo.

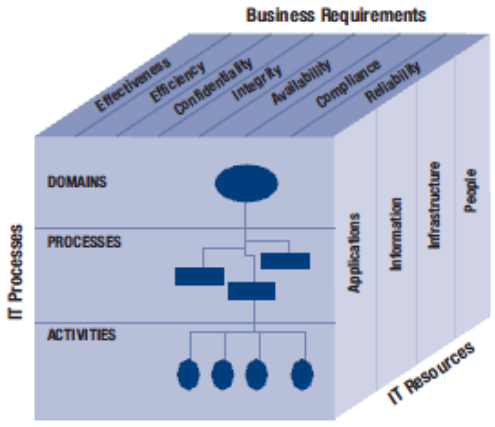


Figura 2.2.2 COBIT Cube

Dentro de cada processo das Tecnologias de Informação, são definidos Objectivos de controlo, constituindo uma declaração genérica do mínimo necessário para assegurar que o processo está sob controlo, de acordo com as definições da gestão.

O conceito chave no COBIT é a definição e o aperfeiçoamento sistemático da maturidade do processo. O COBIT reconhece que atingir os objectivos da organização requer que se desenvolva sistematicamente a capacidade de atingir resultados em cada um dos processos de tecnologias de informação. Estas capacidades exigem a combinação de recursos humanos, de hardware e de software, unidos numa estrutura de políticas e procedimentos.

Cada um destes recursos requer uma monitorização cuidada, através de um conjunto de métricas e a sua revisão, no intuito de assegurar que um dado processo continua a responder como esperado.

O conceito de maturidade do processo decorre directamente do Capability Maturity Model do Software Engineering Institute's (SEI's). Este Modelo define seis níveis para medir a maturidade do processo de tecnologias de informação.

- 0 - Inexistente – A organização não reconhece a existência de um processo a ser seguido.
- 1 - Inicial – Há evidências de que a organização reconhece que o processo existe, no entanto os processos são eventuais e não organizados.
- 2 - Repetitivos – Os processos seguem um padrão regular.
- 3 - Definido – Os processos estão documentados e divulgados.
- 4 - Administrado – Os processos são monitorizados e mensurados
- 5 - Optimizado – As melhores práticas são seguidas e automatizadas.

O objectivo de nível de maturidade deverá variar para cada processo de IT individualmente considerado, dentro de uma mesma organização. De igual modo, varia de acordo com as diferentes organizações e o hardware existente.

Tal como resumidamente ilustrado na figura 2.2.3, para o COBIT, os quatro domínios fundamentais apresentados, deverão ser enquadrados e servirão os objectivos definidos no âmbito da Organização, segundo a gestão do risco, recursos da gestão e performance pretendida. Neste contexto deverão ser definidas métricas de avaliação do cumprimento dos objectivos estipulados.

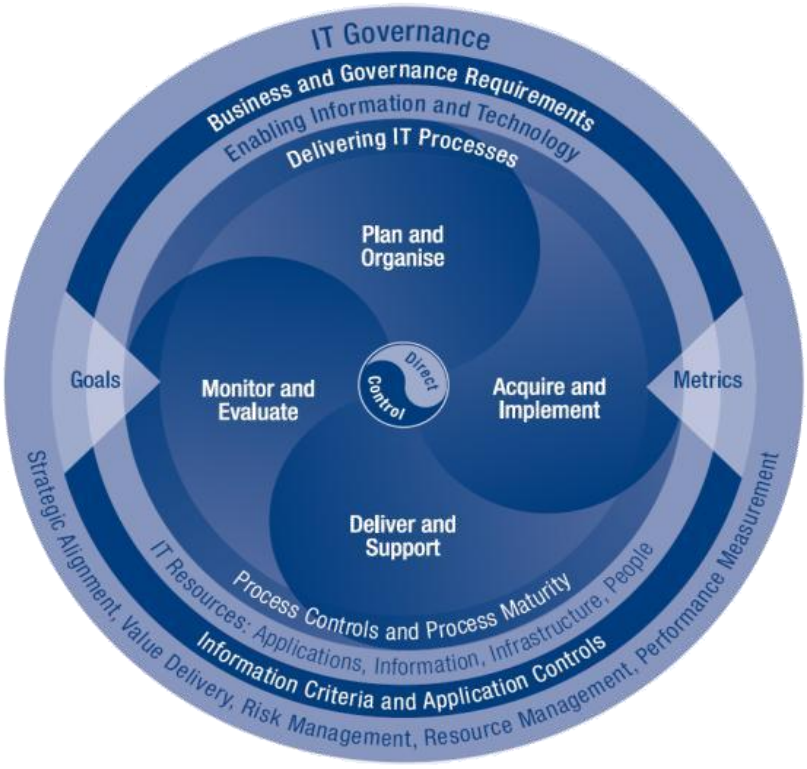
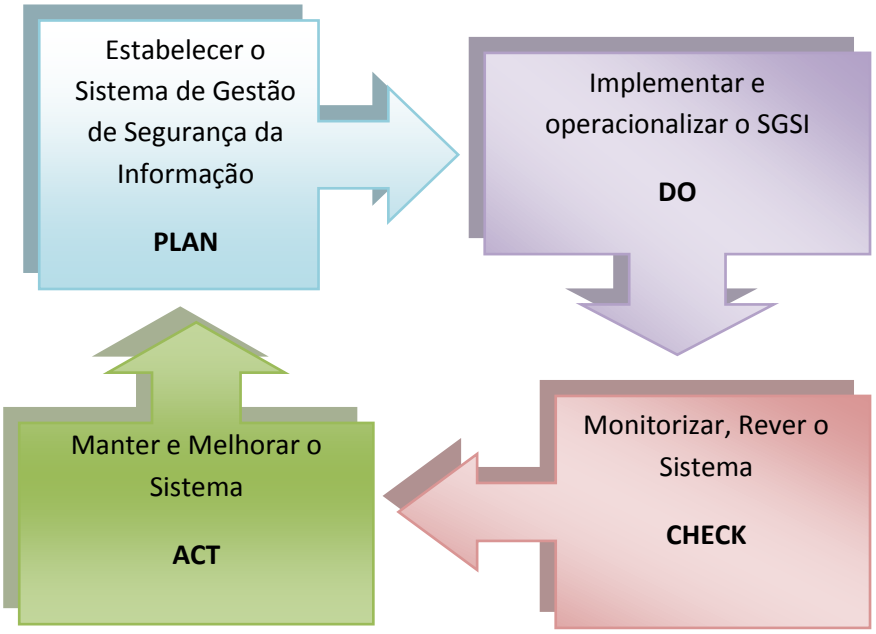


Figura2.2.3 © 2009 ISACA

Nesta linha de trabalho, a International Organization for Standardization, instituição não governamental internacional, que tem como objectivo estabelecer padrões internacionais em diversas áreas, publicou em 2005 a ISO 27001, uma norma que visa definir os requisitos para implementação de um Sistema de Gestão de Segurança da informação.

Esta norma, que no essencial pretende levar à certificação da organização, está delineada de forma a assegurar a selecção de formas de controlo adequadas, que permitirão majorar a Segurança da informação, na óptica da sua confidencialidade; integridade e disponibilidade.

Define, no fundo, a forma de estabelecer, implementar, operacionalizar, monitorizar, rever, manter e melhorar o Sistema de Gestão da Segurança da Informação entendido como uma parte do Sistema Global de Gestão. Baseia-se numa abordagem de risco, isto é, numa aproximação sistemática aos riscos inerentes ao negócio, apelando neste contexto ao tradicional ciclo PDCA – Plan; Do; Check; Act.



A norma apresenta os passos para estabelecer o SGSI, tendo por base as características do negócio, da organização e das tecnologias e a abordagem ao risco que a organização faz. Cada entidade deverá, ela própria, definir o seu nível de risco aceitável. Identificar, analisar e avaliar os riscos e assim avaliar formas de os tratar. Caberá pois à organização seleccionar objectivos de controlo para o tratamento dos riscos, assim como implementar e operacionalizar o SGSI e daí monitorizar, rever e melhorar continuamente o referido Sistema.

A norma em análise descreve um conjunto de documentos essenciais ao processo de controlo, definindo ainda as responsabilidades da Gestão e funções para os auditores internos neste âmbito.

Ainda no âmbito da família ISO 27000 há a referir a ISO 27002, no essencial, um código de boas práticas para a gestão da segurança dos sistemas de informação, um documento genérico de consulta nesta área. Tal como esquematizado na figura abaixo, esta norma, estando dividida em 12 secções, deixa um conjunto de 39 objectivos de controlo direccionados para os riscos de segurança da informação, preservação da sua confidencialidade, integridade e disponibilidade. Enquadrado por estes objectivos de controlo estão referenciados, um total de 139 “controlos”.

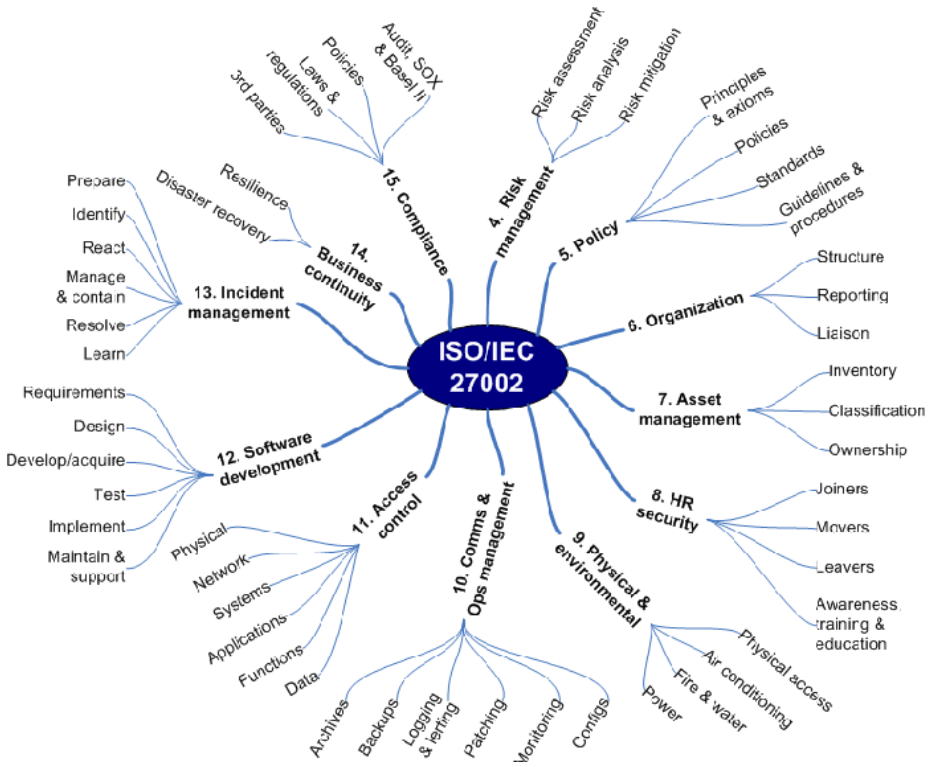


Figura 2.2.4 – ISO 27002

As secções a ter em conta na protecção da segurança da informação vão desde a gestão do risco, a sua avaliação e análise na óptica da minimização, passando pela Politica da Organização, cabendo neste âmbito, à gestão defini-la, no sentido de fazer uma declaração clara das directivas chave a serem levadas em consideração no que diz respeito à segurança da informação. Esta declaração deverá ser emanada para toda a organização, normalmente elaborado sob a forma de um Manual de Políticas de Segurança da Informação, traduzindo num conjunto de regras de segurança da informação, procedimentos e linhas condutoras.

Na secção relativa à Organização, há a ter em consideração, a Organização Interna, no âmbito da qual deverá existir um trabalho base executado no seio da organização, definindo papéis e responsabilidades no âmbito da segurança da informação. O acesso às Tecnologias de Informação deverá ser autorizado, deverão existir acordos de confidencialidade adequados às necessidades da organização, entre outros. Neste campo, será de ter em consideração a intervenção externa, e assim, não negligenciar a intervenção dos agentes externos como fornecedores e clientes em todo o processo.

A gestão do activo - informação, deverá partir do conhecimento pleno da informação que a organização detém, isto é, deverá existir um inventário actualizado dos activos neste campo descrevendo claramente a sua localização e quem os detém. Para além disto, a informação deverá estar devidamente classificada e etiquetada.

Relativamente à segurança dos recursos humanos, a norma preconiza que deverão ser tidas em consideração as responsabilidades pela segurança no momento das contratações, sejam elas permanentes ou não, devendo a organização promover um esquema de gestão de acessos. Importante ainda será manter actividades de formação no âmbito da segurança, e ter atenção ao pessoal que sai da empresa, bem como às alterações de responsabilidade dentro da mesma.

A segurança física dos equipamentos é ainda um ponto a ter em atenção salvaguardando acidentes ou danos intencionais que possam vir a sofrer, mantendo áreas de segurança com controlo de acesso e tentando minimizar o risco de acidentes através de equipamentos de segurança adequados.

Na comunicação e gestão das operações, a norma define que as responsabilidades no âmbito operacional das Tecnologias de Informação deverão estar documentadas, bem como deverão ser controladas as alterações em termos de acesso a estas tecnologias, devendo existir segregação de acessos. A considerar ainda a segurança da informação relativamente ao exterior, tais como possíveis trocas de informação com terceiros ou o comércio electrónico.

Importante também a manutenção de cópias de segurança de rotina, bem como a monitorização e criação de um sistema de alarme, de forma a identificar utilizações não autorizadas. O acesso aos sistemas e dados deverá ser controlado no intuito a prevenir a sua utilização não autorizada, nomeadamente através da criação de perfis de acesso, e da atribuição de direitos de acesso de modo formalmente controlado.
Também são referidos nesta norma os aspectos a ter em consideração relativamente à aquisição, desenvolvimento e manutenção dos Sistemas de Informação, tendo em atenção os requisitos de segurança exigíveis.

Por outro lado, deverá ser tido em consideração que os incidentes e fraquezas detectados na segurança da informação deverão ser prontamente reportados à gestão, de forma a promover a melhoria constante do sistema.

A continuidade do negócio é abordada na óptica da relação existente entre o planeamento da recuperação de incidentes no sistema de tecnologia da informação e a continuidade do negócio.

O cumprimento das normas legais aplicáveis por parte da organização é também considerado.

No final dos anos 80, o Governo britânico desenvolveu o ITIL, que em meados da década de 90 veio a ser reconhecido como um padrão para a gestão de serviços. No fundo, constitui um conjunto de boas práticas a serem implementadas na gestão dos serviços de informação. A presente abordagem focaliza-se essencialmente no cliente e na qualidade dos serviços de tecnologias de informação, numa óptica de relação do custo do serviço de tecnologia e a criação de valor estratégico para o negócio.

Neste âmbito, será possível obter, através de processos padronizados de gestão do ambiente de Tecnologias de Informação, uma relação adequada entre custos e níveis de serviços prestados na área das tecnologias de informação.

A ITIL traz algumas mudanças de paradigma, na medida em que o enfoque passa a ser no valor e não no custo e neste contexto segue a cadeia que leva à prestação do serviço, analisando os processos e pessoas e não apenas a tecnologia. Em Maio de 2007, foi lançado o ITIL V3 constituído por 26 processos e funções. Os processos do ITIL podem ser subdivididos em Gestão de Aplicações; Gestão de Serviços; e Gestão de Infra-estrutura de TI.

A grande novidade está essencialmente ao nível da Gestão de Serviços que contém a maioria dos processos definidos pelo ITIL, tendo como principal objectivo a certificação de que os serviços de TI são coerentes com as necessidades do negócio da empresa. Neste âmbito, os processos estão subdivididos em dois grupos:

● Entrega de Serviço que contém a gestão dos níveis de Serviços, gestão da Disponibilidade e Continuidade do Serviço;

● Suporte de Serviços, ou seja, a gestão dos incidentes e o apoio ao serviço.

Como já referido anteriormente, em ambientes tecnológicos complexos, a auditoria ganha uma nova dimensão.

Em particular, as Normas técnicas de Revisão/Auditoria da OROC, no seu parágrafo 13 chamam a atenção para a necessidade do revisor/auditor avaliar o sistema de controlo interno, referindo em particular a necessidade de ter em consideração a forma como os sistemas informatizados afectam o trabalho do revisor/auditor.

Segundo Weber, citado por José António Oliveira no livro "Método de Auditoria a Sistemas de Informação", *"o reconhecimento da necessidade de uma Auditoria a Sistemas de Informação tem origem em dois pressupostos:*
- os computadores afectam a capacidade dos auditores para a realização de auditoria;

- tanto a gestão da organização como a gestão dos sistemas de informação reconheceram que os computadores são recursos valiosos que necessitam de ser controlados como qualquer outro recurso dentro da organização"

E assim, José António Oliveira, propõe a seguinte estrutura de organização do processo de auditoria de SI:

1. Planeamento da auditoria;
2. Avaliação do controlo interno (avaliação e testes dos controlos gerais; e avaliação e testes dos controlos das aplicações)
3. Testes substantivos;
4. Relatório

O planeamento da auditoria, sendo essencial e determinante para o seu sucesso não é estático, antes deverá ser adaptado no decurso da mesma. A natureza, extensão e duração do planeamento dependem, numa primeira fase, da dimensão e complexidade organizacional da entidade, e numa segunda fase do conhecimento que o auditor obtém da mesma.
De acordo com a OROC, no ponto 15 das Normas técnicas de Revisão/Auditoria: *"O revisor/auditor deve planear o trabalho de campo e estabelecer a natureza, extensão, profundidade e oportunidade dos procedimentos a adoptar, com vista a atingir o nível de segurança que deve proporcionar e tendo em conta a sua determinação do risco da revisão/auditoria e a sua definição dos limites de materialidade."*

De acordo com o definido no "Código de Ética e Normas de Auditoria" do INTOSAI, *"O exame e a avaliação do controlo interno devem ser realizados segundo o tipo de auditoria."*
Para a avaliação do Controlo Interno, é essencial o conhecimento, por parte do auditor, das regras, procedimentos e objectivos da organização.
Ainda segundo José António Oliveira, a avaliação neste âmbito deverá partir do geral para o particular, isto é, partindo da análise de um departamento para a avaliação das suas secções.
Neste campo existe ainda uma nota relevante, os objectivos do Sistema de Controlo Interno são independentes da presença de sistemas de informação, no entanto os procedimentos adoptados pela organização, estes sim são afectados pela existência de sistemas de informação e consequentemente afectam a abordagem realizada no âmbito da auditoria.
Esta avaliação do Controlo Interno contempla a avaliação e testes de controlos gerais que no contexto dos sistemas de informação e de acordo com o mesmo autor *"criam o ambiente no qual as aplicações informáticas trabalham e ajudam a assegurar que funcionam de forma apropriada"*. Sendo que a eficácia dos controlos gerais, relacionados com as instalações informáticas e com os sistemas, determina em grande parte a eficácia dos controlos das aplicações, estes relacionados com as aplicações informáticas.
A realização de testes substantivos é preconizada em duas fases, na primeira dever-se-á avaliar a fiabilidade dos dados utilizados no âmbito da auditoria, enquanto na segunda dever-se-á proceder ao teste dos dados.

Diversos organismos que tutelam a actividade de auditoria desenvolveram um trabalho normativo nesta área.
As normas do INTOSAI estipulam que "*Quando a contabilidade ou outros sistemas de Informação estão informatizados, o auditor deve verificar se o controlo interno funciona correctamente, de modo a garantir a exactidão, fiabilidade e integridade dos dados."*

A Linha Directriz Europeia Relativa à Aplicação das Normas de Auditoria da INTOSAI, número 22, trata da metodologia a utilizar na auditoria dos sistemas de informação, no intuito de *"fornecer as orientações necessárias ao auditor generalista, familiarizado com os temas e métodos de auditoria dos SI, capaz de executar tarefas simples de auditoria dos SI e de recorrer a auditores especialistas em SI para realizar os objectivos gerais de auditoria"*

Ainda segundo Oliveira, *"Com o crescente número de tecnologias emergentes, os auditores sentiram-se incapazes de estar a par do vasto número de potenciais assuntos técnicos de auditoria e, portanto, impotentes para fornecerem uma avaliação especializada dos tópicos que tentam auditar"* e assim num contexto de Auditoria a Sistemas de Informação, *"…,sendo a auditoria executada por auditores orientados para a gestão. Se for necessário examinar em profundidade algum aspecto tecnológico do sistema informático, a entidade que realiza a auditoria deverá considerar a possibilidade de recorrer à ajuda de especialistas das áreas a examinar."*

De acordo com José Maria Pedro no seu documento "Standards internacionais relacionados com controlo interno na perspectiva dos sistemas de informação", *"Os processos e os dados a auditar estão agora no centro de um conjunto de círculos tecnológicos constituídos por hardware, software de sistema, software aplicacional, redes de comunicação de dados e finalmente os próprios utilizadores dos sistemas. Cada um destes círculos pode condicionar a eficácia do controlo interno das organizações."* Carecendo portanto, cada um destes domínios de controlos específicos.

Esta ideia foi esquematizada pelo mesmo autor na figura que se segue:

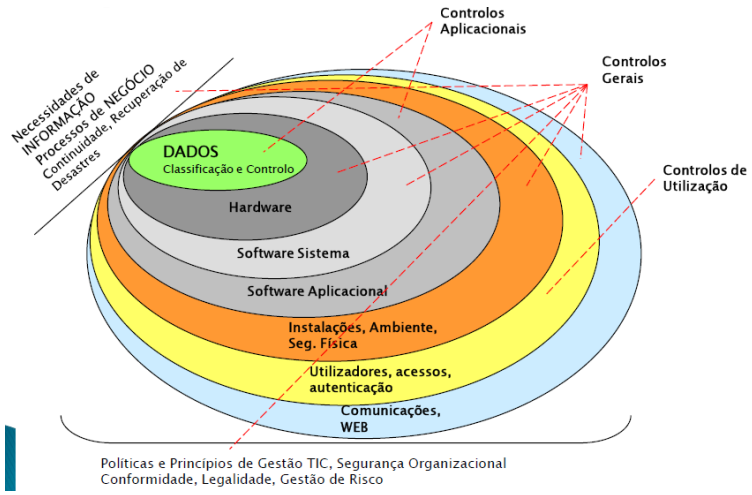


Figura 2.2.5 – Documento "Auditoria a Sistemas de Informação" – José Maria Pedro

No âmbito Organizacional, abrangendo os processos de funcionamento da empresa no contexto dos sistemas de informação, enquadrados pelas políticas e princípios de gestão definidos pela empresa, existem os Controlos Gerais a serem implementados de forma a analisar os procedimentos nesta área. No âmbito dos dados, hardware e

software dos sistemas de informação, há a considerar os controlos aplicacionais, que visam avaliar da eficiência e eficácia de aplicação dos recursos no tratamento da informação de forma a possibilitar que esta esteja acessível e capaz de servir as necessidades da Organização.

Ao nível dos utilizadores deverão existir os controlos de utilização. Numa era de acesso fácil à informação, este tipo de controlo visa avaliar a segurança na utilização da informação, a forma como são cedidos e segregados os acessos aos diversos níveis de utilização da mesma.

Neste contexto, José Maria Pedro descreve, de acordo com as metodologias dos CISA, seis domínios relevantes em termos da auditoria de sistemas de informação:

Gestão, Planeamento e Organização dos SI: Avaliar a estratégia, políticas, standards, procedimentos e práticas relativas à gestão, planeamento e organização dos sistemas de informação.
Infra-estrutura Tecnológica e Práticas Operacionais: Avaliar a eficácia e eficiência da implantação e gestão corrente da infra-estrutura tecnológica e práticas operacionais para atestar que suportam adequadamente os objectivos de negócio da organização.
Protecção de Activos de Informação: Avaliar a segurança da infra-estrutura de software e ambiental nas tecnologias de informação para certificar que satisfaz os requisitos organizacionais de negócio e salvaguarda os activos de informação contra uso não autorizado, divulgação, modificação, danificação e perda. Uma vez que a crescente facilidade de comunicação e de acesso a redes e sistemas tornou este domínio vital para as organizações.
Recuperação de Desastres e Continuidade de Negócio: Avaliar o processo para desenvolvimento e manutenção de planos documentados, comunicados e testados para a continuidade das operações de negócio e do processamento de sistemas de informação em casos inesperados de falha de funcionamento.
Desenvolvimento de Sistemas Aplicacionais, Aquisição, Implantação e Manutenção: Avaliar a metodologia e processos pelos quais o desenvolvimento de sistemas aplicacionais, aquisição, implantação e manutenção são levados a cabo, para certificar que cumprem os objectivos de negócio da organização.
Avaliação de Processos de Negócio e Gestão de Risco: Avaliar os sistemas de negócio e processos para assegurar que os riscos são geridos de acordo com os objectivos de negócio da organização.

O IIA – The Institute of Internal Auditors preparou e editou um Guia de Auditoria intitulado Global Technology Audit Guide, uma publicação direccionada para as questões relacionadas com as tecnologias de informação. Esta publicação contém diversas regras das quais destacamos:

A GTAG 1 (Global Technology Audit Guide 1), que diz respeito a Controlos das Tecnologias de Informação e que trata assuntos como o controlo das Tecnologias de informação, análise do risco, monitorização e técnicas, contém um guia dos tópicos, que no âmbito das tecnologias de informação, têm impacto ao nível do controlo e das práticas de auditoria.

A GTAG 4 aborda o tema da Gestão das Auditorias a Sistemas de Informação, este referencial fornece uma ajuda para delinear a estratégia no planeamento da auditoria, alertando para o facto de este dever ser feito em consonância com o Risco que a entidade apresenta.

A GTAG 7 foca o tema do Outsourcing nas Tecnologias de Informação, transmitindo a ideia de que os benefícios desta modalidade são acompanhados da necessidade de gerir a complexidade de riscos e desafios que a acompanham. É feita uma chamada de atenção para a importância dos auditores internos perceberem o contexto do outsourcing. Este guia fornece informação dos tipos de actividades em outsourcing existentes no âmbito das Tecnologias de informação, o seu ciclo de vida, e como podem ser geridas no âmbito do risco, sistema de controlo, e da gestão da empresa.

A GTAG 12 tem a ver com a Auditoria a Projectos de Tecnologias de Informação, fornecendo um resumo das técnicas a serem levadas a cabo de forma a avaliar os riscos relacionados com os projectos de TI.

Finalmente a GATG 15 focaliza-se no tema Gestão da Segurança da Informação, partindo da consciência de que a informação é uma componente importante na estratégia competitiva da maioria das organizações. Este trabalho pretende ser um guia para possibilitar a inclusão de uma auditoria à segurança da informação no âmbito dos planos de auditoria.

Capitulo 3 – Metodologia e Dados

Entendemos como pertinente abordar o Tema do Controlo Interno num ambiente de Sistemas de Informação em duas vertentes:

- No contexto do **Ensino Superior** - a forma como o sistema de ensino Superior consagra esta temática.
- Nas Empresas - a forma como as empresas em Portugal concebem os seus Sistemas de Controlo Interno, à luz dos standards internacionais.

3.1 – Ensino Superior

A Metodologia utilizada para a análise deste Tema no contexto do ensino superior foi a seguinte:

1. Partimos da Listagem de Escolas Públicas (Universidades e Politécnicos) - o estudo foi limitado ao Ensino Superior público, por o considerarmos representativo do universo do Ensino Superior em termos de conteúdos programáticos nesta área.
2. Foi efectuada pesquisa dos cursos – Licenciaturas; Mestrados e Pós-Graduações - que poderão ter no seu âmbito este tema: Gestão/Contabilidade/Auditoria/Sistemas de Informação/ Informática de Gestão, foram os cursos seleccionados.
3. O Universo ficou então definido como 44 Licenciaturas; 35 Mestrados e 7 Pós-Graduações – Anexo I.
4. Foi efectuada consulta do Plano Curricular para cada um dos cursos – nos casos em que se encontrava disponível na internet, com selecção das disciplinas que poderiam focar estes temas.
5. Consulta do conteúdo programático, para os casos em que se encontra disponível na internet, das referidas disciplinas, aferindo se focam de 3 pontos, considerados por nós, básicos.
    i. Controlo Interno
    ii. Sistemas de Informação contextualizado na Organização
    iii. Segurança dos Sistemas de Informação
6. Nos casos em que o conteúdo programático não estava disponível nos sites das respectivas instituições de ensino, foi solicitada essa informação por correio electrónico, directamente e por ordem de preferência, ao responsável da

disciplina em apreciação, ao responsável do curso em causa ou, no caso de não existir o contacto de nenhuma destas entidades, ao estabelecimento de ensino. Nem todas responderam.

7. Assim o nosso estudo ficou limitado a elementos relativos a 33 Licenciaturas, 27 Mestrados e 5 Pós-graduações – Anexo II.

8. Os dados recolhidos são então apresentados sob a forma qualitativa, isto é, para cada parâmetro analisado teremos uma valor S ou N, consoante a disciplina no seu conteúdo programático cubra ou não o assunto em apreço. Teremos assim, apenas três variáveis, que assumirão o valor S ou N, são dados nominais ou categóricos.

9. Os referidos dados foram objecto de tratamento de acordo com os seus atributos.

    - A análise foi estratificada por grau de ensino.
    - Os resultados foram analisados para cada curso, se as disciplinas seleccionadas, no seu conjunto, focavam um, dois ou a globalidade dos temas em apreço.
    - Temos então uma proporção de cursos para cada Grau de ensino que abrangem as áreas em estudo.
    - Foi ainda realizada uma análise sintética do conjunto dos cursos estudados.

3.2 - Empresas

1. Definição do inquérito.

2. Selecção do Universo de empresas alvo de inquérito - o Universo entendido como relevante para o presente estudo foi a Lista Indicativa de Entidades de Interesse Público e destas, considerada uma amostra das entidades emitentes de valores mobiliários.

3. Pretendeu-se aferir da adopção ou não dos modelos internacionalmente definidos e genericamente aceites na área em estudo.

4. Partindo do Universo acima descrito, foi seleccionada uma amostra com base na referida listagem – Amostra constituída por 29 empresas – Anexo IV.

5. Foi enviado o inquérito directamente às empresas através de correio electrónico, tendo sido realizadas diversas insistências pela mesma via e tendo

sido efectuado contacto telefónico nos casos em que não se obteve resposta da forma inicial.

6. Foram recepcionadas 10 respostas, e procedeu-se então ao tratamento estatístico dos resultados, que não tendo sido um grau de resposta elevado possibilitou verificar à partida uma tendência - Anexo V.

7. Os dados recolhidos são apresentados na forma qualitativa, isto é, para cada parâmetro analisado teremos uma valor S ou N, são dados nominais ou categóricos.

   Basicamente o inquérito é repartido em dois campos, numa primeira fase procura-se perceber qual a preocupação das empresas com o Controlo Interno no âmbito dos Sistemas de Informação e qual o referencial seguido. Numa segunda fase o inquérito é voltado para o Tema Auditoria a Sistemas de Informação.

8. O tratamento dado à informação recolhida espelha a repartição existente no inquérito realizado.
   - Aferir se existe especial preocupação com o Controlo Interno no âmbito dos Sistemas de Informação.
   - Existindo, qual o referencial ou referenciais que utilizam no tratamento destes processos.
   - Auditoria aos Sistemas de informação, é realizada ou não, por quem e com que periodicidade.

Capitulo 4 – Análise dos Resultados

4.1 – Análise da forma como o Ensino Superior aborda este tema

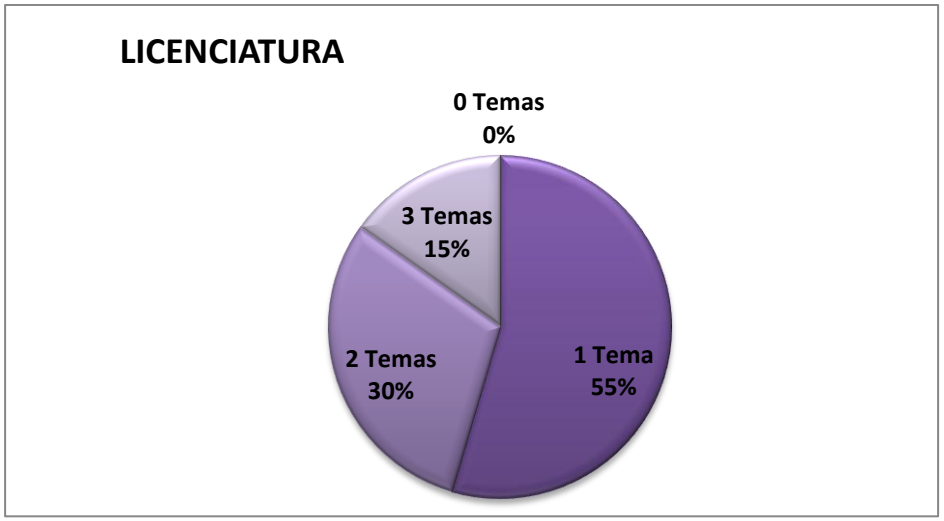
De acordo com a Metodologia descrita, o Universo objecto de estudo foram 44 Licenciaturas; 35 Mestrados e 7 Pós-Graduações. Destas obtiveram-se elementos relativos a 33 Licenciaturas, 27 Mestrados e 5 Pós-graduações.

Os Resultados do Estudo são resumidos no Quadro 1 que se segue:

Quadro 4.1.1: Síntese de Resultados por Grau de Ensino

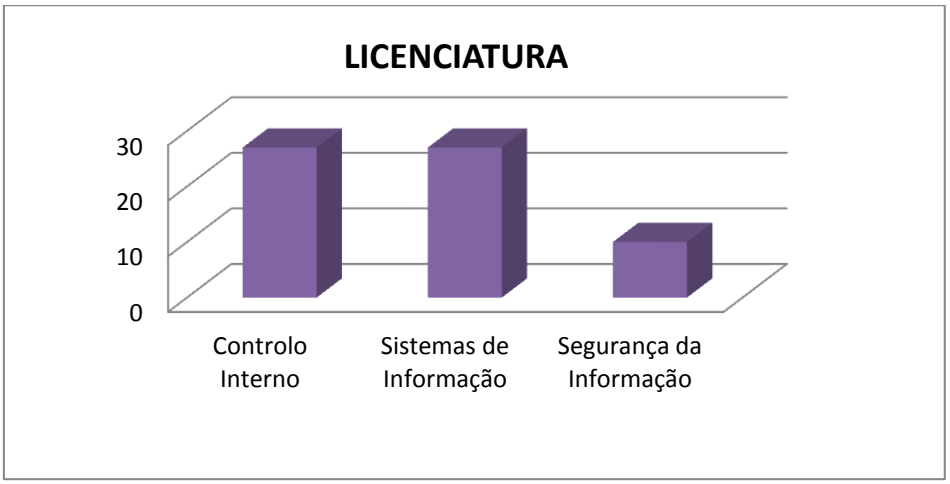
Licenciatura	Nº de Cursos	%	Mestrado	Nº de Cursos	%	Pós -graduação	Nº de Cursos	%
0 Temas	0	0%	0 Temas	2	7%	0 Temas	0	0%
1 Tema	18	55%	1 Tema	10	37%	1 Tema	2	40%
2 Temas	10	30%	2 Temas	7	26%	2 Temas	1	20%
3 Temas	5	15%	3 Temas	8	30%	3 Temas	2	40%
TOTAL	33		TOTAL	27		TOTAL	5	

Gráfico 4.1.1: Resultados Licenciatura – Número de Temas abordado por curso



No grau de ensino de Licenciatura, 55% apenas abordam um dos temas objecto do estudo, 30% cobrem 2 dos aspectos em análise e apenas **15% das Licenciaturas abrangem a globalidade dos aspectos**. Assim, neste grau de ensino, a maioria dos cursos (85%) aborda apenas um ou dois dos temas objecto deste estudo, maioritariamente o Controlo Interno e os Sistemas de Informação no contexto da Organização.

Gráfico 4.1.2: Resultados Licenciatura – Frequência de abordagem por tema



Analisando os Mestrados, 30% dos Cursos estudados cobrem a totalidade dos temas, e 7% não abordam nenhuma das matérias. Também neste grau de ensino a maioria dos cursos (63%) abrange nos seus conteúdos programáticos 2 dos temas, se bem que a este nível de ensino existe um claro incremento do número de cursos que abordam os 3 temas. Em particular os temas Controlo Interno e Sistemas de Informação no contexto das Organizações são os temas mais amplamente focados no âmbito dos Mestrados.

Gráfico 4.1.3: Resultados Mestrado – Número de Temas abordado por curso

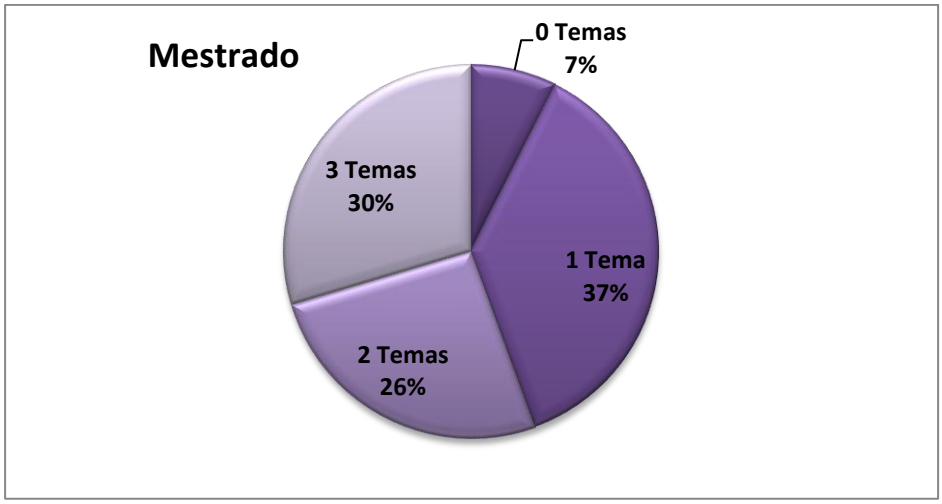
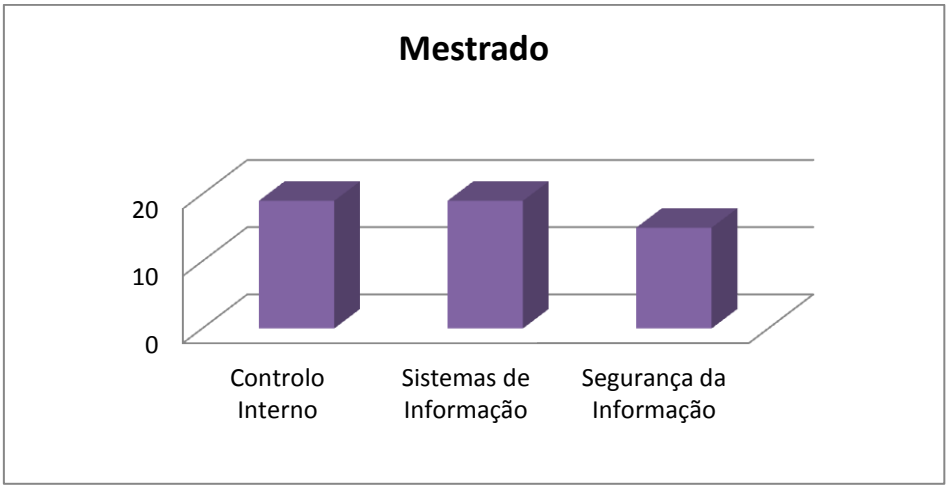


Gráfico 4.1.4: Resultados Mestrado – Frequência de abordagem por tema



No que diz respeito às Pós-graduações, 40% cobrem a totalidade dos temas, os mesmos 40% para as que apenas abordam um dos temas.

Mais uma vez o Tema Controlo Interno é o tema maioritariamente abordado no contexto do Ensino superior.

Gráfico 4.1.5: Resultados Pós-Graduação – Número de Temas abordados por curso

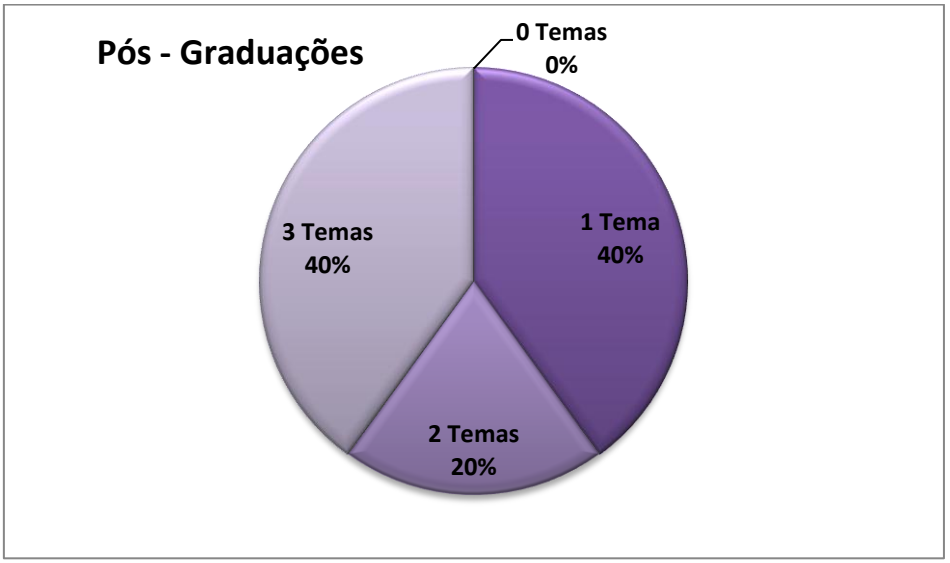
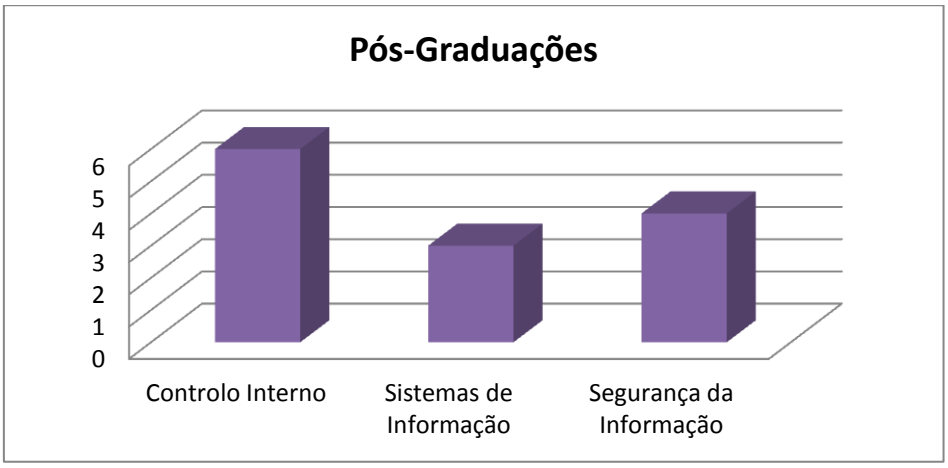


Gráfico 4.1.6: Resultados Pós-Graduação – Frequência de abordagem por tema

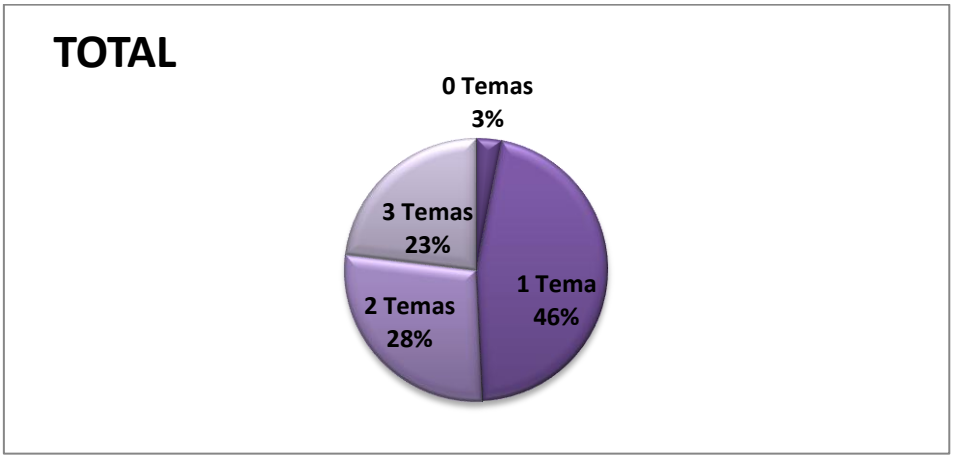


Na análise global dos valores obtidos, as conclusões são similares às extraídas anteriormente por Grau de Ensino, grande parte dos cursos analisados apenas aborda um dos temas em estudo, e a grande maioria aborda um a dois dos temas, 73%. Genericamente, dos 63 cursos analisados, apenas 15 abrangem no seu plano curricular a totalidade dos temas objecto de análise, isto é cerca de 23% da totalidade de cursos estudados fazem uma cobertura da generalidade dos temas em estudo.

Quadro 4.1.2- Síntese Total dos Resultados – Número de Temas de abordado por Curso

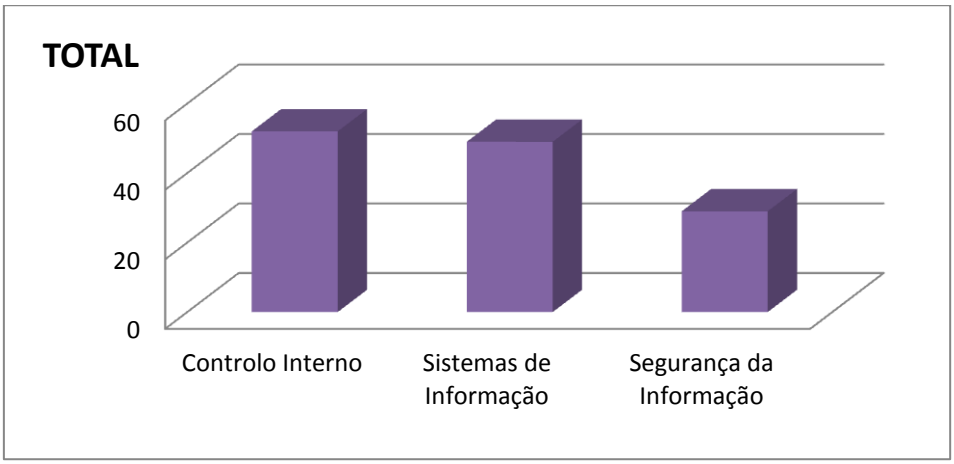
Nº de Temas Aborados	Nº	Percentagem
0 Temas	2	3%
1 Tema	30	46%
2 Temas	18	28%
3 Temas	15	23%
	65	100%

Gráfico 4.1.7: Resultados no Total – Número de Temas de abordado por Curso



No âmbito dos cursos analisados maioritariamente são abordados os temas Controlo Interno e Sistemas de Informação no Contexto da Organização. Sem excepção, o tema Segurança da Informação é o menos frequentemente estudado.

Gráfico 4.1.8: Resultados no Total – Frequência de abordagem por tema



Secção 4.2 – Análise da forma como as empresas em Portugal concebem os seus sistemas de Controlo Interno, à luz dos standards internacionais.

Das 29 empresas objecto de inquérito, 10 responderam ao pedido de informação.

Será de notar que apenas 37% das empresas inquiridas responderam, mesmo após insistência por diversos meios. Não podemos ignorar que se trata de um assunto sensível em termos de gestão e que portanto para muitas das entidades se torna mais cómodo não responder.

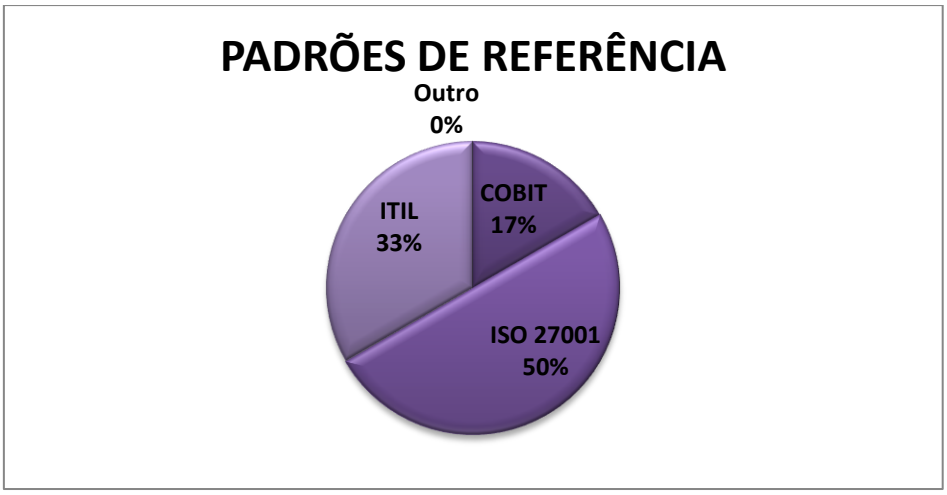
Relativo ao item no qual se pretende aferir, no âmbito do controlo interno da existência de preocupação especial com os Sistemas de Informação, temos 90% das entidades com resposta afirmativa, transparecendo de facto que existe a consciência da importância deste assunto.

Neste contexto, interessou-nos saber qual/quais o/os referencial/referenciais utilizado(s) pela Organização para trabalhar este aspecto. O resultado é sintetizado no Quadro que se segue:

Quadro 4.2.1: Síntese do Inquérito – Controlo Interno e sistemas de informação

1. Controlo Interno. Existe especial preocupação c/ SI?	2. Quais os padrões de Referência?			
	COBIT	ISO 27001	ITIL	Outro
9	2	6	4	0

Gráfico 4.2.1: Repartição de Padrões de Referência



Das respostas obtidas, 90% das empresas admite ter esta preocupação. O padrão maioritariamente seguido é a ISO 27001, no entanto será de notar que algumas das empresas analisadas admitem utilizar como referência mais do que um dos padrões apresentados. Nenhuma indicou outro padrão que não o indicado pelos autores do questionário.

Quadro 4.2.2: Quadro Síntese do Inquérito - Auditoria

	Por quem é realizada a auditoria?			Auditoria Externa. É realizada por:	
É Realizada Auditoria aos SI?	Aud. Interna	ROC (CLC)	Aud. Externa	Aud. Inf. Especializado	Outro
7	2	0	5	5	0

Das empresas que admitem existir uma preocupação especial com os Sistemas de informação no âmbito do Controlo Interno, 77% realizam Auditorias aos Sistemas de Informação, estas maioritariamente realizadas por Auditores Externos Especializados.

Gráfico 4.2.2: Repartição – Entidade que realiza a auditoria

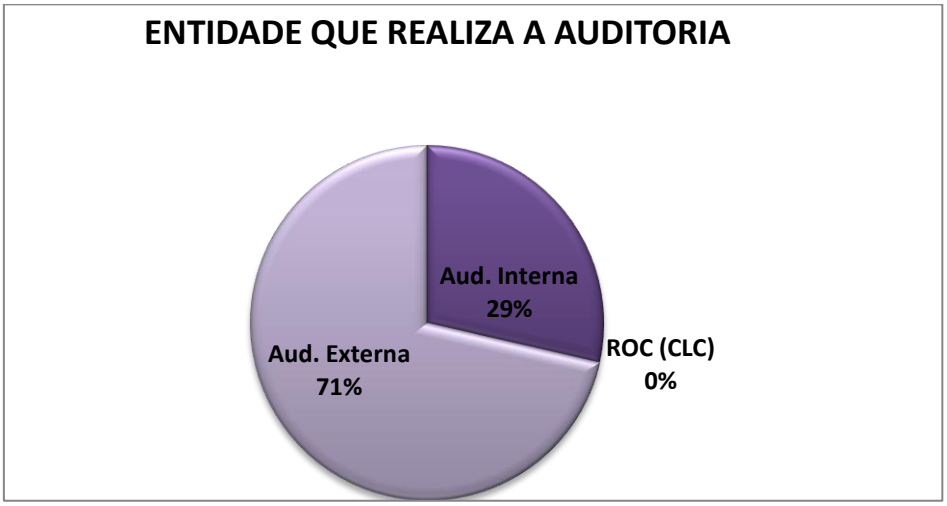
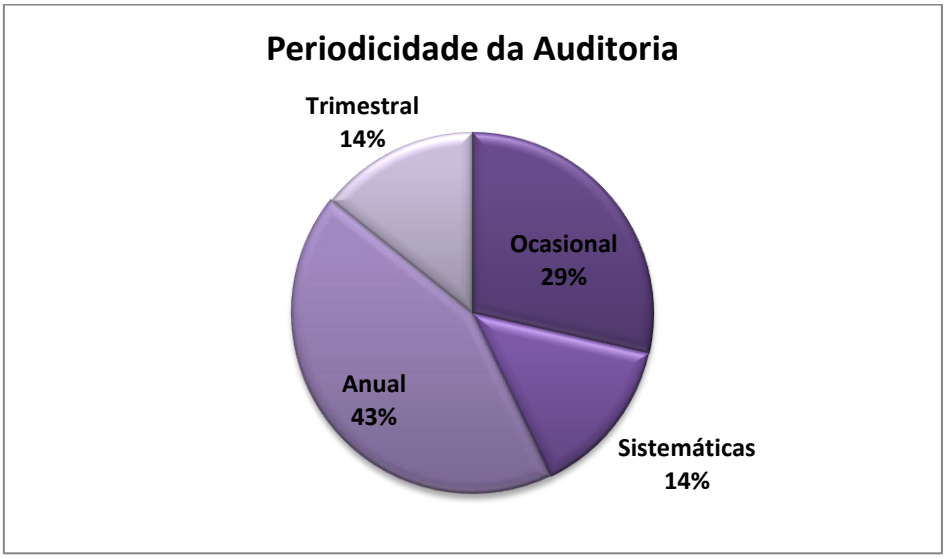


Gráfico 4.2.3: Periodicidade de realização da auditoria



Nas empresas em análise, a Auditoria aos Sistemas Informáticos, é maioritariamente executada com periodicidade anual 43%, em 29% dos casos estas Auditorias são executadas de forma ocasional.

Capitulo 5 – Conclusões, Contributos, Limitações e Investigação futura

5.1 – No contexto do Ensino Superior

Globalmente os resultados obtidos corroboram as nossas expectativas, ou seja, constata-se que pouco frequentemente os temas por nós considerados como chave nesta matéria, são analisados em simultâneo nos planos curriculares dos cursos em estudo. Esta é, portanto, ainda uma área pouco explorada ao nível do Ensino Superior. Os temas, Controlo Interno; Sistemas de Informação e Segurança da Informação apenas em 24% dos casos são abordados no mesmo curso.

Como seria expectável, essa abordagem simultânea é mais frequente nas pós-graduações e mesmo ao nível do Mestrado e menos frequente ao nível da Licenciatura, apenas 16%, uma vez que este grau de ensino quer-se mais generalista e os seguintes mais especialistas em determinadas áreas.

No entanto, há a ter em atenção o facto de, mesmo numa área que se pretende especialista, esta matéria ser abordada em menos de metade dos cursos analisados, o que se poderá reflectir futuramente nas preocupações das empresas neste campo.

Os licenciados, mas essencialmente os pós-graduados e mesmo os mestres nestas áreas são os recursos humanos das nossas empresas, na maioria pequenas e médias empresas, pelo que seria interessante que eles pudessem entrar no mundo empresarial com a visão da interligação entre o Controlo Interno no seio de organizações crescentemente utilizadoras de Sistemas de Informação e a performance da organização. Esta situação tem, naturalmente, uma relação directa com o risco de mau funcionamento.

Este alerta poderá funcionar no tecido empresarial nacional, principalmente ao nível de pequenas e médias organizações que hoje, suspeitamos, ainda não aplicam estes conceitos de forma consistente.

O conhecimento prático da realidade empresarial nacional leva-nos a perceber como estes conceitos são incipientes e pouco desenvolvidos nestas organizações - Controlo Interno sim, algum existe certamente, mais numas áreas do que noutras, nem sempre conscientemente relacionados com uma análise de risco da organização, nem sempre devidamente adaptados.

O maior enfoque nestes temas a um nível generalista da formação universitária, certamente permitiria que estas organizações tomassem consciência destes assuntos.

As grandes empresas, essas apoiadas por especialistas, em maior ou menor grau, estão atentas a estes assuntos. Neste âmbito poderemos partir para a fase posterior deste estudo.

O estudo limitou-se a apreciar três tópicos específicos destes temas, todos eles considerados essenciais mas que em si mesmo não esgotam o tema.

O desenvolvimento futuro deste assunto poderá abordar outros temas relevantes nesta área, ou explorar melhor alguns dos temas já analisados, como o Risco, sendo possível analisar a abordagem do Risco em duas vertentes, o Risco de Auditoria no

contexto de Organizações crescentemente informatizadas e o Risco como elemento preponderante na definição dos Sistema de Controlo Interno no Contexto da Organização.

5.2 – No contexto Empresarial

Os resultados obtidos no presente estudo são representativos do Universo escolhido e da amostra seleccionada. Tratando-se de empresas emitentes de valores mobiliários, será expectável uma preocupação significativa com esta área. São sociedades que pelas suas características e dimensão têm de recorrer a profissionais especialistas na área, conhecedores da matéria e conscientes da importância do Sistema de Controlo Interno adequado para o sucesso da empresa.

Neste ambiente de necessidade de implementar e manter um Sistema adequado, torna-se então inevitável enquadrar os Sistemas de informação como uma componente básica e essencial no funcionamento da Organização e portanto um elemento chave ao nível do Controlo Interno da mesma.

O referencial utilizado diverge, em algumas das organizações estudadas, existindo mesmo uma confluência de vários referenciais numa mesma Organização. A maior apetência para a utilização da ISO 27001 poderá ter a ver com a possibilidade de Certificação no âmbito desta norma.

Podemos, portanto, concluir que ao nível destas empresas existe a consciência da proeminência deste tema para o sucesso na concretização dos objectivos delineados para a organização.

As limitações que se poderão apresentar a este estudo têm a ver com a escolha do Universo, e consequentemente, a escolha da amostra para trabalho, que no seu essencial não é representativa do tecido empresarial nacional, nem foi isso o pretendido, representa apenas a realidade de uma parte restrita das empresas nacionais – as que têm maior impacto para os utilizadores externos da informação.

Existiu a preocupação de assegurar que o inquérito fosse transversal, abrangendo um leque alargado de sectores, contudo foi excluído à partida um ramo de actividade, o sector financeiro – banca e seguros que foram retirados da amostra deliberadamente por serem sectores onde normalmente existe uma maior preocupação neste domínio, nomeadamente na segurança dos sistemas de informação. São sectores que estão mais conscientes deste tema, desenvolvendo departamentos de auditoria interna que dedicam especial atenção a estes temas.

Neste encadeamento, surgem diversas possibilidades para o desenvolvimento futuro deste tema, o que poderá passar por considerar o universo de empresas nacionais, alargando o inquérito a entidades de menor dimensão, ou, numa outra vertente, estudar especificamente um ramo de actividade, ou ainda, em alternativa, analisar empresas de dois ou mais ramos de actividade e comparar os resultados entre si.

BIBLIOGRAFIA

- CMVM. (2010). Código de Governo das Sociedades da CMVM, Lisboa; Portugal: 2010.
- CNSA. Lista Indicativa de entidades de Interesse Público - http://www.cnsa.pt
- COBIT. (2000). Framework, 3rd Edition, COBIT Steering Committee and IT Governance Institute.
- COSO. (1992). Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission.
- COSO. (2004). Enterprise Risk Management – Integrated Framework. Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission.
- Costa, Carlos Baptista. (2010). Auditoria Financeira. Rei dos Livros.
- FEE. (2003). Discussion Paper on the Financial Reporting and Auditing Aspects of Corporate Governance; Bruxelas, Bégica.
- FEE. (2005). Risk Management and Internal Control in the EU – Discussion Paper; Bruxelas, Bégica
- FEE. (2009). Discussion Paper for Auditor's Role Regarding Providing Assurance on Corporate Governance Statements; Bruxelas, Bégica.
- Governo. (2007). Decreto-lei nº300/2007. Lisboa, Portugal. Diário da República: Imprensa Nacional – Casa da Moeda.
- Governo. (2007).Resolução do Conselho de Ministros nº49/2007
- Haynes, Rick S., Schilder, Arnold. (1998). Principles of Auditing an International Perspective; compilated outline.
- IFAC. (2005) Internal Controls – A Review of Current Developments – Information Paper; New York, International Federation of Accountants.
- IFAC. (2006). Internal Controls – A review of Current Developments; New York, International Federation of Accountants.
- IFAC.(2009) ISA 265
- International Organization for Standartization. (2005) ISO/IEC 27001,
- INTOSAI. (1998). Código de Ética e Normas de Auditoria; Estocolmo; Suécia; Comissão de Normas de Auditoria.
- INTOSAI. Guidelines for Internal Control Standards for the Public Sector; INTOSAI Internal Control Standards Subcommittee, Bruxelas, Bélgica.
- IT GI - IT Governance and Process Maturity
- Oliveira, José António. Método de Auditoria a Sistemas de Informação. Porto Editora
- OROC. (2000). Directriz de Revisão/Auditoria 410 - Controlo Interno.

- OROC. (2009). A Adopção das Normas Internacionais de Auditoria da IFAC, Lisboa, Portugal: Revisores e Auditores.
- Pedro, José Maria .Auditoria de Sistemas de Informação – apresentação ao curso de Auditoria e Fiscalidade do IPT.
- Pedro, José Maria. (2010). Standards internacionais relacionados com controlo interno na perspectiva dos sistemas de informação. Sinais de Inovação nas Metodologias de Controlo, Inspecção-Geral de Finanças.
- Ratcliffe,Thomas A.; Landes, Charles E. (2009). Understanding Internal Control and Internal Control Services; New York, AICPA
- Sabarnes- Oxley Act; July 30, 2002; United States of America.
- Silva, Artur Santos; Vitorino, António; Alves, Carlos Francisco; Cunha, Jorge Arriada da; Monteiro, Manuel Alves. (2006). Livro Branco sobre Corporate Governance em Portugal. Instituto Português da Corporate Governance.
- Tribunal de Contas Europeu. Linhas Directrizes Europeias Relativas à Aplicação das Normas de Auditoria da INTOSAI nº 21 e nº22
- Tribunal de Contas. (1999). Manual de Auditoria e Procedimentos – Volume 1.