UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

TRABALHO DE LICENCIATURA

METODOLOGIA DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO
ESTUDO DE CASO - INSPECÇÃO-GERAL DE FINANÇAS

Autor: José Alberto Cossa

Maputo, Abril de 2010

UNIVERSIDADE EDUARDO MONDLANE

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

TRABALHO DE LICENCIATURA

METODOLOGIA DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO
ESTUDO DE CASO - INSPECÇÃO-GERAL DE FINANÇAS

Autor: José Alberto Cossa

Supervisor: Dr. Zeferino Saugene

Maputo, Abril de 2010

DEDICATÓRIA

À memória do meu Pai, Alberto Ticuápa Cossa, pelo seu apoio em todos momentos de minha vida

À minha mãe, Albertina Manhengue e aos meus irmãos,

À minha filha Wene.

AGRADECIMENTOS

À DEUS, por tudo que pude realizar.

À Universidade Eduardo Mondlane, em especial os docentes e funcionários do Departamento de Matemática e Informática.

Ao meu supervisor, Dr. Zeferino Saugene, pelas críticas e apoio em ideias.

Ao dr. Mário Estêvão Xavier, pelos dez anos de luta.

Aos "*companheiros de batalha"* Elísio Anselmo, Diogo Lucas Chavana, Pascoal Chambe, José Matsinhe, Nelson Mazibe, e outros não mencionados pelo apoio moral e material nos momentos difíceis da nossa árdua formação.

Às Irmãs Missionarias da Consolata, pelo apoio moral e material.

Aos meus pais Alberto Ticuápa Cossa e Albertina Manhengue, pelo seu inquantificável apoio.

Aos meus irmãos João, Glória, Maria pelo apoio nos bons e maus momentos

A minha namorada Saquina Júlia, que sempre acreditou e incentivou-me a lutar.

Ao meu sobrinho Idaldêncio pela paciência nos momentos em que precisou do carinho do tio,

E a todos aqueles que não por má fé não foram aqui mencionados, mas que contribuíram para a minha formação.

EPÍGRAFE

"Feliz o homem que descobre a sabedoria e adquire inteligência! Pois adquiri-la vale mais do que a prata, e seu lucro mais que o ouro."

Provérbios 3, 13-14

DECLARAÇÃO DE HONRA

Declaro por minha honra, que este trabalho é resultado da minha investigação e que não foi submetido a outro grau que não seja o indicado – **Licenciatura em Informática** na Universidade Eduardo Mondlane.

Maputo, Abril de 2010

O Estudante

_____

(José Alberto Cossa)

RESUMO

Certamente que, enquanto não existiam sistemas informatizados, nunca se ouvira falar de auditoria de Sistemas de Informação, o espaço desta nova especialidade deve ser encontrado no contexto actual do desenvolvimento das tecnologias de informação e comunicação.

O presente trabalho propõe uma metodologia de auditoria baseada no referencial metodológico COBIT e padrões e normas de melhores práticas de auditoria, aplicáveis à Administração Pública. A metodologia permite avaliar os Sistemas de Informação quanto à sua integridade e segurança, bem como, quanto à sua eficácia e eficiência.

Foi igualmente realizado um estudo de modelos, padrões e normas de auditoria aplicáveis aos Sistema de Informação.

Como estudo de caso, apresentam-se considerações e análises sobre a Inspecção Geral de Finanças, que é um órgão do Ministério das Finanças, que tem por vocação efectuar auditoria às instituições do Estado com excepção do ramo do seguro e das instituições para – bancárias, contribuindo para a economia, a eficácia e a eficiência na obtenção das receitas e na realização das despesas públicas nacionais.

LISTA DE ABREVIATURAS E ACRÓNIMOS

MS ACCESS	Sistema de Gestão de Banco de Dados MS ACCESS
ACL	*Software* de Auditoria ACL
ACROBAT	*Software* usado para a troca e distribuição electrónica de documentação no formato PDF *(Portable Document Format)*
AICPA	*American Institute of Certified Public Accountants*
BSC	*Balanced Scorecard*
CAATS	*Computer Assisted Audit Techniques*
CBEAM	*Software* de Auditoria CBEAM
CISA	*Certified Information Systems Auditor*
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information and Related Technology*
COBRA	*Software* para Análise de Risco e Avaliação de Conformidade COBRA
DAE	Departamento de Auditoria às Empresas
DGA	Direcção Geral das Alfandegas
DGI	Direcção Geral dos Impostos
DIA	Departamento de Inspecção às Autarquias
DIOE	Departamento de Inspecção aos Órgãos do Estado e suas instituições
DITA	Departamento de Inspecção aos sectores Tributário e Aduaneiro
DRC	Delegação Regional Centro
DRN	Delegação Regional Norte
DSI	Departamento de Sistemas de Informação
DT	Departamento Técnico
EDPAA	*Electronic Data Processing Auditors Association Inc*
e-SISTAFE	Sistema informático de administração financeira do Estado
EXCEL	Folha de Cálculo EXCEL
IDEA	*Software* de Auditoria IDEA
IGF	Inspecção Geral de Finanças
IIA	Instituto Internacional de Auditores Internos
INFOCUS	*Software* de Auditoria INFOCUS
INTOSAI	Organização Internacional das Instituições Supremas de Auditoria

ISACA	Associação de Controlo e Auditoria de Sistemas de Informação
ISO	*International Organization for Standardization*
ITIL	*IT Infrastructure Library*
MF	Ministério das Finanças
MS PROJECT	*Software* de Planificação MS PROJECT
MY SQL	Sistema de Gestão de Banco de Dados MY SQL
ORACLE	Sistema de Gestão de Banco de Dados ORACLE
OUTLOOK	*Software* de Comunicação MS OUTLOOK
POWERPOINT	*Software* de Apresentação MS POWERPOINT
RA	Risco de Auditoria
RAF	Repartição de Administração e Finanças
RC	Risco de Controlo
RD	Risco de Detenção
RI	Risco Inerente
SI	Sistemas de Informação
SICR	Sistema Integrado de Cobrança de Receita
SISTAFE	Sistema de Administração Financeira do Estado
SPSS	*Software* de Estatística SPSS
SQL SERVER	Sistema de Gestão de Banco de Dados SQL SERVER
TA	Tribunal Administrativo
TDM	Empresa Telecomunicações de Moçambique
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação
TIMS	*Trade Information Management System*
VISIO	Programa de Desenho MS VISIO
WORD	Processador de Texto MS WORD

ÍNDICE

ÍNDICE DE FIGURAS E TABELAS

CAPITULO I: INTRODUÇÃO E METODOLOGIA

1. INTRODUÇÃO

Nos últimos tempos, tem se assistido a um enorme avanço ao nível das tecnologias de informação e comunicação, que se reflecte na circulação da informação, nos procedimentos contabilísticos e financeiros, no sistema de controlo interno, na produtividade dos organismos, na celeridade da prestação de serviços, na qualidade da imagem dos organismos perante o seu exterior. Entre outras vantagens, estas tecnologias tem produzido, no geral impacto bastante significativo nas instituições e em particular nos seus clientes.

Muitos destes avanços têm - se verificado com maior notabilidade no sector privado, contudo isso não significa que o sector público esteja alheio a estas transformações. Actualmente, a maioria das instituições da Administração Pública são gestoras ou usuárias de sistemas de informação informatizados.

A Inspecção Geral de Finanças (IGF) é o órgão de controlo superior financeiro do Estado e de apoio ao Ministro que superintende a área das Finanças na gestão dos fundos e controlo patrimonial públicos. Tem como atribuições fundamentais realizar o controlo da administração financeira do Estado, incumbindo-lhe o exercício do controlo nos domínios orçamental, financeiro e patrimonial, de acordo com os princípios da legalidade, regularidade e da boa gestão financeira, contribuindo para a economia, a eficácia e a eficiência na obtenção das receitas e na realização das despesas públicas nacionais.

A actividade que a IGF exerce, constitui actualmente um enorme desafio uma vez que a informação útil para auditar está a passar progressivamente a ser processado pelos sistemas de informação informatizados.

Deste modo, a linha de processamento dos dados que vai desde o momento em que o facto ocorre até ao(s) ponto(s) da utilização da informação resultante dos dados relevados, tornou-se mais complexa, mais rápida, mais curta e também mais perigosa para o auditor. Num ambiente informatizado, as

funções que antes estavam convenientemente segregadas por um conjunto de pessoas, podem estar (agora) aglutinadas num único programa cuja descrição funcional ou orgânica nunca foi escrita.

A opinião dos auditores precisa de ter uma base de informação fiável. E sabendo que a missão e atribuições da IGF dependem da obtenção de informação fiável junto das entidades auditadas, torna-se indispensável à IGF, além de analisar a informação fornecida, proveniente do processamento electrónico, avaliar também os sistemas de informação de modo a assegurar a sua fiabilidade e integridade.

Com o presente trabalho, pretende-se estudar a auditoria de Sistemas de Informação em uso na IGF e sua envolvente externa, com vista a contribuir com uma metodologia que facilitem à IGF a realização de auditorias aos sistemas de informação informatizados das instituições públicas.

1.1. DESCRIÇÃO DO PROBLEMA

A IGF como órgão superior de controlo orçamental, financeiro e patrimonial têm como funções realizar auditorias financeiras, de programas, operacional, de regularidade, de sistemas de informação, de desempenho e inquéritos e sindicâncias[1]:

- aos órgãos do Estado, suas instituições e pessoas colectivas de direito público ainda que personalizados, incluindo as autarquias locais;
- às empresas públicas, estatais e mistas onde o Estado detenha participação no respectivo capital, com excepção das instituições de crédito, para-bancárias e de seguros;

Um dos grandes desafios para a IGF, neste momento, prende-se com as grandes reformas de automatização dos sistemas de informação em curso na Administração Pública. Por um lado, a informação útil a auditar[2], ao passar para dentro dos computadores, não oferece garantias de que ela seja fiável (existe maior risco do auditor financeiro, por exemplo, formular a sua opinião com base em informações com erros, omissões e juízos prévios, aquando da sua disponibilização ao auditor sem que possa verificar a sua autenticidade) ou de que o sistema que a produziu esteja isento de

[1] Decreto n.º 40/99 de 29 de Junho

[2] Quer seja de natureza financeira (relatórios financeiros, demonstrações de resultados, balancetes, registos contabilísticos) ou de natureza operacional, situação que ocorre quando se fazem avaliações sectoriais. Por exemplo uma avaliação ao sector da justiça dá-nos o panorama do funcionamento da administração da justiça, no que concerne ao funcionamento das magistraturas (judicial e do Ministério Público) relativamente ao nº de processos que são julgados pelos tribunais ou do estágio da legalidade da nossa justiça.

falhas. Por outro, constituindo verdadeiros activos das instituições, os equipamentos, *softwares* e dados, também devem ser avaliados.

Actualmente, a IGF não se encontra preparada para fazer face à tais desafios, visto que apesar de ser sua competência fazer auditoria de sistemas de informação, ela não possui um conjunto de pressupostos para actuar nesta área, nomeadamente:

- um sector de auditoria de sistemas de informação;
- técnicos qualificados em auditoria de sistemas de informação; e
- instrumentos metodológicos para este tipo de auditoria.

Daí que continue a executar as suas actividades sem efectuar avaliações sistemáticas, periódicas ou constantes aos sistemas de informação que produzem as informações que ela própria consome.
A importância dos sistemas de informação nas instituições em geral, a pertinência e actualidade deste tema e as reformas em curso na Administração Pública, foram o mote para o presente estudo.

1.2. OBJECTIVO GERAL

Desenvolver uma metodologia que permita facilitar o processo de auditoria de sistemas de informação efectuado pela IGF em Moçambique.

1.3. OBJECTIVOS ESPECÍFICOS

- Avaliar o processo de auditoria efectuado pela Inspecção Geral de Finanças de Moçambique;
- Analisar referências metodológicas de auditoria para sistemas de informação informatizados;
- Desenvolver uma metodologia de auditoria para sistemas de informação informatizados;
- Testar a metodologia proposta.

2. METODOLOGIA DO TRABALHO

Em decorrência do problema de investigação, que se coloca na presente pesquisa, adoptou-se a metodologia de estudo de caso. Segundo Duarte (2006), estudo de caso é uma inquirição empírica que investiga um fenómeno contemporâneo dentro do contexto da vida real e onde múltiplas fontes de evidências são utilizadas.

Ainda, na linha de Lintz (2000), uma pesquisa baseada no estudo de caso pode ser desenvolvida considerando as seguintes fases: exploratória, delimitação de estudo, análise sistemática e redacção do relatório.

2.1. Fase Exploratória

Segundo a concepção de um estudo de caso que pretende não partir de uma visão não predeterminada da realidade, mas aprender e compreender os múltiplos aspectos de uma situação, a fase exploratória coloca-se como fundamental para a definição do escopo do objecto de estudo (Lintz, 2000). É o momento de estabelecer os contactos iniciais para o trabalho de campo.

Esta fase consistiu no envolvimento do estudante nas actividades da instituição (IGF) em forma de estágio. Este envolvimento criou oportunidades para que o estudante realizasse observações participativas. Durante esta fase o estudante integrou-se na IGF, como estagiário, em resposta a um anúncio no jornal Notícias para o recrutamento de técnicos de informática, desde Julho de 2004, onde se foi inteirando da actividade principal da instituição, a auditoria. Esta experiência permitiu colher informação rica e sólida dos principais constrangimentos que afectam a organização. E, a permanência do estudante na IGF como estagiário, também permitiu compreender o funcionamento da instituição, as actividades que desenvolve e, acima de tudo, identificar as áreas de estudo.

2.2. Delimitação do Estudo

A importância de determinar o âmbito da pesquisa e estabelecer os contornos do estudo, decorre do facto de que nunca será possível explorar todos os ângulos do fenómeno. Nessa fase, dependendo

das características próprias do objecto de estudo, são escolhidas as técnicas mais adequadas para a colecta de dados (Lintz, 2000).

Segundo Martins (2007), neste tipo de estudo, os instrumentos mais comuns para a colecta de dados são os questionários e entrevistas.

- Questionários podem ser com perguntas:
  - fechadas – são aquelas questões que apresentam categorias ou alternativas de respostas fixas;
  - abertas – são aquelas perguntas que conduzem o informante livremente com frases ou orações.

- Entrevistas

  São uma técnica que permite o relacionamento entre o entrevistado e o entrevistador. Não é uma simples conversa, trata-se de um diálogo orientado que busca através de interrogatórios informações e dados para a pesquisa. As entrevistas podem ser estruturadas e não estruturadas.
  - Entrevistas estruturadas - quando possuem as questões previamente formuladas, não havendo liberdade para o entrevistador alterar ou fazer inclusão de questões;
  - Entrevistas não estruturadas - o pesquisador busca obter os dados mais relevantes através de conversão objectiva.

Nesta fase optou-se pelos questionários visto que haviam questões formuladas com o objectivo de obter dados estatísticos do ambiente de actuação da IGF e pela facilidade que os mesmos tem na obtenção da informação nas entidades inquiridas tendo em conta a disponibilidade e abertura das entidades para as entrevistas.

O desenho do instrumento de recolha de dados consistiu no desenvolvimento de um questionário que serviu para a colheita, a nível de instituições públicas seleccionadas, de dados relevantes para o estudo. Na recolha de dados, para além da IGF, foram seleccionadas outras instituições de nível central (descritas no anexo 6) como Ministérios, Institutos e algumas Direcções Nacionais com o objectivo de alcançar uma amostra significativa.

No total foram enviados 47 questionários, dos quais se obteve 34 respostas, o que corresponde a uma taxa de adesão de 72,3%, conforme ilustra a tabela 1.

Tipos de Organismos	Organismos Inquiridos (Nº)	Respostas Obtidas (Nº)	Percentagem de Adesão (%)
Ministérios	19	14	73,68
Institutos	5	3	60,00
Empresas Públicas	10	8	80,00
Outros	13	9	69,23
Total	**47**	**34**	**72,34**

Tabela 1: Dados Sobre a Informação Enviada às Instituições

Importa referir que no processo de recolha de dados/informações foram conduzidas entrevistas não estruturadas, baseadas no questionário acima referido, visando o enriquecimento e aprofundamento das respostas obtidas pelos questionários às mesmas instituições inquiridas.

A recolha de dados permitiu um melhor conhecimento actualizado da situação concreta das instituições públicas no domínio de auditoria e das tecnologias de informação e comunicação, e da IGF em particular.

2.3. Análise Sistemática

É uma análise que está presente em todos os estágios da pesquisa (Lintz, 2000). Nesta fase, procedeu-se com a revisão bibliográfica e o desenvolvimento e teste da metodologia proposta.
Martins (2007), refere-se a revisão bibliográfica como sendo um instrumento que dá suporte e fundamentação teórico-metodológica ao estudo. É de facto um dos pontos vitais para o trabalho científico.

O desenvolvimento da metodologia foi efectuado com base no estudo de documentos (regulamentos, planos, relatórios, manuais de procedimento) da IGF, na revisão bibliográfica e na consulta a especialistas da área.

Os resultados desta pesquisa permitem criar a metodologia que seguidamente foi testada no Departamento de Sistemas de Informação do Tribunal Administrativo, como forma de avaliar a sua aplicabilidade.

2.4. Redacção do Relatório

O objectivo do relatório é de apresentar os múltiplos aspectos que envolvem o problema, mostrar sua relevância, situá-lo no contexto em que acontece e indicar acções para modificá-los (Lintz, 2000).

Nisso, foram utilizados meios tecnológicos como computador, impressora, sistema operacional *Windows* e processador de texto *Microsoft Word*. Para a análise e tratamento dos dados recolhidos através dos questionários foi empregue o *software* SPSS e *Microsoft Excel*.

CAPÍTULO II: AUDITORIA DE SISTEMAS DE INFORMAÇÃO

1. CONCEITOS DE AUDITORIA DE SISTEMA DE INFORMAÇÃO

1.1. HISTÓRIA DO SURGIMENTO DA AUDITORIA

Podem se achar rastros da contabilidade datando das mais antigas das civilizações, até mesmo civilizações nas quais a arte da palavra era mal conhecida. Com o advento da escritura e aquisição da arte pela população mais instruída, alguma forma de registos era necessária para ser mantida pelo trabalhador e o mestre que examinava os registos. Assim evoluiu a arte de contabilidade e a prática de auditar. O mestre ouvia e daí veio o auditor. A palavra "auditor" é derivada da palavra "*audire*" que vem do latim que significa "ouvir" (Banze, 2003).

No século XV, com o crescimento fenomenal do comércio, primeiro na Itália e depois nos outros países europeus, os problemas e as complexidades da contabilidade começaram a se demonstrarem na realidade.

Em 1581, na cidade de Veneza, na Itália, foi fundada a primeira sociedade de contabilistas que ficou conhecida por "*Collegio Raxonati*", onde todos os contabilistas tinham que fazer um estágio durante seis anos. Depois da formação desta primeira, mais sociedades foram aparecendo. Estas sociedades eram instituições completamente privadas e resistiam a qualquer forma de interferência estatal. Com o grande desenvolvimento que ocorreu na Europa, durante a era da Revolução Industrial, as instituições sentiram a necessidade de implementar bons procedimentos contabilísticos e eficientes medidas de controlo interno. Por outro lado, o facto de maior parte de tais instituições serem sociedades anónimas implicou que as demonstrações financeiras apresentadas aos accionistas fossem auditadas. Em 1880 foi fundado o Instituto de Contabilistas da Inglaterra e do País de Gales e a partir daí, devido à colonização inglesa nos Estados Unidos e Canadá e ao grande desenvolvimento industrial lá ocorrido, notou-se um incremento da actividade de auditoria, tendo alcançado naqueles países não só uma enorme difusão como também um aperfeiçoamento técnico bastante elevado. Com o progressivo avanço das grandes instituições multinacionais, a auditoria se instalou nos países com maior desenvolvimento e com mais industrialização, como por exemplo Japão, Singapura, África do Sul (Banze, 2003).

Nos países socialistas a auditoria não seguiu o mesmo rumo, dando maior ênfase na conformidade e eficácia das medidas de controlo interno. O avanço da profissão em África tem, também, sido lento, pois a maior parte dos países de Sul do Sahara, não tem institutos de contabilistas.

A auditoria de sistemas de informação (SI) nasce com a introdução dos computadores em sistemas de contabilidade. Acredita-se que a primeira implementação e utilização de um sistema de contabilidade automatizado, tenha sido em *General Electric* em 1954, nos Estados Unidos. De 1954 até meados da década 60, a profissão de auditoria era exercida ao redor do computador. Nesta época só os computadores *mainframe* eram utilizados e, poucas pessoas é que tinham habilidades para programar e operar com este equipamento (Wikimedia, 2006).

O cenário começou a mudar, nos meados da década 60, com a introdução de novos tipos de computadores, menores e menos caros, o que fez com que se aumentasse o uso de computadores e com isso a necessidade de os auditores se familiarizarem com conceitos de utilização de computadores em negócios.

Com o incremento do uso dos computadores, apareceram, também, diferentes tipos de sistemas contabilísticos automatizados. As associações de auditores e de contabilistas, da época, desenvolveram o primeiro *software* de auditoria denominado GAS e anos depois iniciaram com a produção de directrizes, procedimentos e padrões para auditorias de SI.

Em 1977, foi publicada a primeira edição de "Objectivos de Controlo", esta publicação é conhecida como *Objectivos de Controlo Relacionados ao Uso da Tecnologia da Informação* (COBIT). Em 1994, a organização que criou estas normas e directrizes, antes conhecida como EDPAA mudou a designação e passou a chamar-se por Associação de Auditoria e Controlo de Sistemas de Informação, ISACA. Os recursos COBIT são utilizados, tanto pelos gestores de TI como pelos auditores de SI, como uma fonte de orientação para a obtenção de melhores desempenhos (Wikimedia, 2006).

1.2. CONCEITO DE AUDITORIA

Muitas vezes, o termo auditoria foi empregue incorrectamente, pois considerou-se que se tratava de uma avaliação cujo único fim seria detectar erros e assinalar falhas. Segundo Carneiro (2004), o conceito de auditoria é muito mais amplo, podendo ser referido como um exame crítico que tem a finalidade de avaliar a eficácia e eficiência de um departamento ou uma instituição.

Dito de outro modo, toda e qualquer auditoria é a actividade que consiste na emissão de uma opinião profissional sobre o objecto de análise, a fim de confirmar se cumpre adequadamente as condições que lhe são exigidas (Carneiro, 2004).

No âmbito deste conceito pode-se indicar os seguintes elementos fundamentais:

- **Conteúdo:** uma opinião;
- **Condição:** profissional;
- **Justificação:** sustentada em determinados procedimentos;
- **Objecto:** uma dada informação obtida num certo suporte;
- **Finalidade:** determinar se apresenta adequadamente a realidade ou se esta responde às expectativas que lhe são atribuídas, quer dizer, a sua fiabilidade.

Pode-se, então, dizer que a auditoria é uma operação de análise e diagnóstico da instituição, tendo em consideração todos os aspectos da sua gestão, a fim de avaliar a coerência, a racionalização de processos e de apreciar a validade e o rigor dos resultados.

1.3. TIPOS DE AUDITORIA

Os tipos de auditoria mais comuns, segundo Dias (2000) e Carneiro (2004), são classificados de acordo com os seguintes aspectos: quanto ao órgão fiscalizador, à forma de abordagem do tema e ao tipo ou área envolvida.

- **Quanto ao órgão fiscalizador**
  - ✓ Auditoria interna – realizada por um departamento interno responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um dos seus objectivos é reduzir as probabilidades de fraudes, erros, práticas ineficientes ou ineficazes. O serviço de auditoria interna deve ser independente e prestar contas à direcção da instituição.
  - ✓ Auditoria externa – realizada por uma instituição externa e independente à entidade fiscalizada, com o objectivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e ilegalidade de suas operações.
  - ✓ Auditoria articulada – trabalho conjunto de auditorias externas e internas, devido à super-posição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

- **Quanto à forma de abordagem do tema**
  - ✓ Auditoria horizontal – auditoria com tema específico realizado em várias entidades ou serviços paralelamente.
  - ✓ Auditoria orientada – auditoria focada em uma actividade específica qualquer ou em actividades com fortes indícios de erros ou fraudes.

- **Quanto ao tipo ou área envolvida**
  - ✓ Auditoria de programas de governo – acompanhamento, exame e avaliação da execução de programas e projectos governamentais específicos. Em geral, preocupa-se com a efectividade dos programas governamentais.
  - ✓ Auditoria do planeamento estratégico – auditoria que verifica se os principais objectivos da entidade são atingidos e se as políticas e estratégicas de aquisição, utilização e alienação dos recursos são respeitadas.
  - ✓ Auditoria administrativa – auditoria que engloba o plano da organização, seus procedimentos e documentos de suporte à tomada de decisão.
  - ✓ Auditoria contabilística – auditoria relativa à salvaguarda dos activos e à fidedignidade das contas da instituição. Essa auditoria, consequentemente, tem como finalidade fornecer uma garantia de que as operações e o acesso aos activos se efectuem de acordo com as devidas autorizações.
  - ✓ Auditoria financeira – também conhecida como auditoria de contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contabilísticos - financeiros, orçamentários e patrimoniais, verificando se todas as operações foram correctamente autorizadas, liquidadas, ordenadas, pagas e registadas.
  - ✓ Auditoria de legalidade – também conhecida como auditoria de regularidade ou de conformidade. Consiste na análise da legalidade e da regularidade das actividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.
  - ✓ Auditoria operacional – auditoria que incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob o ponto de vista da economia, eficiência e eficácia.
  - ✓ Auditoria integrada – inclui simultaneamente a auditoria financeira e a operacional.
  - ✓ Auditoria de Sistema de Informação – tipo de auditoria, essencialmente operacional, por meio da qual os auditores analisam os sistemas informáticos, o ambiente de informática, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências. Em alguns países é conhecida como auditoria informática, computacional ou de TI.
  - ✓ Auditoria de Qualidade (Desempenho) - A auditoria da qualidade é um processo de análise e avaliação segundo o qual se pretende verificar a eficácia desses sistemas quanto aos objectivos e padrões referidos.

- ✓ Auditoria Ambiental - Sendo muito recente, a Auditoria Ambiental examina e analisa os prováveis impactos negativos ou positivos que as instituições possam causar ao meio ambiente.
- ✓ Auditoria de Marketing - A auditoria de Marketing é uma importante responsabilidade da gestão de topo. Sendo revisões e avaliações de modo sistemático, crítico e imparcial de todas as operações do Marketing, estas auditorias podem beneficiar qualquer instituição e apontar para oportunidades de melhorar o desempenho desta área funcional.

2. PROCESSO DE AUDITORIA DE SISTEMA DE INFORMAÇÃO

De forma geral, o processo de auditoria de SI compreende as fases de Planeamento da auditoria, Execução da auditoria, Elaboração do Relatório e Acompanhamento de auditoria, que são descritas a seguir.

2.1. FASE DE PLANEAMENTO

O ponto 3.1.1 das normas de auditoria da INTOSAI estipula que: "*O auditor deve planear a auditoria de modo a assegurar a execução de uma auditoria de elevada qualidade, de uma forma económica, eficiente e eficaz e num período de tempo adequado*" (INTOSAI, 2005).
Ainda sobre o planeamento, os padrões S5 nº 3, 4, 5 e 6 da ISACA se referem à necessidade e importância do planeamento.

O planeamento, em auditoria, pode ser vista em três dimensões, designadamente:

- Plano estratégico (Visão)
- Plano anual (programa de actividades)
- Programa de Auditoria (Planeamento do trabalho feito pela equipa)

2.1.1. Plano Estratégico

O plano estratégico é estabelecido, normalmente, para um período de 3 a 5 anos. Seus objectivos são mais amplos, atingem toda a instituição e são aprovados pela gestão superior.
Seu conteúdo define as metas da gestão de auditoria, seu modo de actuação, os recursos necessários (pessoal, equipamentos e recursos financeiros) e as necessidades de treinamento. É aconselhável rever e actualizar o plano anualmente.

2.1.2. Plano Anual

Este plano traduz o plano estratégico em um programa de actividades para o ano que se inicia.
Neste plano, as actividades a realizar, são determinadas tendo em conta os critérios previamente estabelecidos para a definição dos trabalhos. Define-se a alocação do pessoal, orçamento, datas de execução, etc.

2.1.3. Programa de Auditoria

O programa de auditoria baseia-se em auditorias individualizadas e contém detalhes exactos dos objectivos a serem atingidos, as áreas a serem auditadas, os recursos necessários e em que prazo, os objectivos de controlo e os procedimentos de auditoria a serem seguidos. É feito pela equipa de auditores que vai executar o trabalho.

2.2. FASE DE EXECUÇÃO

Ao longo da execução da auditoria, a equipa deve reunir evidências suficientemente confiáveis, relevantes e úteis para a consecução dos objectivos da auditoria. Os achados de auditoria e as conclusões da equipa devem ser suportados pela correcta interpretação e análise dessas evidências (Dias, 2000).

Toda a documentação, geralmente organizada em *papéis de trabalho*[3], deve estar disponível, para auxiliar a equipa na elaboração do relatório. Nem todas as evidências são investigadas detalhadamente e descritas no relatório final. A inclusão ou não de determinada evidência depende directamente de sua importância para a consecução dos objectivos da auditoria e do tempo e esforço necessários para esclarecer todos seus pontos nebulosos.

Conforme ilustrado na Figura 1, a execução da auditoria, inicia com a avaliação do ambiente controlo interno (teste de conformidade), descrita no ponto 5.2.1 do capítulo II**,** seguindo-se a realização dos testes substantivos. Como se pode depreender, a extensão dos testes substantivos depende do nível de confiança obtido no ambiente de controlo.

No decorrer da auditoria, os auditores descobrirão inúmeras discrepâncias e erros de menor importância. Cabe-lhes levar todas essas questões ao conhecimento do supervisor da área auditada, que esteja em condições de providenciar a correcção dos erros. Além de fazerem constar em seus papéis de trabalho, nenhuma outra providência é necessária por parte dos auditores. Os pontos de maior relevância devem ser apresentados em um relatório formal.

Durante a execução da auditoria, os auditores devem também discutir os pontos de auditoria e possíveis recomendações com o gestor e com os supervisores responsáveis pelos sistemas, pois a

[3] Toda a documentação, preparada ou obtida pelo auditor, relacionada com a realização de uma auditoria

reacção e os comentários desses funcionários serão importantes para as conclusões iniciais e recomendações, bem como servem para esclarecimento de eventuais dúvidas.

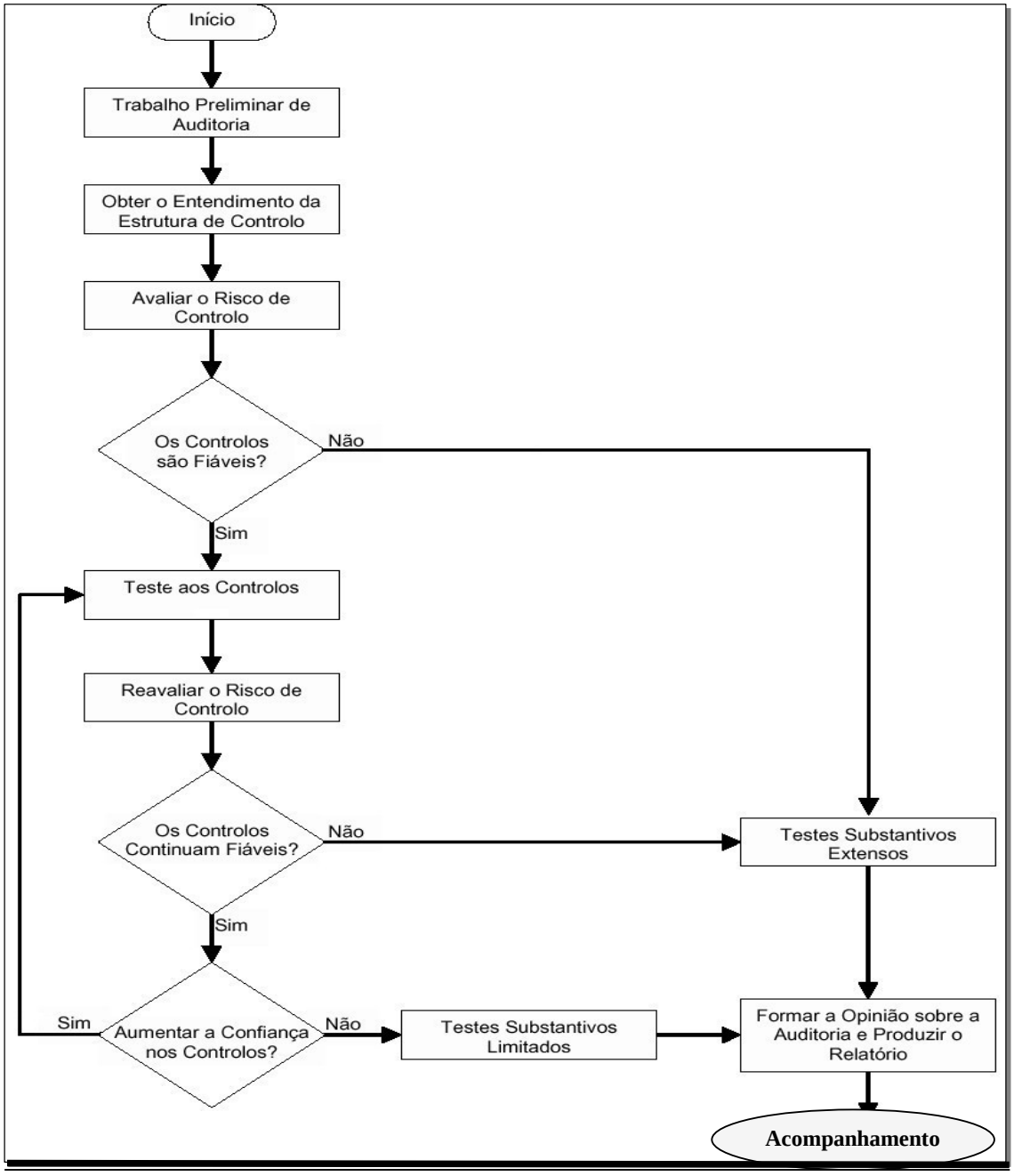


Figura 1: Processo de Auditoria

2.2.1. Papéis de trabalho

Para que fique registado todo o trabalho do auditor, ele elaborará os papéis de trabalho, que são o conjunto de formulários e documentos que contém as informações e os apontamentos redigidos pelo auditor, no decurso do exame, as provas por ele realizados e, em muitos casos, a descrição dessas provas, que constituem o testemunho do trabalho executado e o fundamento de sua opinião (GODY, 1999).

Para que atinjam sua finalidade, os papéis de trabalho devem ser sempre claros e concisos e fornecer um registo completo e sem ambiguidades do trabalho realizado e para que outros auditores não envolvidos na auditoria, sejam capazes de chegarem às mesmas conclusões a partir dos motivos ali mencionadas.

2.3. FASE DE ELABORAÇÃO DE RELATÓRIO

O auditor normalmente apresenta suas constatações e conclusões na forma de um relatório escrito, o qual inclui factos sobre a instituição auditada, comprovações, conclusões e, eventualmente, recomendações e/ou determinações (Dias, 2000).

As normas, da INTOSAI (ponto nº 4.0.7), para a elaboração do relatório prescrevem que a linguagem utilizada pelo auditor deve ser clara, objectiva e simples, evitando-se o uso de termos técnicos ou siglas (INTOSAI, 2005). Quando for necessário a utilização de termos técnicos, é recomendável que o relatório apresente glossário ou explanações ao longo do texto.

O relatório deve ser revisto por todos os membros da equipa de auditoria com intuito de verificar sua conformidade com os padrões e práticas da instituição auditora e a inexistência de inconsistências, erros ou lacunas (Dias, 2000). É conveniente também fazer uma revisão em termos gramaticais e estilísticos, para garantir clareza e objectividade do texto. Antes de ser apresentado formalmente ao auditado, o relatório é revisto pela chefia da equipa, pela direcção da instituição auditora ou por outra instituição supervisora.

2.3.1. Destinatários do Relatório

Dependendo do motivo que levou a realização da auditoria, o relatório pode ser encaminhado a direcção da instituição (auditoria solicitada para identificar falhas em sua própria administração), ao organismo que financia a instituição auditada (auditoria solicitada como forma de proteger seus

investimentos) ou ao organismo responsável pelo controlo e auditoria geral da instituição (auditoria de sistemas solicitada como parte de uma auditoria genérica, financeira ou de regularidade).

2.3.2. Estrutura do relatório

A seguir serão apresentados, como sugestão, tópicos normalmente abordados em um relatório elaborado por um órgão de auditoria interna, dirigido aos responsáveis pelo controlo da administração de recursos das instituições auditadas.

- **Sumário Executivo –** Apresenta um breve resumo do relatório;
- **Introdução** – Identifica sumariamente a questão que é objecto de relatório, os objectivos do trabalho, o método utilizado e o âmbito considerado;
- **Resultados obtidos** – São evidenciadas as situações constatadas e o significado e relevância das eventuais desconformidades;
- **Conclusões** – Indica as conclusões obtidas do trabalho;
- **Recomendações** – Lista as medidas necessárias à correcção das situações anómalas detectadas;
- **Propostas** – Propõe um conjunto de tomadas de decisão, a um nível superior, que assegurem a adequada tramitação, seguimento e eficácia do relatório.

2.4. FASE DE ACOMPANHAMENTO DOS RESULTADOS DE AUDITORIA

Segundo o padrão S8 das normas de procedimentos sobre actividades de acompanhamento do ISACA, no seu nº 3, estabelece que após o relatório de resultados e recomendações, o auditor de SI deve solicitar e avaliar informações relevantes para concluir se a acção apropriada foi tomada pela direcção de maneira oportuna.

Para cumprir com este padrão, de acordo com IIA (2004), deve-se estabelecer procedimentos para incluir o seguinte:

- Um prazo no qual a resposta da direcção, da entidade auditada, sobre as revelações de auditoria deverá ser dada;
- Uma avaliação da resposta dada;
- Uma verificação da resposta (quando apropriado);
- Um procedimento de comunicação que faça subir as respostas/acções insatisfatórias.

Determinadas revelações e recomendações feitas podem ser tão relevantes que requeiram uma acção imediata por parte da instituição auditada. Tais condições deverão ser monitoradas pela actividade de auditoria interna até serem corrigidas, devido ao efeito que possam ter na organização.

2.5. SUPERVISÃO DO TRABALHO

O padrão S6 das normas de procedimento na execução da auditoria da ISACA, no seu nº 3, estipula que a equipe de auditoria de SI deve ser supervisionada para fornecer garantia razoável de que os objectivos da auditoria estão sendo atingidos e que os padrões de auditoria profissional aplicáveis estão sendo seguidos.

Segundo GODY (1999) é essencial que haja uma supervisão, para garantir a consecução dos objectivos da auditoria e a manutenção da qualidade do trabalho realizado. O supervisor serve-se dos papéis de trabalho resultantes do exame para verificar o trabalho realizado.

Uma supervisão e um controle adequados são, portanto, sempre necessários, independentemente da competência individual dos auditores.

3. OS REFERENCIAIS METODOLÓGICOS APLICADOS À AUDITORIA DE SI

Existem actualmente um conjunto de normas (*standards*) internacionais de SI que habitualmente incorporam modelos estruturados (*frameworks*) e que aqui optou - se 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 auditoria de SI.

3.1. Metodologia

A Metodologia é o estudo dos métodos ou seja, as etapas a seguir num determinado processo (Wikimedia, 2010). Tem como finalidade captar e analisar as características dos vários métodos disponíveis, avaliar suas capacidades, potencialidades, limitações ou distorções e criticar os pressupostos ou as implicações de sua utilização. Além de ser uma disciplina que estuda os métodos, a metodologia é também considerada uma forma de conduzir a pesquisa ou um conjunto de regras para ensino de ciência e arte.

3.2. Tipos de Referenciais Aplicados aos SI e à Auditoria

Segundo Terzian (2007), devido à necessidade de melhorar os processos de negócio e garantia da qualidade as organizações americanas, apreensivas com o poderio industrial do Japão nos anos 80, começaram a desenvolver e adoptar modelos e padrões de qualidade. Ainda, de acordo com Terzian (2007) e Coutinho (2007), dentre esses referenciais inclui-se *IT Infrastructure Library* (ITIL), *COBIT*, *Six Sigma*, Norma BS 7799 - *Britsh Standard* 7799/ ISO 17799, *Capability Maturity Model Integration* (CMMI), ISO *e Balanced Scorecard* (BSC).

3.2.1. ITIL – *Information Technology Infraestructure Library*

Trata-se de um conjunto de orientações desenvolvidas pelo governo britânico, que descreve um modelo de processo integrado de melhores práticas para prover a qualidade de serviços de TI. Desenvolvido em 1989, é um modelo (não proprietário) que pode ser implementado por qualquer

organização seja ela de pequeno ou grande porte demonstrando assim sua flexibilidade de adaptação.

O ITIL endereça estruturas de processos para a gestão de uma organização de TI apresentando um conjunto compreensivo de processos e procedimentos de gestão organizados em disciplinas com os quais uma organização pode fazer sua gestão táctica e operacional com vista a alcançar o alinhamento estratégico com os negócios.

Pontos fortes: Bem estabelecido, amadurecido, detalhado e focado em questões de qualidade operacional e produção de TI. Pode ser combinado à CMMI para cobrir todos processos relacionado a TI.

Limitações: Não aborda o desenvolvimento de sistemas de gestão de qualidade e não é voltado para processos de desenvolvimento de *software*.

3.2.2. COBIT - *Control Objectives for Information and related Technology*

O COBIT é um conjunto de directrizes baseadas em auditoria para processos, práticas e controlos de TI. Foi publicado em sua primeira edição em 1996 pela ISACA *e IT Governance Institute*. Está voltado para a redução de risco com enfoque na integridade, confiabilidade e segurança.

3.2.2.1. Estrutura do COBIT

O COBIT está estruturado em objectivos de controlo de alto nível que definem 34 processos de TI agrupados em 4 domínios, designadamente:

- PLANEAMENTO & ORGANIZAÇÃO (PO): Cobre a estratégia e táctica e diz respeito à identificação da maneira que a TI pode melhor contribuir para o atendimento dos objectivos do negócio. Além do mais, a realização da visão estratégica precisa ser planeada, comunicada e gerida em diferentes perspectivas. Finalmente, uma organização apropriada bem como uma infra-estrutura tecnológica devem ser estabelecidas.
- AQUISIÇÃO & IMPLEMENTAÇÃO (AI): Para concretizar a estratégia de TI, soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, bem como implementadas e integradas no processo do negócio. Adicionalmente, mudanças e manutenções nos sistemas existentes estão cobertas por este domínio para assegurar que o ciclo de vida continue para esses sistemas.
- PRODUÇÃO & SUPORTE (DS): Se preocupa com as entregas reais dos serviços requeridos que abrangem as operações tradicionais sobre aspectos de segurança e continuidade até ao

treinamento. A fim de entregar serviços, os processos necessários de suporte devem ser estabelecidos. Este domínio inclui o processamento real de dados pelos sistemas aplicativos, frequentemente classificados como controlos de aplicações.

- MONITORIA (M): Todos os processos de TI precisam ser regularmente avaliados ao longo do tempo com relação a sua qualidade e conformidade com os requisitos de controlo.

Na Figura 2, é possível ver como os quatro domínios do COBIT estão relacionados, assim como os processos que compõem cada domínio.

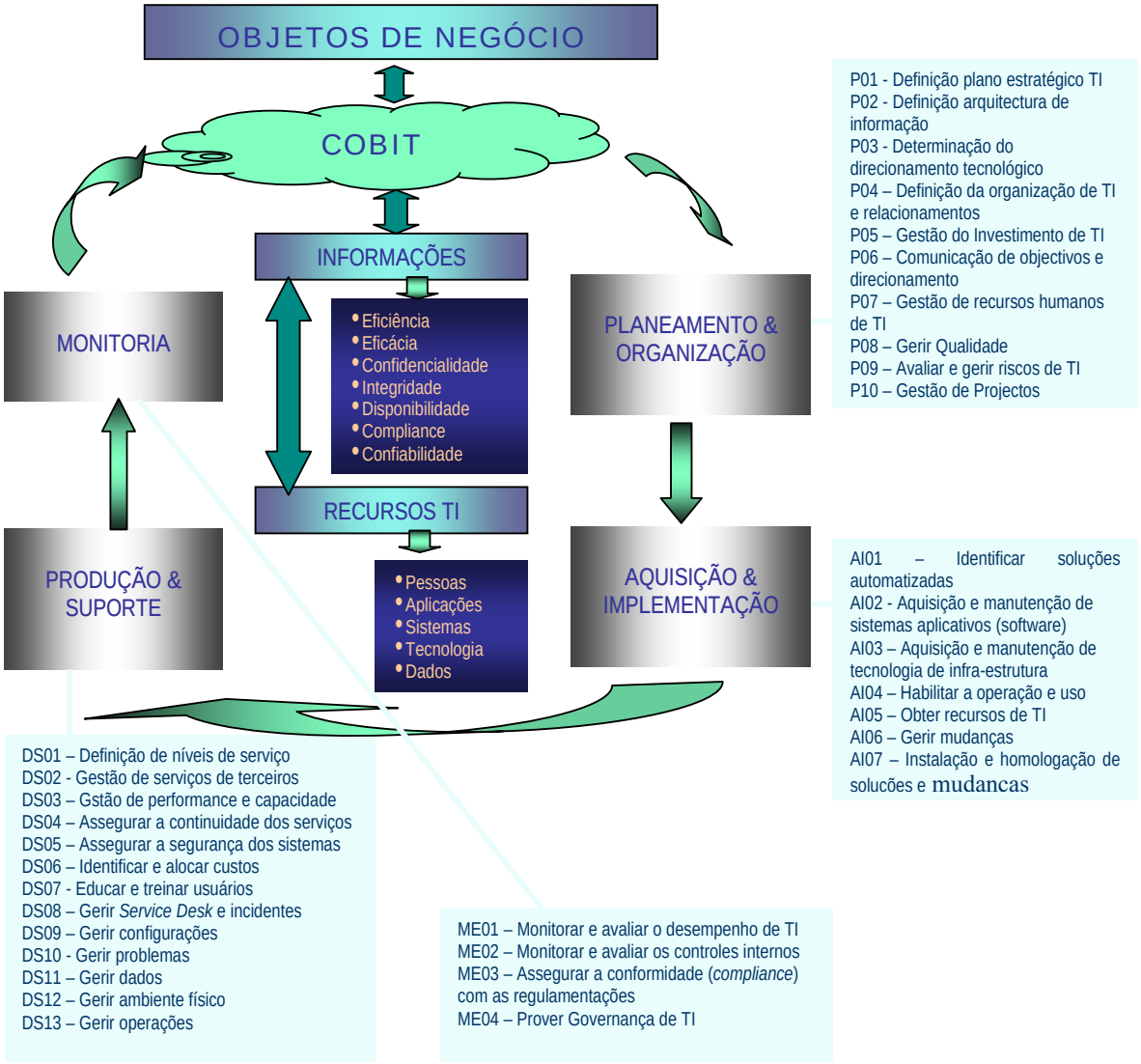


Figura 2: *Framework* do COBIT

3.2.2.2. Objectivo de Controlo

Pode se entender como uma formalização sobre o resultado desejado ou propósito a ser alcançado pela implementação de procedimentos de controlo em actividades específicas à TI.

O COBIT começa com um Objectivo de Controlo de alto nível, ligado a um requisito de negócio. DS-5, por exemplo, se define como sendo um "*Controlo sobre o processo de TI de garantir a segurança de sistemas*", que preenche uma necessidade do negócio de "*salvaguardar a informação contra uso não autorizado, divulgação ou modificação, e contra dano ou perda*". O objectivo de controlo DS-5 se divide em 21 controlos secundários, que vão desde o Plano de Segurança da Informação, passando por controlo de acesso e protecção contra vírus, até a protecção do valor económico.

Para cada controle secundário, o COBIT informa um conjunto de melhores práticas que permitem atingir o Objectivo de Controlo e um conjunto de Directrizes de Auditoria.

Pontos fortes: Permite que TI aborde riscos não endereçados explicitamente por outros modelos e que seja aprovada em auditorias. Funciona bem com outros modelos de qualidade, principalmente ITIL.

Limitações: Diz o que fazer, mas não como fazer. Não lida directamente com desenvolvimento de *software* ou serviços de TI. Não fornece um "*road map*" para aprimoramento contínuo de processos.

3.2.3. Norma BS 7799 - *British Standard* 7799/ ISO 17799

A BS 7799 é uma norma que deve servir de base para a criação de uma política de segurança. Teve sua primeira versão publicada em 1995. A segunda versão desta norma foi elaborada em 1999 e está dividida em duas partes:

- *Parte I*: BS 7799-1:1999 é um catálogo que agrupa 36 objectivos de controlo decompostos em 127 medidas de controlo que explicam os pontos que devem ser trabalhados na implementação dessas medidas. O foco desta parte está na gestão de risco.
- *Parte II*: BS 7799-2:1999 apresenta um Sistema de Gestão da Segurança da Informação utilizado para fazer avaliações eficientes em qualquer aplicação, departamento ou organização. É composta de quatro fases:
    - *Avaliação de riscos*;
    - *Gestão de riscos*;
    - *Implementação de meios de segurança*;
    - *Declaração de aplicabilidade*.

No ano de 2000 houve a homologação da primeira parte a BS 7799 pela ISO (*International Organization for Standardization*) que originou a Norma Internacional de Segurança da Informação – ISO/IEC 17799.

Em Novembro de 2005, a ISO publicou a segunda edição da norma sob o título ISO/IEC FDIS 17799:2005(E), que inclui a segunda parte da BS 7799, que refere-se a implementação, de um conjunto de melhores práticas de segurança aplicáveis em organizações de qualquer porte. Esta edição cancela e substitui a norma ISO/IEC 17799:2000.

Limitado à aspectos de segurança da informação.

3.2.4. Six Sigma

Um método de aprimoramento de processo estatístico com enfoque na qualidade do ponto de vista do cliente ou do usuário desenvolvido pela Motorola. Define níveis de serviço e mede variações em relação a estes níveis. Os projectos percorrem cinco fases nomeadamente: definir, medir, analisar, aprimorar e controlar.

A variante *Design for Six Sigma* aplica os princípios deste método à criação de produtos ou serviços sem defeitos, e não ao aprimoramento dos que já existem.

Pontos fortes: Uma abordagem orientada a dados para descobrir a raiz de problemas de negócio e resolvê-los. Leva em conta o custo de qualidade. Em TI, é melhor aplicado em actividades passíveis de repetição e relativamente homogéneas, como operações de *call center* ou *help desk*. *Design for Six Sigma* pode ajudar a desenvolver boas especificações de *software*.

Limitações: Projectado originalmente para ambientes de manufactura; pode ser difícil aplicá-lo em processos que ainda não estão bem definidos e mensuráveis. Pode aprimorar o processo, mas não diz se tem o processo certo.

3.2.5. *Capability Maturity Model Integration* (CMMI)

Desenvolvido pela *Software Engineering Institute e Carnegie Mellon University*, é uma colecção de melhores práticas para desenvolvimento e manutenção de *software*. Permite que as empresas avaliem suas práticas e as comparem com as de outras empresas. SW-CMM mede a maturidade do processo, que progride em cinco níveis: 1 (inicial), 2 (gestão), 3 (definição), 4 (previsão) e 5 (optimização).

Pontos fortes: Criado especificamente para organizações de desenvolvimento de *software*. Focaliza o aprimoramento contínuo, e não apenas a manutenção de uma certificação. Pode ser usado para auto-avaliação.

Limitações: Não aborda aspectos de operações de TI como gestão de segurança, mudança e configuração, planeamento de capacidade, diagnóstico e funções de *help desk*. Estabelece metas, mas não diz como atingi-las.

3.2.6. ISO 9000

Trata-se de um conjunto de padrões auditáveis de alto nível voltados ao cliente (ISO 9000, 9001 e 9004) para sistemas de gestão de qualidade desenvolvido pela *International Standards Organization*. Destinado a garantir controlo, repetibilidade e boa documentação de processos (não de produtos).

Pontos fortes: Bem estabelecido, amadurecido. Goza de prestígio global. Pode ser aplicado em todas organizações. Cobre o desenvolvimento de *software*, operações e serviços de TI.

Limitações: Requer adaptação considerável quando utilizado em organizações de TI. Está mais virada para aspectos repetitivos e consistência de processos, e não directamente a qualidade dos processos. Não é bom para descobrir a origem de problemas.

3.2.7. *Balanced Scorecard*

O *Balanced Scorecard* (BSC) é um padrão usado para identificar a relação de causa - efeito entre processos e resultados e para desdobrar a estratégia em acções exequíveis. O BSC, é um método concebido inicialmente por Robert Kaplan e David Norton num artigo para a *Harvard Business School* no ano de 1992, ajuda as organizações a planear e entender sua estratégia de forma "balanceada" e, possibilita um raciocínio estratégico que leva em consideração questões de curto, médio e longo prazo.

Pontos fortes: Funciona muito bem para definir, planear, comunicar a estratégia e medir e monitorar o desempenho.

Limitações: Falha no suporte às actividades de melhoria contínua e não supre totalmente a necessidade de análise dos dados sobre a satisfação dos clientes ou sobre o desempenho do processo e do produto.

3.3. Razões Para Adopção de Referenciais

As organizações podem encarar o Governo dos SI (*IT Governance*) como 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 e permitem que todas as partes interessadas nos SI (*stakeholders*) tenham uma referência comum.
- 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 - As organizações podem beneficiar da partilha de conhecimento e de ideias (exemplos: grupos de utilizadores, *websites*, revistas, livros, etc.).
- 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.

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.
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.

3.4. Uma Selecção de Três Referenciais: COBIT, ITIL E ISO 17799

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 (Gomes, 2007). 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.

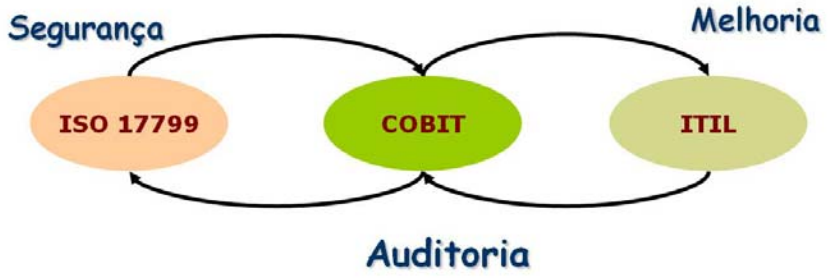


Figura 3: Três Referenciais Metodológicos Integrados

Da interpretação do esquema proposto por (LeBlanc, 2004), Figura 3, que relaciona três dos referenciais metodológicos, pode –se concluir o seguinte:

Numa primeira fase, *de definição*, 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*). 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.

Ainda, segundo Gomes (2007), o COBIT é o referencial aplicado preferencialmente na Auditoria de SI pelas seguintes razões:

- 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), 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. O ITIL também considera o alinhamento com o negócio, 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 de 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.

4. TÉCNICAS DE ANÁLISE E DE CONTROLO EMPREGUES NA AUDITORIA DE SI

Várias técnicas podem ser utilizadas em uma auditoria de sistema de informação, desde uma simples observação, em visitas à instituição, até entrevistas com os funcionários e dirigentes, e uso de ferramentas de apoio.

4.1. ENTREVISTAS

Ao longo da auditoria podem ser feitas entrevistas com os dirigentes e funcionários da instituição auditada, com o intuito de apresentar o plano da auditoria a ser realizada, colher dados, identificar falhas e indícios de irregularidades e, por fim, apresentar os resultados do trabalho. Segundo Dias (2000), as entrevistas podem ser:

4.1.1. Entrevista de Apresentação

É recomendável que a equipa de auditoria, no início de seu trabalho de campo, faça uma entrevista de apresentação com os dirigentes da instituição auditada. Em geral, nessa entrevista são apresentados todos os membros da equipa, o cronograma de actividades, os objectivos da auditoria, as áreas a serem auditadas, o período de execução dos trabalhos e as metodologias que serão adoptadas. Normalmente é solicitada a cooperação do auditado, assim como acomodações adequadas para a equipa (sala, mesa, armário, etc.), durante a execução do trabalho de campo.
Com frequência as instituições designam um dos seus gestores para actuar como ponto focal entre a equipa de auditoria e as chefias dos departamentos envolvidos.

4.1.2. Entrevistas de Recolha de Dados

Durante a auditoria podem ser feitas entrevistas aos gestores e funcionários da área auditada, com intuito de recolher dados sobre os sistemas ou ambiente de informática. Nessas entrevistas, podem ser identificados os pontos fortes de controlo, as falhas e possíveis irregularidades.
A equipa deve confirmar os factos relatados e, de preferência, apresentar ao entrevistado, antes da revisão final do relatório, partes do texto referentes a assuntos tratados com ele durante a entrevista.

Dependendo dos casos pode-se produzir um **Auto Declaração**[4] que é assinado pelos auditores presentes e pelo declarante. O Auto Declaração é um documento de suporte e serve como evidência perante factos constatados durante a auditoria. Com isso evita-se qualquer mal-entendido ou desvios de interpretação do que foi dito por cada entrevistado.

4.1.3. Entrevistas de Discussão das Deficiências Encontradas

No término das investigações, é comum serem apresentadas aos responsáveis de cada área auditada, as deficiências encontradas. Nessas entrevistas, os responsáveis podem discutir abertamente os pontos críticos e apresentar justificativas para tais falhas. Dependendo da justificativa dada, a falha correspondente pode ser desconsiderada ou a própria justificativa pode ser incluída no relatório de auditoria. Dessa forma interactiva, a equipa de auditoria dá oportunidade ao auditado de expor seus pontos de vista.

Vale ressaltar, entretanto, que nem todas as auditorias permitem essa discussão aberta com o auditado.

4.1.4. Entrevista de Encerramento

Ao final dos trabalhos de auditoria, a equipa se reúne novamente com os dirigentes da instituição auditada. Nessa ocasião, são feitos agradecimentos à colaboração da direcção e seus funcionários e são relembrados os objectivos de auditoria como também, se apresenta um resumo dos resultados de auditoria.

4.2. QUESTIONÁRIOS

É habitual que o auditor comece por solicitar o preenchimento de questionários previamente impressos e enviados aos responsáveis das diversas áreas a auditar, podendo o mesmo envio ser feito para utilizadores de outros níveis (Carneiro, 2004). As respostas permitem uma análise inicial que, por sua vez, irá orientar o trabalho do auditor e até a elaboração do seu relatório final.

Se o auditor tiver obtido uma informação adequada por outros meios, este instrumento pode ser omitido.

[4] Documento elaborado durante a auditoria mediante factos relatados mas que não possuem evidência pela qual o auditor se pode apoiar. É assinado pelo declarante e pelos membros da equipa de auditoria presentes.

4.3. CHECKLIST

O auditor deve construir perguntas muito estudadas e de formulação flexível, que o conduzam a obter respostas coerentes e que permitam uma correcta descrição dos pontos fracos e fortes. Este conjunto de perguntas tem o nome de *checklist* (Carneiro, 2004). Regra geral, os *checklists* devem ser respondidos oralmente, pois podem fornecer conteúdos mais individualizados e mais ricos do que as outras formas.

Segundo Carneiro (2004), os *checklists* podem ser avaliados por dois processos:

4.3.1. *Checklists* com escala de avaliação

Contém perguntas cujas respostas devem ser classificadas dentro de um intervalo preestabelecido (por exemplo, de 1 a 5, sendo 1 a resposta mais negativa e 5 o valor mais positivo).

Exemplo de um *checklist* com escala de avaliação

> *Durante uma auditoria sobre a segurança física de uma dada instalação, pretende-se analisar o controlo dos acessos de pessoas e objectos diversos ao Centro de Processamento de Dados.*

As respostas formuladas são avaliadas de acordo com uma escala da tabela 2.

Designação	Muito deficiente	Deficiente	Aceitável	Algo correcto	Inteiramente correcto
Pontuação	1	2	3	4	5

Tabela 2 :Escala de Avaliação

As perguntas devem ser colocadas ao auditado sem qualquer comentário às suas respostas para evitar problemas de fiabilidade (Tabela 3).

O resultado seria a média das pontuações: (1 + 2 + 2 + 4) /4 = 2,25, o que significa, de acordo com a escala referida, que a situação deve ser classificada como "deficiente".

Perguntas	Respostas	Pontuação
Existe algum pessoal dos serviços de segurança que vigie as zonas externas do edifício?	Não. Durante a noite há apenas um guarda que se encarrega também de um outro edifício que existe perto deste.	1
No que se refere à segurança interna do edifício, há pelo menos um vigilante por turno na zona do Centro de Processamento de Dados?	Sim, mas este funcionário tem de deslocar-se a outros 4 andares quando é necessário.	2
Há alguma saída de emergência além daquela que é usada para a entrada e saída de equipamento?	Sim, mas muitas vezes há caixotes empilhados junto à porta, o que dificulta a passagem.	2
O pessoal que se ocupa das comunicações internas pode entrar directamente na Sala dos Computadores?	Não. Apenas tem autorização para tal o chefe desse serviço. Os seus colaboradores necessitam de ter uma justificação e de avisar o Chefe da Sala.	4

Tabela 3: Exemplo de *Checklist* com Escala de Avaliação

4.3.2. *Checklist* com perguntas fechadas

Como se infere do nome, as respostas apenas podem ser "Sim" ou "Não". Em termos de pontuação, a primeira equivale a 1 (um) e a segunda a 0 (zero).

Exemplo de um checklist com perguntas fechadas

Suponha-se que está a decorrer uma revisão dos métodos de provas de programas no âmbito de um Desenvolvimento de Projectos (Tabela 4).

Perguntas	Respostas	Pontuação
Existe alguma norma segundo a qual o utilizador final faça a comprovação dos resultados finais dos programas?	Sim	1
O pessoal do Desenvolvimento sabe da existência dessa norma?	Sim	1
Essa norma aplica-se em todos os casos?	Não	0
Existe uma norma segundo a qual as provas tenham de realizar-se com jogos de ensaio ou fazendo uma cópia de bases de dados reais?	Não	0

Tabela 4:Exemplo de *Checklist* com Perguntas Fechadas

Os *checklists* com escala são adequados se a equipa técnica que efectua a auditoria não é muito grande e se têm critérios uniformes e equivalentes nas avaliações, pois permitem uma maior precisão na avaliação do que os *checklists* com perguntas fechadas. No entanto, a justeza do método depende muito da formação e competência dessa mesma equipa.

Os *checklists* com perguntas fechadas têm a vantagem de poderem ser utilizadas por vários membros da equipa de auditoria, mas apresentam o inconveniente de exigirem respostas "Sim" e "Não", não permitindo, assim, captar outras alternativas que poderiam ter interesse para o processo de análise.

4.4. ANÁLISE DE RELATÓRIOS DE CONTROLO INTERNO

A análise dos relatórios sobre o controlo interno é uma técnica muito importante para se poder avaliar a eficácia do sistema e exige que sejam considerados aspectos como o nível de utilização de cada utilizador, a forma de distribuição desses relatórios, a sua maior ou menor confidencialidade e a utilização da informação que contém (Carneiro, 2004).

4.5. ANALISE PRESENCIAL

No decurso da sua análise, é indispensável que o auditor visite as instalações da organização a auditar, em particular das que integram o sistema de informação informatizado, no que se refere a equipamentos, procedimentos e recursos técnicos. A análise presencial acompanha a aplicação de outras técnicas, em particular os questionários.

4.6. USO DE TÉCNICAS OU FERRAMENTAS DE APOIO

Além de auditar sistemas de informação, os auditores também utilizam a informática para realizar suas tarefas de auditoria. O termo *CAATs* (*Computer Assisted Audit Techniques*) define uma série de técnicas reconhecidamente úteis na execução de auditorias, as quais podem ser divididas em três categorias básicas (Dias, 2000), designadamente:

- Técnicas para análise de dados,
- Técnicas para verificação de controlos de sistemas e
- Outras ferramentas.

4.6.1. Técnicas Para Análise de Dados

Os dados do auditado podem ser colectados e analisados com auxílio de *softwares* (Tabela 5) de extracção de dados, de amostragem, e de analise de *logs*.

4.6.1.1. Análise do Log/Accounting

O ficheiro *Log/Accounting* é uma anotação histórica que informa sobre as alterações que vão acontecendo e como aconteceram durante utilização do *hardware* e do *software* que integram o SI informatizado.

4.6.2. Técnicas Para Verificação de Controlos de Sistemas

Essas técnicas permitem ao auditor testar a efectividade dos controlos dos sistemas do auditado. Pode-se analisar sua confiabilidade e ainda determinar se estão operando correctamente a ponto de garantir a fidedignidade dos dados. Dentre as técnicas mais utilizadas, pode-se citar:

- Simulações,
- Mapeamento estatístico de programas,
- Rastreamento de programas.

4.6.2.1. Mapeamento Estatístico dos Programas

O auditor utiliza esta técnica para verificar situações como a existência de rotinas que não são utilizadas e identificar o número de vezes que cada rotina foi utilizada durante o processamento de dados.

4.6.2.2. Rastreio de Programas

Apoiando-se em *softwares* potentes e modulares que permitem seguir o percurso dos dados no contexto de um dado programa, o auditor informático verifica até que ponto é que os programas instalados no sistema realizam exactamente as funções pretendidas e previstas e não outras. Em particular, estes percursos são utilizados para comprovar a execução das validações de dados previstas, sem que o sistema seja modificado (Carneiro, 2004).

4.6.2.3. Simulação *Test-Deck*

Para a aplicação desta técnica, submete-se um conjunto de dados de teste ao programa ou rotina que vigora no sistema. Se se verificar que todos os resultados obtidos através desse programa ou rotina estão incorrectos, pode-se concluir pela inadequação da lógica do processo que está a ser auditado.
A simulação dos dados que são utilizados para testar a situação de um dado programa deve poder prever situações correctas e incorrectas como, por exemplo, transacções incompletas, incompatíveis, duplicadas ou com campos inválidos. A aplicação da técnica de simulação de dados implica que o auditor tenha bons conhecimentos de análise de sistemas. A Figura 4 descreve as fases empregues na simulação *test-deck*.

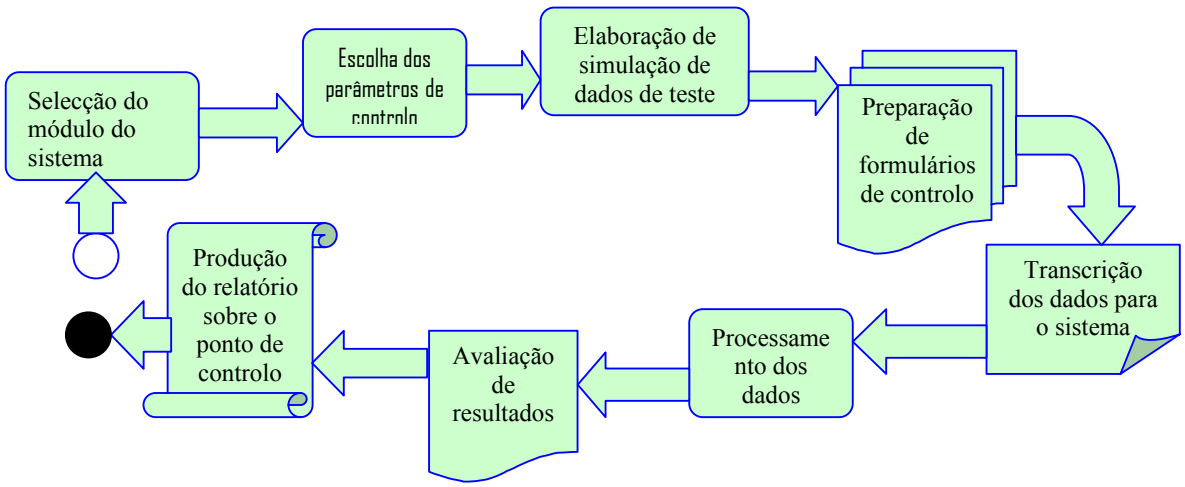


Figura 4: Sequência das Fases da Técnica Test-Deck

4.6.2.4. Simulação Paralela

Na chamada simulação paralela, o auditor começa por identificar a rotina que deve ser auditada e os ficheiros com os dados que têm sido utilizados. Posteriormente, prepara um programa informático de acordo com a lógica da rotina em questão, a fim de simular as funções de rotina do sistema que está a ser auditado. A este programa são submetidos conjuntos de dados de rotina que foram previamente processados no programa instalado no sistema. Consegue-se assim uma comparação entre as duas formas de processamento, o que permite avaliar a operacionalização do programa em análise.

4.6.3. Outras Ferramentas

Existem ferramentas que não são necessariamente de auditoria, mas sem dúvida, auxiliam o auditor durante a execução da auditoria e na elaboração do relatório. Nessa categoria se encontram os editores de texto, planilhas electrónicas, bancos de dados, *softwares* para apresentações e outros. A tabela 5 mostra os *softwares* mais usados na auditoria de SI.

Fases de Auditoria	***Software***	**Finalidade**
Planeamento	*MS Project, Cbeam, EXCEL e Outlook*	planos, cronogramas
Execução (Recolha de evidência)	*Visio, Powerpoint*	esquemas, fluxos e desenho
	Word, Excel, SPSS, COBIT,COBRA	questionários
	SQL Server, MY SQL, ORACLE	extracção de dados
	ACL, IDEA, SPSS	amostras
	ACL, Access, Excel, IDEA	análise de dados
	SPSS, Excel	regressão Linear
	Excel	simulação, gráficos
	Cbeam, Infocus	documentação, avaliação do controlo interno
	Outlook	comunicação
Relatório	*Word, Excel*	texto
	Powerpoint	apresentação
	Acrobat, Outlook	divulgação

Tabela 5: *Software* utilizado na Auditoria de Sistemas de Informação

5. ANÁLISE DE RISCO E TESTES NA AUDITORIA DE SI

5.1. RISCO EM AUDITORIA DE SI

De acordo com a norma SAS Nº 47, do Instituto Americano de Certificação dos Auditores Públicos, o risco de auditoria é aquele em que auditor incorre ao emitir uma opinião favorável quando existem erros materialmente relevantes (AU312, 2006).

5.1.1. Natureza do Risco de Auditoria

Segundo Oliveiras (2005), os riscos podem ser agrupados em duas dimensões, conforme ilustrado na Figura 5.

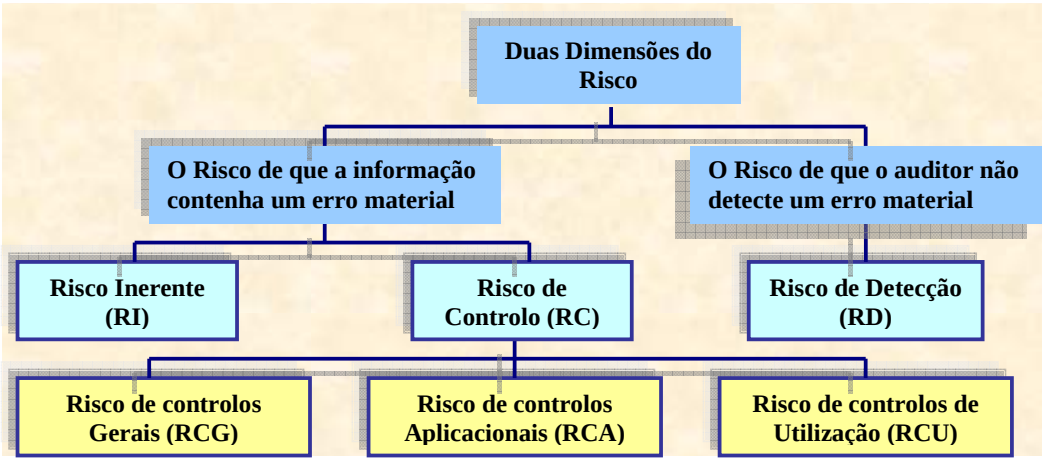


Figura 5: Dimensões de Risco

5.1.1.1. Risco de que a informação contenha um erro material

Nesta perspectiva, se encontra, dois tipos de risco, designadamente risco inerente e risco de controlo.

- **Risco inerente**

  É a susceptibilidade dos recursos de informação ou dos recursos controlados pelo Sistema de Informação serem roubados, destruídos, ignorados, modificados sem autorização, ou

sofrer outros danos, assumindo que não existem controlos internos relacionados. Este risco refere-se ao negócio e à sua envolvente.

Todos os negócios têm os seus próprios níveis de risco porém, deve-se prestar particular atenção nos seguintes aspectos:

- História conhecida no sector,
- Atracção para o abismo…
- Contexto
- Ramo de actividade (Banca, Saúde, Construção Civil, etc).

- **Risco de controlo**

  É o risco de que um erro materialmente relevante nos dados da entidade não será prevenido ou detectado e corrigido atempadamente pela estrutura de controlo interno da entidade.

  A Figura 6 descreve os três tipos de risco de controlo e suas respectivas abrangências, no contexto de sistemas de informação informatizados.

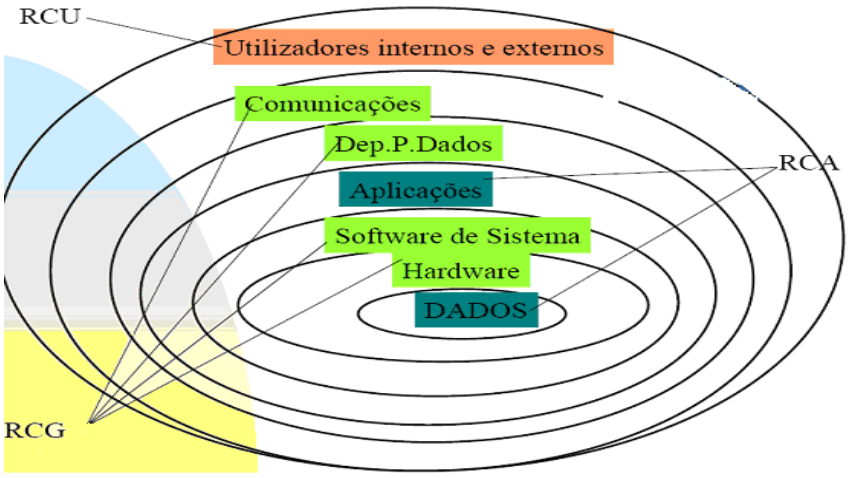


Figura 6: Tipos de Riscos de Controlo

O risco global de controlo interno será obtido a partir da combinação dos resultados obtidos nos controlos: gerais, aplicacionais e de utilização.

5.1.1.2. Risco de que o auditor não detecte um erro material

Conforme ilustrado na Figura 5, nesta dimensão se encontra o risco de detecção.

- **Risco de detecção**

  É o risco de que os procedimentos de auditoria não permitam detectar um erro material existente na informação. Pode ser determinado a partir da matriz de risco mostrado na Figura 7.

5.1.2. Relação entre os riscos

O risco geral de auditoria (RA), pela forma como se relaciona com os SI, pode ser pensado como o produto dos três riscos componentes:

RA = RI * RC * RD

É com base no nível do risco de auditoria e na avaliação dos riscos inerente e de controlo da entidade, que o auditor determina a natureza, duração e extensão dos procedimentos substantivos de auditoria necessários para se atingir o risco de detecção desejável.

Desta forma pode-se determinar o tamanho da amostra a partir do risco de detecção, quanto maior for o risco de detecção menor é o tamanho da amostra (EFICIÊNCIA) (Banha, 2005).

Por este método obtém - se uma aproximação científica à auditoria de SI baseada na análise de risco.

Figura 7: Matriz de Riscos

5.2. TESTES EM AUDITORIA DE SISTEMA DE INFORMAÇÃO

O objectivo dos testes é de obter uma evidência suficiente para emitir opinião e concluir a missão de auditoria (Banha, 2005).

Ainda, de acordo com Banha (2005), em auditoria existe dois tipos de testes, nomeadamente:

- Testes de conformidade; e
- Teste substantivos.

5.2.1. Testes de Conformidade

Destinam-se a confirmar se os procedimentos contabilísticos e as medidas de controlo interno sobre os quais a auditoria se irá basear, sendo adequados, se encontram em funcionamento ao longo do exercício.

Estes testes, não verificam directamente se os dados de um computador em particular são válidos e fiáveis.

Nessa avaliação, identifica-se os pontos fortes, fracos e as ineficiências. Essa identificação é importante, pois pode-se dirigir os testes substantivos dando maior atenção às áreas em que os controlos são fracos e a probabilidade de erros é maior.

5.2.1.1. Avaliação do Controlo Interno

Como parte da avaliação do risco de controlo, o auditor deve também efectuar uma avaliação preliminar que verifique se os controlos relacionados com os sistemas de informação são eficazes. Esta avaliação tem por base:

- Reuniões com o pessoal;
- Observação das operações relacionadas com a informática; e
- Revisão de políticas e procedimentos da entidade.

Ao confiar nestas avaliações preliminares para planear os testes de auditoria, o auditor pode evitar o dispêndio de recursos nos testes de controlo que claramente não são eficazes.

A avaliação do controlo interno é realizada em três fases:

1. Avaliação e teste dos controlos gerais;
2. Avaliação e teste dos controlos das aplicações; e

3. Avaliação e teste dos controlos de utilização.

Estes controlos têm de ser eficazes para ajudarem a assegurar a fiabilidade, confidencialidade apropriada e a disponibilidade da informação crítica automatizada.

O auditor avalia e testa a eficácia dos controlos através da utilização de diversas técnicas, descritas no ponto 4 do capítulo II. Estas incluem:

- A observação do funcionamento e execução dos controlos;
- A análise da documentação relacionada com os controlos;
- Discussão dos controlos com os funcionários; e
- Questionários, inquéritos e inspecções.

5.2.2. Testes Substantivos

Teste para determinar se certos dados produzidos por um sistema são válidos e fiáveis. Não estabelecem a existência ou adequabilidade dos controlos de sistema ou se tais controlos estão em conformidade, mas podem indicar fraquezas de controlo.

Destinam-se a confirmar o adequado processamento comparado com o suporte documental das operações, análises de pormenor de transacções e dos procedimentos analíticos (análises de rácios e tendências significativas).

Segundo Banha (2005), o nível de materialidade seleccionando pelo auditor, juntamente com a avaliação do risco da auditoria, estão em relação directa com a profundidade dos testes a realizar, sobretudo no que se refere aos testes substantivos.

CAPÍTULO III: METODOLOGIA PARA AUDITORIA DE SISTEMA DE INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA – ESTUDO DE CASO IGF

1. APRESENTAÇÃO DA IGF

1.1. Missão e competências

Segundo o Decreto nº 40/99 de 29 de Junho, a Inspecção Geral de Finanças (IGF) é um órgão de controlo superior financeiro do Estado e de apoio ao Ministro que superintende a área das Finanças no âmbito da gestão dos fundos públicos e controlo patrimonial.

A IGF é parte integrante do Ministério das Finanças e funciona na directa dependência do respectivo Ministro.

A IGF tem como atribuições fundamentais realizar o controlo da administração financeira do Estado, incumbindo-lhe o exercício do controlo nos domínios orçamental, financeiro e patrimonial, de acordo com os princípios da legalidade, regularidade e da boa gestão financeira, contribuindo para a economia, a eficácia e a eficiência na obtenção das receitas e na realização das despesas públicas nacionais.

A IGF exerce a sua actividade em todo o território nacional e nas missões ou delegações do País no exterior.

No âmbito do controlo orçamental, financeiro e patrimonial cumpre à IGF:

a) Realizar inspecções/Auditorias aos órgãos do Estado, suas instituições e pessoas colectivas de direito público ainda que personalizados, incluindo as autarquias locais;
b) Efectuar inspecções/auditorias a empresas públicas, estatais e mistas onde o Estado detenha participação no respectivo capital, com excepção das instituições de crédito, parabancárias e de seguros;
c) Efectuar, mediante despacho do Ministro que superintende a área das Finanças, auditorias ou exames à escrita das empresas e entidades privadas ou cooperativas, quando sejam sujeitas de relações financeiras ou tributárias com o Estado ou quando se mostre indispensável ao controlo indirecto de quaisquer entidades objecto de intervenção da IGF;
d) Proceder a inquéritos e sindicâncias superiormente determinados ou por conhecimento directo de matéria pertinente no decurso das suas actividades;
e) Levantar autos de transgressão quando, no decurso ou em resultado de inspecções, inquéritos ou sindicâncias, se detectem infracções às leis fiscais;

f) Acompanhar a adopção e implementação de medidas por si propostas;
g) Exercer quaisquer funções que lhe sejam ou venham a ser atribuídas por lei.

1.2. Estrutura Orgânica Actual da IGF

Ainda de acordo com o Decreto nº 40/99 de 29 de Junho a IGF é dirigida por um Inspector-Geral, coadjuvado por um Inspector Geral Adjunto, ambos nomeados por despacho do Ministro que superintende a área das Finanças.
O anexo 3 ilustra a estrutura orgânica da IGF, que compreende cinco departamentos, uma repartição e duas delegações regionais, designadamente:

a) Departamento de Inspecção aos Órgãos do Estado e suas instituições (DIOE)
Compete a este departamento proceder com inspecção ou auditoria respeitantes à gestão e à situação económico-financeira de quaisquer serviços públicos e suas instituições subordinadas, incluindo instituições com autonomia administrativa, financeira e patrimonial.

b) Departamento de Inspecção às Autarquias (DIA)
Compete fiscalizar a legalidade da gestão financeira e patrimonial das autarquias, incluindo serviços municipalizados e empresas públicas municipais e das associações ou federações autárquicas.

c) Departamento de Auditoria às Empresas (DAE)
Efectua inspecções ou auditorias às empresas públicas e estatais, às associações de capitais públicos e empresas de capitais mistos, com excepção das instituições de crédito, parabancárias e seguros.

d) Departamento de Inspecção aos sectores Tributário e Aduaneiro (DITA)
Inspecciona as Direcções Nacionais de Tesouro, Imposto e Auditoria e das Alfandegas, no que refere a gestão dos recursos humanos e, controlo e execução orçamental, contabilístico, patrimonial, da receita, da despesa e das actividades subsidiarias com elas relacionadas.

e) Departamento Técnico (DT)
Ao DT compete efectuar estudos sobre matérias de interesse da IGF e promover a realização de projectos de interesse para o organismo; providenciar apoio técnico às equipas de inspecção;

promover acções de formação; coordenar a utilização de meios informáticos e apoiar o desenvolvimento das aplicações informáticas;

f) Repartição de Administração e Finanças (RAF)

À RAF compete conceder todo apoio logístico e burocrático à IGF.

g) Delegação Regional Centro (DRC) e Delegação Regional Norte (DRN)

Às delegações regionais, compete-lhes apoiar o desenvolvimento das acções promovidas pelos departamentos operacionais e executar tarefas de carácter administrativo inerentes ao seu funcionamento.

1.3. Destinatários dos Produtos da IGF

Os principais destinatários dos produtos da IGF são o Ministro das Finanças e os outros membros do Governo. Porém, poderão existir outros interessados no trabalho desenvolvido pela IGF, tais como a Procuradoria-Geral da República, o Tribunal Administrativo, as entidades auditadas e os doadores.

2. CARACTERIZAÇÃO DO AMBIENTE DE INTERVENÇÃO DA IGF

Para a obtenção da informação foi utilizado um questionário, anexo 1, dividido em cinco áreas designadamente: Auditoria e Controlo Interno, Organização do Sector de Informática, Infra-estrutura Aplicacional, Infra-estrutura Tecnológica e Utilização da Internet e Correio Electrónico.

O inquérito foi realizado nos meses de Março, Abril e Maio de 2007, na cidade de Maputo, visto possuir mais de 50% do parque informático nacional[5]. O estudo centrou-se em instituições como ministérios, empresas públicas, institutos públicos e outras de nível central.

No total foram enviados 47 questionários às instituições, dos quais obteve-se 34 respostas, o que corresponde a uma taxa de adesão de 72,3%, conforme ilustra a tabela 1.

Os resultados que se apresentam seguem a sequência do questionário, descrita anteriormente, anexo 1.

[5] Segundo o 1º Inquérito Nacional sobre a Capacidade Informática do País, realizado no ano 2000, ficou demonstrado que mais de 50% do parque informático nacional está concentrado na cidade capital. (Politica de Informática)

2.1. Auditoria e Controlo Interno

De referir que apesar de maior parte das instituições, abrangidas pelo estudo, possuírem órgãos de controlo (*Quadro 1 do anexo 4*), cerca de 76 % não realizam auditoria no ambiente informático o que representa preocupação sabidos os investimentos realizados nesta área e os riscos inerentes à utilização das tecnologias de informação. Importa referir que mesmo as instituições que realizam auditoria no seu ambiente informático, 44% não o fazem com periodicidade.

2.2. Organização do Sector de Informática

Dos dados obtidos relativamente à Organização dos Sectores de Informática (Quadro II do Anexo 4), constata-se que 9% das instituições com particular destaque para os Ministérios não possuem sectores de informáticas, apesar de serem detentoras e utilizadores de recursos computacionais (computadores, aplicações informáticas, entre outros). Verifica-se ainda que 65% das instituições possuem contratos de assistência técnica tanto de *hardware* como de *software*. De referir que boa parte das instituições, 65% trabalham na base de um plano estratégico.

2.3. Infra-Estrutura Tecnológica e Aplicacional

Os dados obtidos relativamente à infra-estrutura tecnológica e aplicacional existentes a nível das instituições inquiridas (Quadro III e IV do Anexo 4) permitem constatar que:

- Dos computadores existentes, 79% são da família do *Pentium* III e IV, o que parece indicar que, apesar dos condicionalismos existentes, há um esforço de apetrechamento do parque informático. Será interessante tentar relacionar a frequência com que são actualizados os equipamentos com a facilidade de se obter financiamentos para investimentos realizados nesta área.
- Cerca de 88 % das instituições possuem rede interna, sendo que a maioria dessas redes estão ligadas à Internet.
- Todos os inquiridos utilizam o sistema operativo *windows* nos postos de trabalho. Os outros sistemas operativos como *Linux, Solares, Unix, Macintosh, Novell* e outros são usados nos sectores de informática muitas vezes em servidores, com excepção do e-SISTAFE que utiliza o *linux* como sistema operacional no posto de trabalho.

2.4. Utilização da Internet e Correio Electrónico

Do total das instituições inquiridas, 56% possuem correio electrónico interno suportado por meios tecnológicos da instituição e nessas instituições a percentagem dos funcionários que utilizam o correio electrónico aproxima-se aos 100% (Quadro V do Anexo 4).

A Internet é um meio a que a Administração Pública pode recorrer, quer como utilizadora quer como prestadora de serviços.

Na perspectiva de utilizadora, a percentagem de instituições com ligação à Internet é de 97%, Quadro IV do Anexo 4.

Na perspectiva de prestadora de serviços, a percentagem de organismos que disponibiliza informação/serviços na Internet é de 65%, destes 68% suportam estes serviços com recursos tecnológicos próprios, isto é, possuem a *Página Web* alojada na instituição (Quadro V do Anexo 4).

2.5. Considerações Gerais

Apesar das dificuldades encontradas na recolha da informação, para o presente estudo, o inquérito cobriu uma parte significativa dos Ministérios (64 %) o que permitiu obter uma visão geral do ambiente de actuação da IGF na vertente das Tecnologias de Informação e Comunicação (TIC).

De referir que as instituições do sector público, a nível da infra-estrutura tecnológica e aplicacional, estão razoavelmente equipadas. Algumas instituições, com maior destaque para as empresas públicas, são detentoras de aplicações de suporte para recursos humanos, contabilidade e finanças e outras áreas operacionais.

As instituições do Estado sem autonomia financeira, administrativa e patrimonial, estão de forma paulatina a integrar o novo Sistema de Administração Financeira do Estado (SISTAFE), o que significa que a IGF terá de envidar esforços de forma a lidar com este novo ambiente. Prevê-se, ainda, a integração de outras instituições como Municípios e Institutos Públicos.

A nível das instituições que tem por vocação a arrecadação de receitas do Estado, como as Direcções Gerais das Alfandegas e dos Impostos, verifica-se também um esforço na automatização dos seus processos de negócio, exemplos disso são os sistema TIMS (DGA) e SICR e NUIT (DGI).

A maior parte das instituições está conectada em redes de computadores e estas à Internet. Possuem correio electrónico interno e tem presença na Internet através das páginas *Web.*

Com a efectivação da rede electrónica do Governo (GovNet), levado a cabo pela Comissão Para a Politica de Informática, que visa a interligação das instituições do Governo, prevê-se que num futuro breve, maior parte das instituições que não detêm servidores de correio electrónico possam vir a beneficiar-se deste projecto, uma vez que presta serviços nesta área.
Este cenário poderá levar a que, caso se crie regulamentação para tal, uma percentagem razoável das interacções/contactos entre instituições da Administração Pública se façam prioritariamente de forma electrónica.

3. PROCEDIMENTO ACTUAL DE REALIZAÇÃO DE AUDITORIA

O procedimento de auditoria efectuado pela IGF compreende as fases de planificação, execução e elaboração de relatório, descritas a seguir:

3.1. Fase de Planificação

Nos finais de cada ano, todos os departamentos/delegações da IGF, iniciam o processo de preparação do plano anual de actividades para o ano seguinte. Os Departamentos operacionais e as Delegações submetem ao Departamento Técnico as propostas do plano de actividades a nível do departamento/delegação para compilação. Estas propostas são discutidas em Colectivo de Direcção, no qual participam todos os chefes dos departamentos/delegados, chefe da RAF e alguns técnicos convidados, sendo depois submetida ao Ministro das Finanças para homologação.
O Plano de Actividades aprovado pelo Ministro das Finanças, é divulgado em todos órgãos da instituição para o seu conhecimento e execução. A partir daí, os departamentos operacionais elaboram propostas de equipas de auditoria e submetem à apreciação e aprovação do Inspector-geral. Uma vez designada a equipa que irá executar uma determinada acção, esta inicia o processo de planificação para execução dos trabalhos, recolhendo toda a documentação/legislação relacionada com a instituição que será objecto da auditoria. Deste processo, resulta o programa de auditoria, no qual, dentre outras informações devem constar os integrantes da equipa, os recursos necessários, estimativas de prazos, objectivos da auditoria, áreas de intervenção, entre outros. O programa de auditoria, elaborado pela equipa, é submetido à apreciação do chefe do departamento.
Neste processo de preparação da execução da auditoria, envolve-se também a RAF, com vista a criar condições logísticas necessárias à realização da acção. Antes de a equipa deslocar-se à instituição a auditar, recebe uma credencial que a legitima a realizar a auditoria.

3.2. Fase de Execução

Chegada à instituição, a auditar, a equipa apresenta-se ao dirigente ou representante ao qual é exposta a credencial passada pela IGF e são dados os esclarecimentos sobre os objectivos e objecto da auditoria. É, ainda, solicitado à instituição a indicação de uma sala de trabalhos para a equipa e indivíduos que interagirão com a equipa durante a realização da auditoria. Nesta etapa, faz-se o levantamento, verificações, avaliação do controlo interno e recolha das evidências. Se necessário, são solicitados esclarecimentos à instituição relativamente às irregularidades detectadas. Durante esta fase a equipa é acompanhada por um supervisor ou chefe do departamento, para ajudar a dissipar possíveis dificuldades e garantir que os objectivos da auditoria sejam alcançados.

3.3. Fase de Elaboração do Relatório

As constatações apuradas são apresentadas num relatório onde, também são indicadas as recomendações e conclusões a que se chegou com a realização da auditoria. Normalmente, o relatório da auditoria é elaborado na IGF, apesar de a equipa de auditoria proceder à apresentação de um breve resumo do trabalho realizado ao dirigente da instituição antes de deixar a mesma. O relatório é submetido ao chefe do departamento para apreciação e posterior submissão ao Inspector-Geral. Em seguida, o relatório de auditoria é enviado à instituição auditada para num prazo de 15 dias se pronunciar em relação às constatações do relatório. A equipa que realizou a auditoria procede a consolidação do relatório com base nos comentários recebidos da instituição auditada.

O relatório consolidado, segue ao Ministro das Finanças para Despacho e seguidamente é dado a conhecer à instituição auditada e a outros intervenientes (relatório com despacho do Ministro) para o seu cumprimento.

3.4. Resumo das constatações/ Deficiências no Processo Actual

No actual processo de realização de auditorias na IGF, podem-se destacar as seguintes situações:

- Ausência do planeamento de auditorias de SI

  Até ao momento, este tipo de auditoria não é realizado. Em alguns casos, no decurso de uma auditoria financeira normal, se os auditores, se depararem com um sistema informático onde se duvida da conformidade da informação financeira fornecida, proveniente de tal sistema, solicitam o apoio dos técnicos de informática para auxiliarem nas avaliações. Contudo, as

acções de auditoria de SI devem ser planificadas e constarem do Plano de Actividades da instituição.

- Nº demasiado reduzido de técnicos de informática
  Actualmente, a IGF possui um efectivo de três técnicos de informática, afectos ao Departamento Técnico. Este nº é insuficiente se se partir do princípio de que os mesmos, para além do apoiar as equipas de auditoria no terreno, desempenham outras tarefas, algumas de carácter rotineiro tais como: desenvolvimento e manutenção de aplicações, gestão da infra-estrutura de rede, manutenção de equipamento informático, apoio aos utilizadores, etc.

- Ausência no organigrama da IGF de um sector de auditoria de SI
  A existência deste sector na IGF iria possibilitar a realização de auditorias especializadas na área de SI e permitir que os seus integrantes desenvolvessem habilidades e competências técnicas com foco nesta área.

- Falta de operacionalização do Centro de Documentação
  Existe um Centro de Documentação que não está sendo explorado devido ao facto desta não conter bibliografia actual e de interesse para os auditores. Segundo Dias (2000), o grupo de auditores de SI e demais auditores de uma instituição deve ter, a sua disposição, uma biblioteca técnica para consulta. Dessa forma poderão orientar seus trabalhos de acordo com os padrões conhecidos na área, manter-se actualizados com relação as novas tecnologias e utilizar publicações técnicas como fonte de consulta durante a auditoria e na elaboração do relatório.

- Ausência de um sector para velar pela qualidade dos relatórios
  Este sector é de vital importância para organizações deste tipo uma vez que os auditores trabalham com matérias sensíveis que afectam a vida de pessoas e instituições, sendo assim importantíssima a revisão dos relatórios de auditoria por pessoal especializado.

- Ausência de procedimentos para acompanhamento das recomendações
  Actualmente, não existe uma forma uniforme e padronizada para o processo de acompanhamento das recomendações, muitas vezes os auditores aproveitam saber do que foi feito durante a realização de acções de auditorias normais, o que não deveria ser pois, esta é

também uma verdadeira acção de auditoria que procura saber o estado de implementação das recomendações emanadas nos relatórios de auditoria.

- Ausência de uma metodologia de auditoria de SI

  A ausência de uma metodologia de auditoria de SI padronizada, acarreta acções desordenadas realizadas por um mesmo órgão, com critérios de avaliação diferentes e, muitas vezes, para um mesmo tipo de constatação, recomendações incoerentes e conflituosos.

4. METODOLOGIA PROPOSTA

Analisadas as deficiências apresentadas no procedimento actual de auditoria, efectuada pela IGF, e tendo estudado os referenciais metodológicos apresentado no ponto 3 do capítulo II e tendo como ponto de partida a natureza e missão da IGF, se apresenta a metodologia proposta.

Referir igualmente que grande parte da metodologia baseou-se no referencial metodológico COBIT por ser, segundo Gomes (2007), o referencial mais adequado para a auditoria de SI.

Esta metodologia segue igualmente as quatro fases (boas práticas) propostas por organizações internacionais de auditoria como são os casos do IIA, INTOSAI, ISACA, entre outros, abordadas no Capítulo II.

Foi desenvolvido um fluxograma representado na Figura 8, na qual cada fase se desdobra em uma série de actividades, as quais estão descritas a seguir:

4.1. Fase de Planeamento

Nos finais de cada ano, o responsável pelo sector de auditoria de SI, em coordenação com a sua equipa, deve identificar as acções que o sector irá realizar com base em critérios previamente definidos pela instituição e submeter ao Departamento Técnico. Desta forma, assegura que todas as suas acções estejam contidas no Plano de Actividade aprovado pelo Ministro das Finanças.

Nesta fase, deve-se definir os objectivos das acções de auditoria, áreas objecto de intervenção, estimativas de tempo, técnicos e custos necessários para a realização da acção e alocação de recursos às acções.

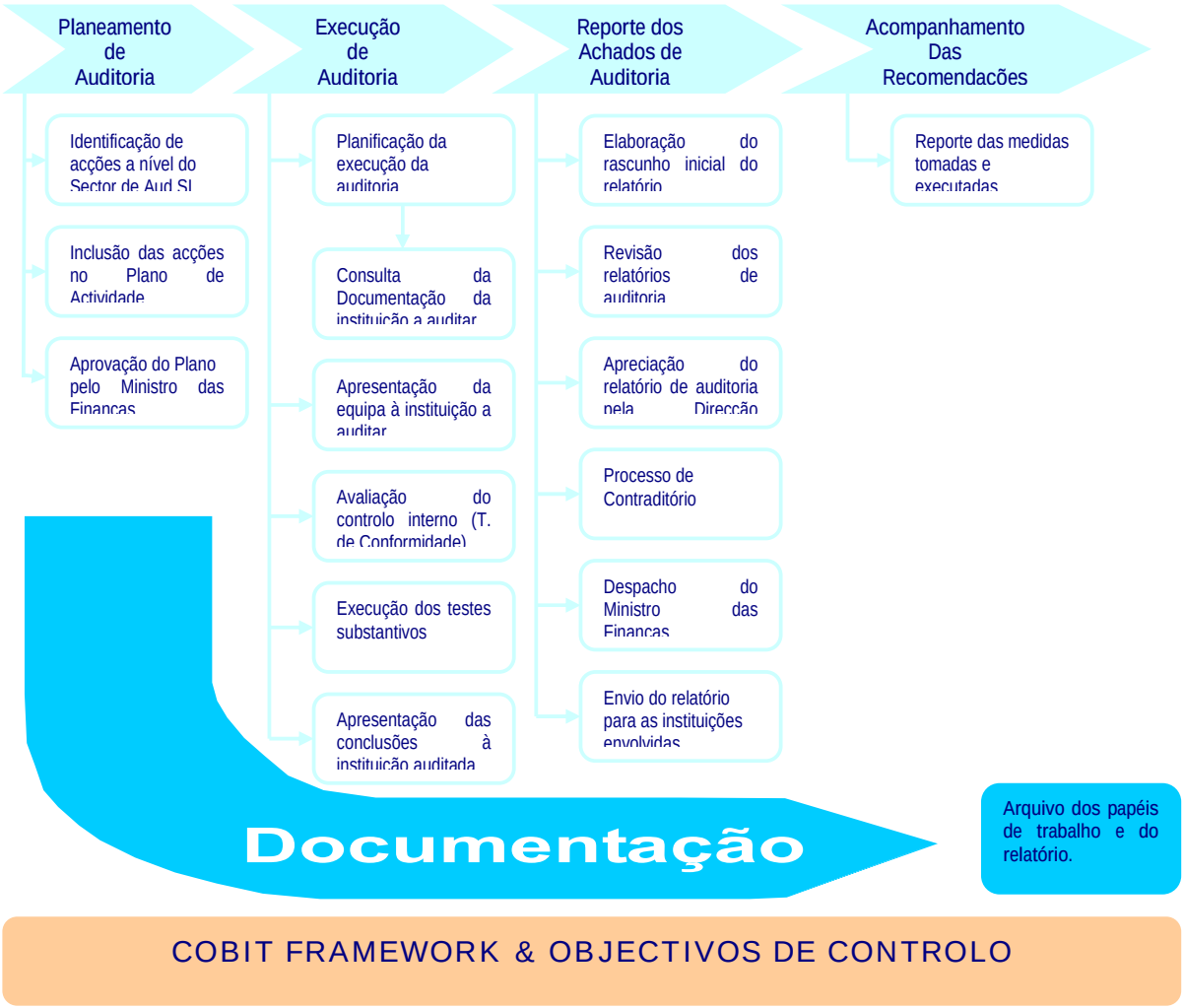


Figura 8: Fluxograma da Metodologia proposta

4.2. Fase de Execução

Conforme ilustrado na Figura 8, esta etapa compreende cinco passos descritos abaixo.

- ✓ Planificação da execução da auditoria – elabora – se o programa de trabalho que é a definição detalhada dos objectivos, procedimentos e tarefas específicas. Para isso é necessário a efectivação de levantamentos iniciais como consulta da documentação da instituição a auditar (Legislação, relatórios de auditoria anteriores e outros dispositivos).

- ✓ Apresentação da equipa à instituição a auditar – antes de iniciar os trabalhos de auditoria na instituição a auditar, a equipa de auditores deve-se apresentar aos responsáveis da instituição. É nesta ocasião onde são apresentados os objectivos da auditoria, é solicitada a colaboração e criação de condições de trabalho.

- ✓ Avaliação do controlo interno (Testes de Conformidade) – o auditor precisa conhecer a estrutura organizacional do sector, a distribuição de tarefas, o fluxo e natureza do trabalho. Este conhecimento deve ser consubstanciado com os objectivos de controlo COBIT que definem os processos agrupados em domínios. Desta forma poder-se-á efectuar uma avaliação geral do controlo interno com o auxílio de várias técnicas (descritas no nº 4 do capítulo II) como observação, entrevistas, questionários. A título de exemplo, o anexo 5 apresenta um *checklist*, desenvolvido com recurso ao referencial COBIT, que pode ser usado para avaliação dos controlos gerais.

- ✓ Execução dos testes substantivos – estes testes poderão ser realizados com recurso a várias técnicas (descritas no nº 4 do capítulo II). Normalmente são feitos por amostragem. De referir que neste processo serão solicitados dados na forma electrónica para a efectivação dos testes. Porém, se não se tomarem precauções e adoptar-se procedimentos de controlo dos dados recebidos, estes poderão tornar-se em pontos de discórdia com o auditado colocando em causa os resultados do trabalho realizado. Daí que seja importante a utilização de um formulário que descreva e classifique a informação recebida. O anexo 2 é um exemplo de um modelo de formulário desenvolvido com base no referencial COBIT e que pode ser utilizado para descrição dos dados transferidos (recebidos).

- ✓ Apresentação das conclusões à instituição auditada – segundo Dias (2000), no final dos trabalhos de auditoria, a equipa deve se reunir novamente com os dirigentes da instituição auditada. Nessa ocasião, são feitos agradecimentos à colaboração da direcção e seus funcionários e são relembrados os objectivos da auditoria como também, se apresenta um resumo dos resultados da auditoria.

No decurso deste processo deve-se documentar todo processo de auditoria e assegurar a recolha da documentação relevante que servirá de evidência para suportar a opinião do auditor.

4.3. Fase de Elaboração do Relatório

Nesta etapa, é importante o registo dos diversos estágios do relatório com vista a garantir o seu acompanhamento. Conforme ilustrado na Figura 8, o relatório passa por seguintes estágios:

- ✓ Elaboração do projecto inicial do relatório;
- ✓ Revisão dos relatórios de auditoria – o relatório reflecte a imagem do auditor e do órgão de auditoria. Com vista a garantir a qualidade do trabalho realizado, é necessário que o mesmo seja revisto por profissionais formados nas áreas de letras;
- ✓ Apreciação do relatório de auditoria pela Direcção – tanto o chefe do sector de auditoria de SI como o Inspector-Geral de Finanças, precisão de apreciar o trabalho feito por forma a assumi-lo como da Instituição;
- ✓ Processo de Contraditório – este processo permite esgotar os possíveis pontos de discórdia com o auditado, consolidando desta forma a informação do relatório de auditoria.
- ✓ Despacho do Ministro das Finanças;
- ✓ Envio do relatório para as instituições envolvidas – o relatório com Despacho do Ministro das Finanças é encaminhado pela IGF para todos os interessados pelos resultados da auditoria (auditado, doadores, Procuradoria Geral da República, Tribunal Administrativo, etc).

4.4. Fase de Acompanhamento

O processo de auditoria não termina com a entrega do relatório, é preciso monitorar a implementação das recomendações emanadas. A IGF deve estabelecer procedimentos gerais que incluem prazos para a instituição auditada informar as meditas tomadas face as recomendações, verificação e avaliação da resposta. Os referidos procedimentos devem incluir, também, visitas e reuniões com o auditado.

	Cod Relatorio:			
	Nome da Instituição Auditada:			
	Tipo de Acompanhamento:			
Datas de	Despacho	Comunicação	Acompanhamento	
Ref	**Recomendação**	**Medidas Tomadas**	**Observações IGF**	**Avaliação IGF**
1				
2				
...				

Tabela 6: Monitorização das Recomendações

Para situações de falta de cumprimento ou de tomada de medidas inadequadas, a IGF deve comunicar essas revelações para instituições apropriadas para a tomada de acções correctivas tais como (consoante os casos) o Governo através do Ministro das Finanças, Procuradoria Geral da República, para casos de matéria criminal e Tribunal Administrativo para situações de responsabilidade financeira.

As acções de acompanhamento, podem ser feitas no gabinete (o auditado envia a informação sobre as acções tomadas) ou no campo (os auditores visitam a instituição auditada). O quadro da tabela 6, apresenta alguns elementos a ter em conta no processo de acompanhamento das recomendações. A IGF pode adoptar um quadro destes (tabela 6) para a monitorização das recomendações emanadas em seus relatórios.

4.5. Avaliação da Metodologia

Por forma a testar a metodologia proposta, foi feita uma experiência piloto no Departamento de Sistemas de Informação do Tribunal Administrativo (TA) que é um órgão superior da hierarquia dos tribunais administrativos, fiscais e aduaneiros.

O TA possui na sua estrutura orgânica um Departamento de Sistemas de Informação (DSI) constituído por 11 técnicos de nível superior e médio técnico. O mesmo está sedeado na Cidade de Maputo em três edifícios geograficamente dispersos. Estes edifícios possuem redes estruturadas de dados e estão conectados através de ligações dedicadas das TDM, que garantem a comunicação e a partilha de serviços através da rede. Existe uma sala de servidores centrais separada da sala de

operação dos técnicos, possuem ainda, algumas aplicações informáticas desenvolvidas localmente, dentre elas a de gestão de visto, uma *Intranet*, serviço de correio electrónico, serviço de *Internet*, página *Web*, serviço centralizado de antivírus, dentre outros.

4.5.1. Programa de Auditoria

Para a efectivação desta acção, foi desenhado um programa que compreendeu o planeamento de auditoria, obtenção e análise das evidências e relato.

- Planeamento de auditoria
  a) Tomar conhecimento do ambiente informático
  b) Entrevista a técnicos do sector
- Obtenção e análise das evidências
  a) Avaliação do Controlo Interno
  b) Definição da amostra a verificar
  c) Execução dos testes substantivos
- Relato das constatações

4.5.2. Desenvolvimento da acção

No processo de teste da metodologia foram usados *checklist* com perguntas fechadas de avaliação do controlo interno, dentre eles o anexo 5, como também entrevista a alguns técnicos de informática do TA. Porém, não foi possível efectuar os testes de conformidades e substantivos por motivos de protecção de informação.

Objectivo de Controlo	Total de Requisitos	Nº de Requisitos Aplicados pelo DSI	% de Requisitos Aplicados pelo DSI
Organização e Gestão Gerais	31	25	81%
Segurança Física	26	15	58%
Segurança Lógica	22	6	27%
Desenvolvimento e Manutenção de Sistemas	12	10	83%
Operação de Rotina da Instalação Central	23	14	61%
Telecomunicações	15	9	60%
Microcomputadores	13	8	62%
Planos de Emergência	10	0	0%

Tabela 7: Requisitos Aplicados Pelo DSI

Da apreciação global dos resultados de auditoria – piloto, resumidos na Tabela nº 7, revelou-se o seguinte:

- **Organização e Gestão Gerais**

A Estratégia das Tecnologias de Informação e Comunicação está alinhada com a estratégia da organização. As Políticas, Normas e Procedimentos, a separação de funções, a política de pessoal estão adequadamente previstas e em funcionamento. Neste item, apenas a auditoria de SI é que não tem sido realizado. No geral, 81% dos requisitos são aplicados pelo DSI.

- **Segurança Física**

No que se refere a este Item, foi verificado que 58% dos requisitos de segurança estão implementados, o que significa que algumas medidas preventivas e de detecção de danos físicos, acidentais ou deliberados, causado às instalações informáticas estão implementados, apesar de não ser de forma efectiva.

- **Segurança lógica para os dados ou servidores de aplicações**

Aqui foi onde se verificou haver maior fraqueza nos controlos implementados, que é de 27% dos requisitos aplicáveis. Este facto deve-se essencialmente, dentre outros factores, a falta de um responsável pela segurança e do acesso ilimitado ao pessoal de desenvolvimento ao ambiente de produção.

- **Desenvolvimento, programação e manutenção dos sistemas**

Neste item, constatou-se a existência de planos e manuais de procedimentos para orientar os trabalhos de desenvolvimento e teste dos sistemas. Em termos de cumprimento dos requisitos para o desenvolvimento, a situação é considerada boa, 83%.

- **Operação de Rotina**

Os recursos informáticos são supervisionados e são efectuados cópias de segurança dos ficheiros de dados de modo a proteger contra a perda de informação. O DSI cumpre com 61% dos requisitos para este item.

- **Telecomunicações**

Neste item verificou-se que o DSI cumpre com cerca de 60% dos requisitos. Foi, ainda, constatado que estão instaurados alguns procedimentos destinados a salvaguarda das redes de telecomunicações.

- **Microcomputadores**

No que se refere aos microcomputadores, constatou-se que o DSI situa-se na ordem dos 62% o que significa que existem procedimentos relativos às condições de aquisição, utilização e controlo dos microcomputadores e do suporte lógico associado mesmo que não sejam efectivos.

- **Planos de emergência**

O DSI não possui um plano de emergência para a salvaguarda das aplicações informáticas fundamentais e para a recuperação dos serviços informáticos após interrupções imprevistas. Esta é uma grande fraqueza detectada.

4.5.3. Considerações Gerais

No geral, o ambiente de controlo interno do DSI, pode ser considerado como razoável tendo em conta que em termos médios o DSI cumpre com cerca de 54% dos requisitos aplicados pela metodologia.

Com base na experiência efectuada e da facilidade de assimilação desta metodologia e da sua aplicabilidade no terreno, pode-se afirmar que é adequada e pode ser implementada em qualquer tipo de instituição, quer seja ela pública ou privada, seja de pequeno ou grande porte, ou ramo de actividade, precisando apenas de algumas adaptações naquilo que não for aplicável. De realçar, ainda, que a metodologia apresentou-se bastante eficaz, pois, através das planilhas resultantes da mesma foi possível avaliar o ambiente do controlo interno, identificando os pontos fortes e fracos dos controlos gerais, aplicacionais e de utilização.

CAPÍTULO IV: CONCLUSÕES E RECOMENDAÇÕES

1. CONCLUSÕES

Como resultado do presente estudo conclui-se o seguinte:

- Existem vários referenciais metodológicos aplicados à auditoria de sistemas de informação, contudo o referencial COBIT é o mais adequado para a auditoria pelas seguintes razões:
  - ✓ Na sua génese esteve a necessidade de criar um referencial para auditar os processos de SI;
  - ✓ A entidade responsável pela elaboração do COBIT é uma Associação de Auditores de SI (ISACA), o que não acontece com os outros dois referenciais designadamente ITIL e ISO 17799;
  - ✓ O COBIT possui uma visão de gestão dos processos de SI e privilegia o alinhamento destes com o negócio;
  - ✓ 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 de controlos de SI poderão ser auditados.

- Boa parte das instituições públicas são detentoras e utilizadoras das tecnologias de informação e comunicação e num futuro próximo poder-se-á ter mais instituições a utilizar plenamente as TICs. Daí que a IGF precisa estar preparada para acompanhar as mudanças que estão a acontecer no seu campo de actuação;

- A metodologia proposta permite avaliar os Sistemas de Informação quanto à sua integridade e segurança, bem como, quanto à sua eficácia e eficiência. Pode ser aplicada por órgãos de auditoria interna como a IGF.

Importa também, referenciar que o presente trabalho não teve, em momento algum, a pretensão de ser um manual sobre auditoria. O tema é extremamente amplo e dinâmico, o que se pretendeu foi trazer um instrumento metodológico que de forma geral pudesse delinear directrizes de realização de auditoria de SI. O mesmo está aberto a mais contribuições no sentido de enriquece-lo principalmente os aspectos que não foram suficientemente tratados.

2. RECOMENDAÇÕES

Como recomendações, propõem-se que se:

- continue com o presente estudo por forma a melhorar e desenvolver ainda mais os instrumentos metodológicos, com base no referencial COBIT, para auditoria de SI;

- apresente a metodologia proposta à IGF e respectiva auscultação das opiniões em relação a este, de forma a avaliar a aceitação e enriquecimento do mesmo;

- recrute técnicos de informática com nível superior e a sua capacitação em matérias de auditoria de SI.

- crie um sector de informática estruturado em três áreas funcionais designadamente:
    - Desenvolvimento – com responsabilidades para desenvolver e manter aplicações informáticas, bases de dados da instituição, página de Internet,
    - Infra-estrutura – para garantir a gestão de toda a infra-estrutura de rede interna e serviços de correio electrónico, assegurar o apoio técnico aos utilizadores, e
    - Auditoria e Apoio Externo – com competências para realizar auditorias de sistemas de informação e conceder apoio especializado às equipas no terreno;

- crie e operacionalize um sector responsável pela revisão e garantia de qualidade dos relatórios de auditoria;

- desenvolva e implemente procedimentos institucionais para acompanhamento das recomendações; e

- reactive e se apetreche o Centro de Documentação com obras actuais de auditoria.

BIBLIOGRAFIA

- ARAÚJO, Inaldo da Paixão, at all (2005), **Código de Ética e Normas de Auditoria**, **INTOSAI**, Estocolmo – Suécia.

- AU312 (2006), **Audit Risk and Materiality in Conducting an Audit,** Disponível em http://www.pcaobus.org/standards/interim_standards/auditing_standards/au_312.html, Consultado em 5 de Julho de 2006.

- BANHA, Francisco (2005), **Procedimentos de Auditoria,** Disponível em http://www.gesbanha.pt/revisao/4r9798/sld001.htm, Consultado em 30 de Maio de 2005.

- BANZE, Marta, at all (2003), **Curso Prático de Auditoria,** Ernest&Young, Maputo - Moçambique.

- CARNEIRO, Alberto (2004), **Auditoria de Sistemas de Informação**, 2ª edição, Editora FCA, Lisboa – Portugal.

- COUTINHO, Pedro Célio Borge Rodrigo (2007), **Trabalho de Mestrado - Análise de Sistemas de Detecção de Intrusos em Redes de Computadores,** Universidade de Franca, Franca – Brasil.

- Decreto nº 40/99 de 29 de Junho que aprova o Estatuto Orgânico da Inspecção-Geral de Finanças (Conselho de Ministros)

- DIAS, Cláudia (2000), **Segurança e Auditoria da Tecnologia da Informação**, Axcel Books, Rio de Janeiro – Brasil.

- DUARTE, Jorge, at all (2006), **Métodos e Técnicas de Pesquisa em Comunicação**, 2ª edição, Editora Atlas, São Paulo – Brasil.

- GODY, José António de, at all (1999), **Auditoria Por Meios Electrónicos - 11**, Editora Atlas, São Paulo – Brasil.

- GOMES, Pedro Manuel (2007), **Trabalho de Mestrado - A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências**, Universidade do Minho, Minho – Portugal.

- IIA (2004), **O Enquadramento de Práticas Profissionais de Auditoria Interna**, IIA, Florida – USA.

- ISACA (2006), **Padrões para Auditoria de Sistemas de Informação**, Disponível em http://www.isaca.org/Standards for IS Auditing (Portuguese).htm, Consultado em 24 de Julho de 2006.

- LEBLANC, K (2004), **The Big Picture: ITIL as an Integrated Framework", ITIL & ITSM Knowledge Base,** Disponível em http://www.itilworx.com/,Consultado em 10 de Abril 2007,

- LINTZ, Alexandre e MARTINS, Gilberto de Andrade (2000), **Guia para Elaboração de Monografias e Trabalhos de Conclusão de Curso,** 1ª edição, Editora Atlas, São Paulo – Brasil.

- MARTINS, Gilberto de Andrade (2007), **Manual para Elaboração de Monografia e Dissertações,** 3ª edição, Editora Atlas, São Paulo – Brasil.

- OLIVEIRA, José (2005) **Abordagem Metodológica à Auditoria a Sistemas de Informação,** Disponível em http://www.igf.min-finacas.pt, Consultado em 30 de Maio de 2005.

- SPAFFORD, G (2003) **The Benefits of Standard IT Governance Frameworks,** Disponível em http://www.itpi.org/, Consultado em 10 April 2007.

- TERZIAN, Françoise (2007), **Um Guia de Certificações e Melhores Práticas de TI,** Disponível em http://www.lyfreitas.com/pdf/Praticas%20de%20TI.pdf , Consultado em 15 de Abril de 2007.

- Wikimedia (2006), **History of information technology auditing**, Disponível em http://en.wikipedia.org/wiki/History_of_information_technology_auditing, Consultado em 10 de Novembro de 2006.

- Wikimedia (2010), **Metodologia**, Disponível em http://pt.wikipedia.org/wiki/Metodologia, Consultado em 6 de Abril de 2010.

ANEXOS

Anexo 1: *Questionário Dirigido às Instituições*

Universidade Eduardo Mondlane
Faculdade de Ciências
Departamento de Matemática e Informática

Questionário

O presente questionário tem por finalidade a recolha de dados, para elaboração do Trabalho de Licenciatura em Informática, **com o objectivo de avaliar o grau de implementação dos sistemas informáticos, na Administração Pública, e realização de auditoria nesses sistemas.**

NB: A informação recolhida não será usada para qualquer outro fim a não ser o indicado anteriormente.

Agradece-se a sua colaboração!

I. Identificação do Organismo

Denominação _____

II. Auditoria e Controlo Interno

1. Existe, no organismo, um órgão de controlo interno ou uma equipa de supervisão?
   Sim ☐ Não ☐
2. Quem realiza auditoria **aos sistemas informáticos/ambiente informático** do organismos?
   Auditores internos ou Uma equipa interna de TI ☐
   Consultores externos ou Empresa de auditoria contratada ☐
   Ambos ☐
3. Qual é a periodicidade em que se realiza as auditorias aos sistemas/ambientes informáticos no organismo?
   Semestralmente ☐ Anualmente ☐ Não Periódica ☐
   Outro ☐

III. Organização do Sector de Informático

1) Existe um plano estratégico das tecnologias de informação e comunicação, com a estratégia informática?
   Sim ☐ Não ☐
2) O desenvolvimento de novos sistemas está considerado no plano estratégico de informática?
   Sim ☐ Não ☐
3) Quais as áreas de informática e de soluções de suporte existentes?
   Desenvolvimento ☐ Infra-estrutura de rede e comunicações ☐
   Ambos ☐ Outra ☐

4) Indique se para a resolução dos problemas informáticos do organismo são utilizados os recursos seguintes:

Aquisição externa dos serviços ☐ Resolução interna ☐ Ambos ☐

5) O organismo possui contratos de assistência técnica relativamente a:

Conservação/manutenção de hardware ☐ Ambos ☐

Desenvolvimento e Manutenção de software ☐ Nenhum ☐

IV. Aplicações Informáticas

1) As aplicações existentes foram desenvolvidos:

Internamente ☐ No exterior ☐

Exterior e Internamente ☐ Não existem ☐

2) Essas aplicações possuem certificação de controlo interno concedida pelos auditores ou empresas de certificação?

Sim, possuem ☐ Não possuem ☐ Alumas possuem ☐

3) Está definido nos sistemas existentes algum percurso (trilho) de auditoria?

Sim ☐ Não ☐

4) Quais as áreas da instituição que estão informatizadas?

_____

_____

_____

V. Infra-estrutura Tecnológica

1) O Organismo possui computadores da família de:

Pentium I e II ☐ Pentium III e IV ☐ Outro ☐

2) Tipos de sistemas operativos que o organismo possui

Windows ☐ Windows e Linux ☐

Linux ☐ Outros ☐

3) Os microcomputadores estão conectados a outros sistemas?

Não ☐ Em rede local ☐ À Internet ☐

Outro ☐ Em rede local e à Internet ☐

VI. Utilização da Internet e Correio Electrónico

1) Meio de ligação à Internet

Ligação individual ☐ Partilhando uma ligação ☐

Ambos ☐ Não Possui ☐

2) O correio electrónico da instituição é suportado por meios (equipamento):

Externos ☐ Internos ☐ Não Possui ☐

3) A percentagem dos trabalhadores que possuem Correio Electrónico é aproximadamente a:

100% ☐ ***75%*** ☐ ***50%*** ☐ ***25%*** ☐

4) A Web *Site do* organismo está alojada:

No organismo ☐ Num outro organismo ☐ Não possui ☐

Anexo 2: Caracterização dos Dados Transferidos / Copiados

Universidade Eduardo Mondlane
Faculdade de Ciências
Departamento de Matemática e Informática

Descrição dos Dados Transferidos

1. Objectivo da cópia:

2. Formato dos dados

3. MODELO DE DADOS E CARACTERIZAÇÃO DE TABELAS:

3.1. Relacionamento das tabelas, no caso de existirem várias:

3.2. Estrutura das tabelas com dimensão dos campos e descrição sintética do seu conteúdo:

3.3. Número de registos incluídos em cada tabela:

3.4. Total e nome de um ou todos os campos numéricos da tabela

4. ORIGEM DOS DADOS

4.1. Principais características do computador:

4.2. Descrição sintética da base de dados ou sistema de informação a que as tabelas pertencem:

4.3. Departamento que controla o sistema de informação ou a base de dados:

4.4. Localização física dos dados (Sistema, Disco, Directório, etc):

4.5. Formato dos dados na origem:

5. CÓPIA DOS DADOS

5.1. Intervalo de tempo que os dados cobrem (DATA, HORA e MINUTOS):

5.2. Identificação e forma de contacto de quem copiou os dados (NOME e CARGO):

5.3. Data e Hora em que a cópia foi efectuada:

5.4. Processo utilizado para a cópia e versão dos comandos utilizados (TAR, CPIO, COPY, BACKUP, etc):

Data,

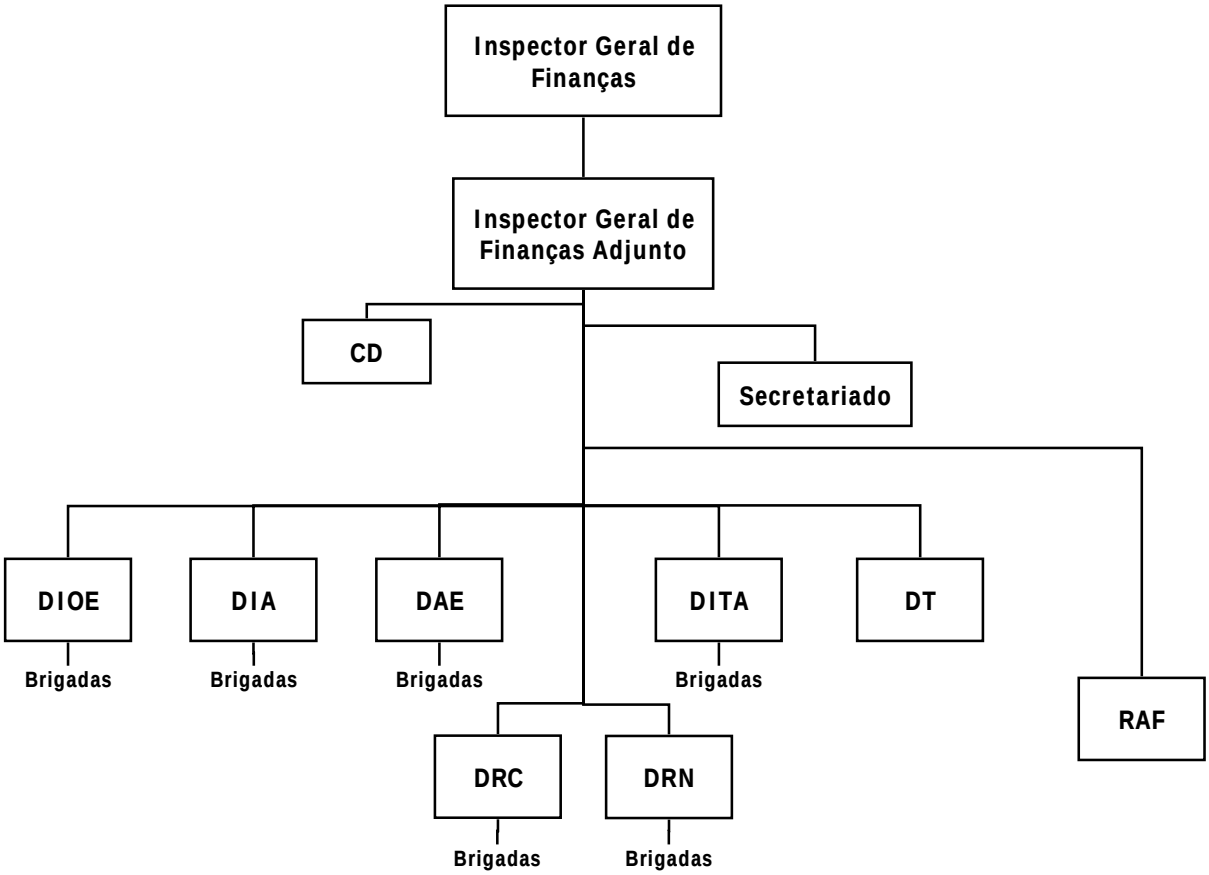
Nome legível e assinatura do responsável pelos dados na origem

_____

Nome legível e assinatura de quem recebe os dados

_____

Anexo 3: *Estrutura Orgânica da IGF*



Legenda

DIOE – Departamento de Inspecção aos Órgãos do Estado e suas instituições

DIA – Departamento de Inspecção às Autarquias

DAE – Departamento de Auditoria às Empresas

DITA – Departamento de Inspecção aos sectores Tributário e Aduaneiro

DT – Departamento Técnico

RAF – Repartição de Administração e Finanças

DRC – Delegação Regional Centro

DRN – Delegação Regional Norte

CD – Colectivo de Direcção

Brigadas – Equipas de Auditoria

ANEXO 4 - Resultados do Inquérito

Auditoria e Controlo Interno		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Existencia de orgao de CI	nao existe	0	13	25	63	24
	existe	54	8	23	15	76
Quem realiza Auditoria	equipa externa	14	0	29	57	21
	equipa interna	33	22	11	33	26
	ambos	50	0	50	0	18
	nao existe	58	8	17	17	35
Periodicidade de realização da Auditoria	nao periodica	27	13	33	27	44
	anualmente	43	0	14	43	21
	nao existe	58	8	17	17	35

Quadro I.A): Auditoria e Controlo Interno (Dados Percentuais)

Auditoria e Controlo Interno		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Existencia de orgao de CI	nao existe	0	1	2	5	8
	existe	14	2	6	4	26
Quem realiza Auditoria	equipa externa	1	0	2	4	7
	equipa interna	3	2	1	3	9
	ambos	3	0	3	0	6
	nao existe	7	1	2	2	12
Periodicidade de realização da Auditoria	nao periodica	4	2	5	4	15
	anualmente	3	0	1	3	7
	nao existe	7	1	2	2	12

Quadro I.B): Auditoria e Controlo Interno (Dados Numéricos)

Organização do Sector de Informática		Dados Percentuias Por Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Existencia do plano estrategico	nao existe	67	8	8	17	35
	existe	27	9	32	32	65
Areas Existentes	outra	75	0	0	25	12
	infaestrutura	38	25	0	38	24
	ambos	32	5	37	26	56
	não existe	67	0	33	0	9
Resolução dos problemas	externa	75	0	25	0	12
	interna	0	0	100	0	3
	ambos	38	10	21	31	85
Existencia de contratos	nenhum	58	17	8	17	35
	hardware	50	0	25	25	12
	software	33	17	33	17	18
	ambos	25	0	33	42	35

Quadro II.A): Organização do Sector de Informática (Dados Percentuais)

Organização do Sector de Informática		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Existencia do plano estrategico	nao existe	8	1	1	2	12
	existe	6	2	7	7	22
Areas Existentes	outra	3	0	0	1	4
	infaestrutura	3	2	0	3	8
	ambos	6	1	7	5	19
	não existe	2	0	1	0	3
Resolução dos problemas	externa	3	0	1	0	4
	interna	0	0	1	0	1
	ambos	11	3	6	9	29
Existencia de contratos	nenhum	7	2	1	2	12
	hardware	2	0	1	1	4
	software	2	1	2	1	6
	ambos	3	0	4	5	12

Quadro II.B): Organização do Sector de Informática (Dados Numéricos)

Infra-estrutura Aplicacional		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Aplicaçoes existentes	nao existem	88	13	0	0	24
	internamente	17	0	17	67	18
	no exterior	50	0	25	25	12
	interior e exterior	25	13	38	25	47
Possuem certificação	não possuem	29	10	19	43	62
	possuem	33	0	67	0	9
	alguns	0	0	100	0	6
	nao existe	88	13	0	0	24
Definido trilho de auditoria	não está definido	40	20	10	30	29
	esta definido	19	0	44	38	47
	não existem	88	13	0	0	24

Quadro III.A): Infra-estrutura Aplicacional (Dados Percentuais)

Infra-estrutura Aplicacional		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Aplicaçoes existentes	nao existem	7	1	0	0	8
	internamente	1	0	1	4	6
	no exterior	2	0	1	1	4
	interior e exterior	4	2	6	4	16
Possuem certificação	não possuem	6	2	4	9	21
	possuem	1	0	2	0	3
	alguns	0	0	2	0	2
	nao existe	7	1	0	0	8
Definido trilho de auditoria	não está definido	4	2	1	3	10
	esta definido	3	0	7	6	16
	não existem	7	1	0	0	8

Quadro III.B): Infra-estrutura Aplicacional (Dados Numéricos)

Infra-estrutura Tecnológica		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
tipos de computadores	actualizados	41	11	22	26	79
	ambos	43	0	29	29	21
Sistema operativo	windows	63	19	6	13	47
	ambos	22	0	39	39	53
Conectividade a outros sistemas	nao estao	100	0	0	0	3
	internet	67	0	0	33	9
	internet e rede local	37	10	27	27	88

Quadro IV.A): Infra-estrutura Tecnologica (Dados Percentuais)

Infra-estrutura Tecnológica		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
tipos de computadores	actualizados	11	3	6	7	27
	ambos	3	0	2	2	7
Sistema operativo	windows	10	3	1	2	16
	ambos	4	0	7	7	18
Conectividade a outros sistemas	nao estao	1	0	0	0	1
	internet	2	0	0	1	3
	internet e rede local	11	3	8	8	30

Quadro IV.B): Infra-estrutura Tecnologica (Dados Numéricos)

Utilização da Internet e Correio Electrónico		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Meio de ligação Internet	individual	100	0	0	0	12
	partilha	32	11	25	32	82
	ambos	50	0	50	0	6
correio electronico	nao existe	20	20	0	60	15
	interno	32	5	37	26	56
	externo	70	10	10	10	29
percentagem do pessoal com correio electronico	100%	27	18	27	27	32
	75%	46	0	31	23	38
	50%	60	0	20	20	15
	25%	40	20	0	40	15
Site da instituição	não possui	58	0	8	33	35
	numa outra instituição	43	0	29	29	21
	na instituição	27	20	33	20	44

Quadro V.A): Utilização da Internet e Correio Electronico (Dados Percentuais)

Utilização da Internet e Correio Electrónico		Tipo da Instituição				Total
		Ministerio	Instituto	Empresa	Outro	
Meio de ligação Internet	individual	4	0	0	0	4
	partilha	9	3	7	9	28
	ambos	1	0	1	0	2
correio electronico	nao existe	1	1	0	3	5
	interno	6	1	7	5	19
	externo	7	1	1	1	10
percentagem do pessoal com correio electronico	100%	3	2	3	3	11
	75%	6	0	4	3	13
	50%	3	0	1	1	5
	25%	2	1	0	2	5
Site da instituição	não possui	7	0	1	4	12
	numa outra instituição	3	0	2	2	7
	na instituição	4	3	5	3	15

Quadro V.B): Utilização da Internet e Correio Electronico (Dados Numéricos)

ANEXO 5: - AVALIAÇÂO DOS CONTROLOS GERAIS

Preparado por_____Revisto por _____/____/_____	Entidade: _____

Objectivo de Controlo Geral	Controlos	Avaliação do Controlo Chave	
		Efectivo/ Não Efectivo	Obs. / Refer
1. Organização e gestão gerais	A Estratégia das Tecnologias de Informação e Comunicação deve estar alinhada com a estratégia da organização. As Políticas, Normas e Procedimentos, a Separação de Funções, a Política de Pessoal e a Auditoria Informática devem estar adequadamente previstas e em funcionamento na organização das TIC		
2. SEGURANÇA fÍSICA	Qualquer dano físico, acidental ou deliberado, causado às instalações informáticas deve ser evitado através de medidas preventivas e detectado precocemente, afim de garantir protecção contra as eventuais consequências.		
3.Segurança lógica para os dados ou servidores de aplicações	O acesso aos dados e software deve ser limitado às pessoas e programas cujo o acesso foi autorizado, facto que deve estar registado nas pistas de auditoria.		
4. Desenvolvimento, programação e manutenção dos sistemas	A metodologia de desenvolvimento e de manutenção dos sistemas informáticos deve permitir dispor de sistemas eficazes e garantir a segurança dos dados em termos de confidencialidade, integridade, disponibilidade e de pistas de auditoria.		
5. Operação de rotina da instalação central	Os recursos informáticos devem ser supervisionados de modo a garantir a sua eficaz utilização, os ficheiros de dados devem ser protegidos contra a perda e devem ser criadas pistas de auditoria adequadas.		
6. Telecomunicações	Devem ser instaurados procedimentos destinados a salvaguardar as redes de telecomunicações.		
7. Microcomputadores	Devem existir procedimentos relativos às condições de aquisição, utilização e controlo dos microcomputadores e do suporte lógico associado.		
8. Planos de emergência	Devem existir planos testados para a salvaguarda das aplicações informáticas fundamentais e para a recuperação dos serviços informáticos após interrupções imprevistas.		

OBJECTIVO Nº 1 – ORGANIZAÇÃO E GESTÃO GERAIS					
Controlos	Procedimentos	Resultado			Observações/
		S	N	NA	Referências
1.1. Estratégia Informática e Gestão Global	1.1.1. Existe um plano director de informática, com a estratégia informática.				Pedir plano.
	1.1.2. A estratégia informática é da responsabilidade dos órgãos superiores de gestão do organismo? Quais?				
	1.1.3. A estratégia informática abrange um período temporal de 2 a 3 anos? Define objectivos a curto, médio e longo prazo?				
	1.1.4. A estratégia informática é baseada no plano de negócios da organização incluindo objectivos gerais, metas e estratégias.				
	1.1.5. A estratégia informática contempla a manutenção da infraestrutura física e lógica, comunicações e segurança informática?				
	1.1.6. Ao nível da infra-estrutura física e lógica, contempla o desenvolvimento da arquitectura de sistema e aplicacional?				
	1.1.7. Existe planeamento anual?				Pedir plano anual.
	1.1.8. Quem define prioridades e objectivos é o responsável máximo do Dep. Informática em conjunto com a gestão de topo?				
	1.1.9. O plano anual é baseado no plano de negócios da organização, incluindo objectivos gerais, metas e estratégias.				
	1.1.10. O planeamento anual, cobre todo o funcionamento do departamento informático (desenvolvimento, exploração, gestão de bases de dados, infraestruturas físicas e de comunicações, etc)?				
	1.1.11. Os desvios ao plano são acompanhados periodicamente, utilizando como unidade de medida recurso/hora/dia?.				Pedir documentação de suporte
1.2. Políticas e Normas de Procedimentos	1.2.1. Existem normas e procedimentos para as actividades informáticas?				
	1.2.2. Normas e procedimentos a institucionalizar na gestão das estruturas dos dados.				Pedir as normas;
	1.2.3. Normas e procedimentos a institucionalizar no desenvolvimento e programação de sistemas.				Pedir as normas;
	1.2.4. Normas e procedimentos a institucionalizar na exploração.				Pedir as normas;
	1.2.5. Normas e procedimentos a institucionalizar ao nível da gestão de dados e segurança da informação.				
1.3. Separação das Funções	1.3.1. O departamento informático é independente de outros departamentos da organização?				Pedir o organigrama da organização
	1.3.2. Como se encontra estruturado o departamento informático, na teoria e na prática.				Pedir o organigrama
	1.3.3. Existe separação funcional entre a área de desenvolvimento, de administração de sistemas, de operação, de gestão de segurança e de gestão de bases de dados e dados?				
	1.3.4. Os meios orçamentais definidos para o departamento informático, são os necessários?				Pedir o orçamento para o DI
	1.3.5. Quais as áreas com maior peso no orçamento e justificação para tal.				Pedir a distribuição dos custos
	1.3.6. Quais as áreas cujo desempenho e desenvolvimento se encontram limitadas pelo orçamento do departamento informático, ou pela falta de recursos humanos.				

OBJECTIVO Nº 1 – ORGANIZAÇÃO E GESTÃO GERAIS					
Controlos	Procedimentos	Resultado			Observações/
		S	N	NA	Referências
1.4. Política de Pessoal	1.4.1. Para as áreas respeitantes ao controlo de acessos, aos dados e disponibilidade de informação				
	1.4.2. Para a administração de sistemas:				
	1.4.3. Para administração de Bases de Dados				
	1.4.4. Para cada área do desenvolvimento				
	1.4.5. Para a operação do sistema				
	1.4.6. Foi ministrada formação em segurança informática aos utilizadores?				
1.5. Auditoria Informática	1.5.1. A organização contempla no sector da auditoria interna, auditoria informática ou recorre a "peritos" externos?				Pedir comprovativos.
	1.5.2. Foram efectuadas auditorias ao departamento informático ou aos controlos informáticos?				Pedir lista dos trabalhos
	1.5.3. A formação e experiência dos auditores informáticos são adaptados à tecnologia utilizada?				

OBJECTIVO Nº 2 – SEGURANÇA FÍSICA Controlos					
Controlos	Procedimentos	Resultado			Observações/
		S	N	NA	Referências
2.1. Acesso físico	2.1.1. O acesso ao departamento informático é controlado?				Verificar
	2.1.2. O acesso á sala de operação é controlado? Como?				Verificar
	2.1.3. O acesso à sala das maquinas é controlado? Como?				Verificar
	2.1.4. O acesso à bandateca é controlado? Como?				Verificar
	2.1.5. Existe registo das entradas em qualquer da áreas referidas?				Pedir registos para um determinado período.
	2.1.6. O acesso à sala de operação, máquinas e bandateca, é concedido pelo responsável pela área?				Pedir lista de autorizações
2.2. Prevenção, detecção e protecção contra incêndios	2.2.1. O centro informático está afastado de zonas que contêm materiais combustíveis?				Verificar
	2.2.2. Todos os materiais combustíveis são armazenados fora da sala dos computadores?				Verificar
	2.2.3. Existem procedimentos de limpeza, por forma a minimizar a acumulação de papeis e de produtos inflamáveis no interior e na proximidade da sala dos computadores? *(v.g. acumulação de listagens)*				Verificar e pedir norma
	2.2.4. É proibido fumar, comer e beber na sala de computadores e de operações?				Verificar e pedir norma
	2.2.5. A sala de computadores centrais encontra-se devidamente isolada e protegida da sala de operações e das outras salas?				Verificar
	2.2.6. Existem no centro informático e bandateca detectores de incêndio, fumo ou calor?				Verificar
	2.2.7. Estão instalados sistemas de extinção de incêndio, manuais ou automáticos?				Verificar
	2.2.8. Os sistemas de extinção de incêndio utilizam água?				Verificar as especificações

OBJECTIVO Nº 2 – SEGURANÇA FÍSICA Controlos					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
	2.2.9. A manutenção dos sistemas de prevenção e extinção é assegurada com periodicidade?				Pedir resultado da última vistoria
	2.2.10. Os procedimentos em caso de incêndio ou de situação de emergência estão definidos e afixados no centro informático? 2.2.11. São efectuados periodicamente exercícios de combate a incêndios e de evacuação?				Verificar e pedir normas Pedir plano
	2.2.12. O número de saídas de emergência é suficiente?				
	2.2.13. As saídas de emergência estão claramente identificadas e desimpedidas?				Verificar
2.3. Prevenção, detecção e protecção contra inundações	2.3.1. O centro informático está afastado de zonas susceptíveis de serem inundadas?				Verificar
	2.3.2. Se existirem riscos de inundação, estão instalados na cavidade do soalho detectores de água e equipamento de bombagem para evacuar água?				Verificar
	2.3.3. A manutenção dos sistemas de detecção e evacuação é assegurada com periodicidade?				Pedir resultado da última vistoria
2.4. Protecção do abastecimento de energia	2.4.1. Todos os computadores centrais, são protegidos por UPS ou por geradores eléctricos auxiliares, de entrada em funcionamento imediato?				Verificar
	2.4.2. Os computadores pessoais e serviços de comunicações encontram-se protegidos por UPS e por geradores eléctricos auxiliares				Verificar
	2.4.3. A manutenção das UPS ou geradores auxiliares é assegurada com periodicidade?				Pedir resultado da última vistoria.
	2.4.4. O sistema de protecção do abastecimento de energia, é testado regularmente (1 vez por ano)?				Pedir documento comprovativo
2.5. Sistemas de protecção auxiliares	2.5.1. Estão instalados na sala de computadores e bandateca detectores de roedores?				Verificar
	2.5.2. Existem detectores de gases ou produtos químicos susceptíveis de danificarem os computadores centrais, bem como os suportes lógicos?				Verificar
	2.5.3. Está assegurada a manutenção periódica dos sistemas de protecção?				Pedir resultado da última verificação

OBJECTIVO Nº 3 – SEGURANÇA LÓGICA PARA OS DADOS OU SERVIDORES DE APLICAÇÕES					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
3.1. Segurança de acesso lógica	3.1.1. O responsável pela segurança não exerce funções incompatíveis?				
	3.1.2. A concessão dos acessos é sempre rubricada pelo responsável da área?				
	3.1.3. Os acessos lógicos estão estruturados em perfis?				Pedir lista de perfis acessos permitidos.

OBJECTIVO Nº 3 – SEGURANÇA LÓGICA PARA OS DADOS OU SERVIDORES DE APLICAÇÕES					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
	3.1.4. Os utilizadores estão registados em grupos que utilizam os perfis definidos?				Pedir grupos, perfis e lista de utilizadores
	3.1.5. Os acesso à área de produção é vedado aos técnicos do desenvolvimento? E quando têm acesso é provisório?				Verificar
	3.1.6. Não existem acessos à área de produção fora do controlo do responsável pela segurança, incluindo os administradores de sistema, de bases de dados e de exploração?				Pedir lista de todos os acessos, funda-mentalmente da adm de sistemas
	3.1.7. A auditoria interna ou outra entidade procede á validação da atribuição de acessos aos utilizadores e à definição de perfis conforme o autorizado pelo responsável?				Verificar
	3.1.8. Existem auditrails do sistema activos, para controlo dos acessos?				Pedir exemplo de auditrail recente
	3.1.9. Os auditrails referidos são revistos com regularidade?				Pedir comprovativo
3.2. Segurança lógica de programas	3.2.1. As bibliotecas de produção são mantidas em separado das bibliotecas de desenvolvimento e ensaio?				
	3.2.2. As diferentes versões dos programas fonte que entraram em produção estão devidamente identificadas e guardadas?				Pedir norma reguladora e testar para uma aplicação.
3.3. Segurança lógica pessoal	3.3.1. Existem regras que interditam a partilha de palavras passe?				Verificar e pedir norma
	3.3.2. As palavras passe são mantidas secretas pelo sistema?				Verificar
	3.3.3. Está implementada a alteração regular e periódica das palavras passe?				Pedir norma e verificar parâmetro de sistema
3.4. Segurança lógica – dados	3.4.1. Existem processos para que os utilizadores acedam directamente ao dados, sem ser pelos programas ligados à produção? Quais?				Pedir lista de quem pode aceder directamente aos dados
	3.4.2. Em caso afirmativo, estes acessos são controlados pelo responsável da segurança?				
	3.4.3. Em caso afirmativo, estes acessos apenas tem permissão para consultar?				
	3.4.4. Existem auditrails para registo destes acessos?				Pedir auditrail de um dia
	3.4.5. Os acessos para inserção, alteração e eliminação de dados críticos, através dos programas em produção ficam registados em *auditrails*?				Pedir lista das tabel.as de *auditrails* e sobre quais incidem.
	3.4.6. Em caso afirmativo a posição anterior e posterior é salvaguardada?				
3.5. Segurança lógica – suporte lógico de base	3.5.1. Existe certificação da instalação do sistema operativo, da rede, do suporte lógico de segurança e outros subsistemas?				Pedir certificação
	3.5.2. Encontram-se registadas todas as mudanças dos parâmetros do suporte lógico de base?				Efectuar teste

OBJECTIVO Nº 4 – DESENVOLVIMENTO, PROGRAMAÇÃO E MANUTENÇÃO DOS SISTEMAS					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
4.1. Gestão projectos	4.1.1. Todo o desenvolvimento e manutenção dos subsistemas aplicacionais, é controlado por projectos?				
	4.1.2. A definição dos projectos e prioridades é da competência dos órgãos superiores de gestão?				
	4.1.3. Existe um plano dos projectos a executar e a definição de prioridades?				
	4.1.4. Os projectos são geridos no âmbito de equipas de projecto?				
	4.1.5. O acompanhamento e revisão dos projectos é efectuado periodicamente, utilizando uma unidade de medida por recursos envolvido?				
4.2. Normas de desenvolvimento de sistemas	4.2.1. Normas e procedimentos a institucionalizar no desenvolvimento e programação de sistemas.				Pedir as normas
	4.2.2. Normas e procedimentos a institucionalizar na gestão das estruturas dos dados.				Pedir as normas
4.3. Procedimentos em estádios específicos dos projectos	4.3.1. Lançamento do Projecto				Pedir o caderno de encargos de três projectos e analisar
	4.3.2. Estudo de viabilidade				
	4.3.3. Análise e concepção				Pedir especificações
	4.3.4. Elaboração, ensaio e execução				
4.4. Gestão alterações	4.4.1. As respostas deverão ser retiradas do restante ponto 4, que trata das situações de concepção e alteração de forma global.				

OBJECTIVO Nº 5 – OPERAÇÕES DE ROTINA DA INSTALAÇÃO CENTRAL					
Controlo	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
5.1. Manutenção do equipamento	5.1.1. É efectuada manutenção periódica do equipamento central (computadores centrais)?				Pedir comprovativo das últimas revisões
	5.1.2. É efectuada manutenção periódica da rede e das infraestruturas de comunicações?				Pedir comprovativo das últimas revisões
	5.1.3. Todos os equipamentos nucleares para a operacionalidade da organização possuem contratos de manutenção?				Pedir comprovativos
5.2. Separação e rotação de tarefas	5.2.1. Existe rotação nas equipas de operadores?				Pedir escalas
	5.2.2. Esta garantida a duplicidade de recursos para as tarefas críticas da operação?				Verificar pontos críticos?

OBJECTIVO Nº 5 – OPERAÇÕES DE ROTINA DA INSTALAÇÃO CENTRAL					
Controlo	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
5.3. Acções dos operadores	5.3.1. Existe a obrigatoriedade de registar em diário de operação todos os procedimentos efectuados na operação, indicando data, hora, tarefa e operador que a realizou?				Pedir cópia de algumas páginas do diário de operação
	5.3.2. Existem manuais de operação?				
5.4. Execução e programação do trabalho	5.4.1. O acesso aos parâmetros de configuração do sistema, controlo de acessos e controlo do trabalho de produção encontram-se inacessíveis aos operadores?				Testar situação
	5.4.2. Em caso negativo, os acessos a estas áreas possuem *log* de controlo?				Pedir imagem do log de controlo
5.5. Controlo de actividades	5.5.1. Os processamentos a executar diariamente (batch ou não), encontram-se planeados numa folha de trabalhos?				Pedir 3 exemplos de folhas de trabalho
	5.5.2. A folha de trabalho diária é preenchida com que periodicidade?				
	5.5.3. Existe segregação de funções entre quem preenche as folhas de trabalho e quem as verifica?				Analisar a rubrica de verificação
	5.5.4. Todas as folhas de trabalho são verificadas pelo responsável de área?				
	5.5.5. Após a execução dos procedimentos, o realizado é confrontado com o planeado? Por quem?				Verificar
	5.5.6. Todas as folhas de trabalho e do realizado são devidamente guardadas?				Verificar
5.6. Pistas de auditoria das actividades	5.6.1. Todos os *logs* de controlo de processamento estão activos?				Pedir lista de logs activos
	5.6.2. São verificados com periodicidade? Qual? Por quem?				
	5.6.3. Os logs são eliminados? Com que periodicidade?				
5.7. Controlos das bibliotecas	5.7.1. Todos os backups ou "media off line" são armazenados numa biblioteca própria e de acesso restrito?				
	5.7.2. O plano de backups dos dados garante a integridade e capacidade de reposição da situação do dia anterior, dos mesmos em caso de corrupção ou desastre?				Pedir plano de backup,
5.8. Distribuição de saídas	5.8.1. A distribuição de saídas é controlada por uma entidade independente do sector operacional e dos utilizadores que autorizam a distribuição? Ou em alternativa, existe um registo e controlo de todas as saídas ocorridas?				
	5.8.2. Todos os documentos emitidos electronicamente ou em papel, apresentam numeração sequencial?				Verificar a situação de ordens de pagamento, fact
	5.8.3. São armazenadas cópias das ordens de pagamento efectuadas, sempre que tal envolva transmissão de informação?				Verificar

OBJECTIVO Nº 6 – TELECOMUNICAÇÕES					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
6.1. Segurança no acesso interno às redes	6.1.1. Os acessos são controlados e autorizados pelo responsável de segurança?				Pedir comprovativos
	6.1.2. Existem *logs* de controlo de acessos?				Pedir imagem do log de controlo
	6.1.3. É efectuada alguma análise desses *log´s*?				
6.2. Segurança no acesso externo às redes	6.2.1. Existem organismos externos à organização que acedem à rede da organização? Quais?				Pedir lista de organismos
	6.2.2. Os acessos concedidos são autorizados e atribuídos pelo responsável de segurança?				Pedir lista de acessos
	6.2.3. Existem *logs* dos acessos externos?				Pedir *log* comprovativo
	6.2.4. É efectuada uma análise periódica desses *logs*?				
	6.2.5. Além da verificação de login, existem mais tipos de verificações?				Ex.º: verificação de IP, linhas, etc.
	6.2.6. O serviço de Internet encontra-se devidamente protegido por suporte lógico, quando ao acessos do exterior?				Verificar a existência de *firewall*.
6.3. Segurança no envio de informação	6.3.1. A transferência de dados para fora da rede é efectuada por linhas dedicadas?				Pedir esquema
	6.3.2. O envio de informação para o exterior através da Internet é possível pelos utilizadores do organismo?				
	6.3.3. Existem procedimentos para a encriptação de dados confidenciais?				Verificar quais e pedir norma
	6.3.4. Existe algum procedimento de controlo da informação enviada para o exterior através da Internet? Qual?				
	6.3.5. O antivírus encontra-se instalado e activo em todos os computadores?				Verificar
	6.3.6. Existem procedimentos para proceder à sua atempada actualização? Quais?				Verificar

OBJECTIVO Nº 7 – MICROCOMPUTADORES					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
7.1. Normalização ao nível dos micro-computadores	7.1.1. O equipamento e suporte lógico dos micro-computadores é normalizado ao nível da empresa?				Verificar e pedir comprovativo
	7.1.2. Os utilizadores não podem instalar e utilizar suporte lógico sem autorização?				Verificar
	7.1.3. Existe um procedimento automático para efectuar seguranças automáticas dos computadores pessoais?				
	7.1.4. Os backups dos computadores pessoais, são regulados por normas de procedimentos gerais?				Pedir normas
	7.1.5. A existência de backups e o seu correcto armazenamento é verificado periodicamente.				Pedir comprovativo
	7.1.6. O acesso aos dados armazenados em PC é sempre controlado por password?				

OBJECTIVO Nº 7 – MICROCOMPUTADORES					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
	7.1.7. O acesso aos dados armazenados em computadores portáteis, computadores de bolso e material similar são controlados por password?				
	7.1.8. Está implementada a cifragem de documentos, principalmente nos conteúdos que saem da organização?				
7.2. Aplicações locais críticas	7.2.1. Existem aplicações financeiras e de controlo que escapem ao controlo da DI? Quais?				
	7.2.2. Em caso afirmativo, existem procedimentos para salvaguarda dos dados e seu armazenamento regular?				Pedir normas
	7.2.3. É assegurado o cumprimento destas normas, por um sector diferente de quem opera as aplicações?				Verificar e testar
	7.2.4. Os acessos a estas aplicações são controlados pelo responsável de segurança?				
	7.2.5. O acesso aos computadores destas aplicações locais críticas é controlado por *password*?				

OBJECTIVO Nº 8 – PLANO DE EMERGÊNCIA					
Controlos	Procedimentos	Resultado			Observações/ Referências
		S	N	NA	
8.1. Plano de emergência operacional	8.1.1. Existe um plano de recuperação de desastres?				Verificar e pedir plano
	8.1.2. O plano inclui o processamento das aplicações fundamentais (instalação central, servidor cliente e computadores pessoais) em caso de qualquer falha?				Verificar
	8.1.3. O plano baseia-se numa avaliação do risco				
	8.1.4. O plano de recuperação de desastres foi aprovado pelas instâncias superiores de gestão?				
	8.1.5. Este plano é testado pelo menos uma vez por ano?				Pedir comprovativo
8.2. Plano de emergência lógico	8.2.1. As salvaguardas dos suportes lógicos de base e do suporte lógico da aplicação são efectuadas regularmente noutro local?				
	8.2.2. Está garantida a duplicidade das cópias de segurança dos ficheiros de dados, noutro local?				
	8.2.3. A cópia da documentação e das instruções de utilização dos sistemas, estão armazenadas em local diferente do da organização?				
	8.2.4. Os locais de armazenamento alternativo apresentam todas as condições de segurança mínimas, exigidas na gestão informática?				
	8.2.5. O transporte para o local de armazenamento alternativo processa-se em segurança?				

ANEXO 6: - Entidades Inquiridas

A. Responderam os Questionários

1. Aeroportos de Moçambique
2. Caminhos de Ferro de Moçambique
3. Comissão para Politica de Informática
4. Direcção Geral das Alfandegas
5. Direcção Geral dos Impostos
6. Direcção Nacional de Contabilidade Pública
7. Direcção Nacional de Imigração
8. Direcção Nacional do Orçamento
9. Direcção Nacional do Património do Estado
10. Electricidade de Moçambique
11. Empresa Moçambicana de Seguros
12. Instituto Nacional de Aviação
13. Instituto Nacional de Estatística
14. Instituto Nacional de Meteorologia
15. Ministério da Agricultura
16. Ministério da Educação e Cultura
17. Ministério da Energia
18. Ministério da Juventude e Desportos
19. Ministério da Planificação e Desenvolvimento
20. Ministério da Saúde
21. Ministério das Finanças
22. Ministério das Obras Publicas
23. Ministério das Pescas
24. Ministério de Administração Estatal
25. Ministério do Ambiente
26. Ministério dos Negócios Estrangeiro
27. Ministério dos Recursos Minerais
28. Ministério dos Transportes e Comunicação
29. Petróleos de Moçambique

30. Radio Moçambique
31. Telecomunicações de Moçambique
32. Televisão de Moçambique
33. Tribunal Administrativo
34. Unidade Técnica da Reforma de Administração Financeira do Estado

B. Não Responderam os Questionários

1. Administração Nacional de Estradas e Pontes
2. Autoridade Tributária de Moçambique
3. Centro de Processamento de Dados
4. Empresa Moçambicana de Medicamentos
5. Fundo de Estradas
6. Impressa Nacional
7. Instituto Nacional da Acção Social
8. Instituto Nacional de Segurança Social
9. Ministério da Mulher e Acção Social
10. Ministério do Interior
11. Ministério do Trabalho
12. Ministério do Turismo
13. Ministério dos Assuntos dos Antigos Combatentes