

# **AUDITORIA**

**Licenciaturas do ISEG**

**Ano Letivo de 2019/2020**

## **4. Controlo interno**

### **4.1. Princípios gerais de controlo interno (CI): orientações do COSO**

- 4.1.1. O COSO e o seu papel na melhoria do CI das organizações
- 4.1.2. Conceito de CI
- 4.1.3. Relevância do SCI (SCI) para a auditoria
- 4.1.4. Finalidades do CI
- 4.1.5. Componentes do SCI
- 4.1.6. O SCI e dimensão das empresas
- 4.1.7. Limitações dos SCI
- 4.1.8. O crescente reconhecimento da importância do controlo interno

### **4.2. Avaliação do risco e resposta ao risco avaliado**

- 4.2.1. Obtenção de conhecimento sobre o cliente
- 4.2.2. Obtenção de conhecimento sobre o sistema de controlo interno do cliente
- 4.2.3. Identificação dos riscos de distorção material (riscos inerente e de controlo)
- 4.2.4. Obtenção de prova sobre a qualidade do sistema de controlo interno – testes aos controlos
- 4.2.5. Avaliação dos riscos de distorção material
- 4.2.6. Recomendações do auditor sobre o controlo interno

### **4.3. CI em ambientes informatizados**

- 4.3.1. A evolução tecnológica e o seu impacto no controlo das organizações
- 4.3.2. Procedimentos de controlo em ambiente informatizado
- 4.3.3. Identificação dos riscos de distorção material, obtenção de prova e avaliação do SCI em ambiente informatizado

### **4.4. Fraudes e erros**

- 4.4.1. Fraude: conceito jurídico vs. conceito de auditoria
- 4.4.2. Tipos de fraude mais comuns
- 4.4.3. Responsabilidade pela deteção e prevenção de fraudes
- 4.4.4. A identificação e avaliação do risco de fraude pelo auditor
- 4.4.5. Probabilidade de ocorrência de fraudes e erros
- 4.4.6. Dificuldade em detetar fraudes e redução do risco de ocorrência de fraudes
- 4.4.7. Deveres do ROC no caso de detetar uma fraude

[jlacunha@iseg.ulisboa.pt](mailto:jlacunha@iseg.ulisboa.pt)

## 4. Controlo interno (CI)

### 4.1. Princípios Gerais de CI: as orientações do COSO

#### 4.1.1. O COSO e o seu papel na melhoria do CI das organizações



O COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) é uma iniciativa privada<sup>1</sup> de 5 das maiores associações profissionais dos E.U.A., totalmente independente destas e em que participam empresas do sector produtivo e financeiro, auditores e a New York Stock Exchange. Os objetivos do COSO são os de divulgar conhecimento ao mais alto nível sobre gestão do risco, controlo interno e dissuasão da fraude.

No que respeita ao **controlo interno**, o COSO publicou em 1992 o documento *Internal Control – Integrated Framework*, que continha um conjunto de orientações que, desde então, passaram a constituir um **referencial geralmente aceite como recolhendo as melhores práticas** na matéria. Em 2013 este documento foi revisto e aperfeiçoado, tendo originado o **2013 *Internal Control–Integrated Framework*** que é atualmente observado.

---

<sup>1</sup> the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the Institute of Management Accountants (IMA).

#### 4.1.2. Conceito de controlo interno

Existem muitas definições de controlo interno e diferentes entendimentos sobre este conceito, quer no meio empresarial, quer entre os profissionais da contabilidade e auditoria, quer até nas entidades de supervisão e regulação.

Segundo o COSO que, como já dissemos, constitui atualmente o referencial mais respeitado e adotado nesta matéria:

Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

A definição de CI constante na Norma Internacional de Auditoria 315 do IAASB acompanha de perto o conceito acima apresentado, como se pode observar em seguida:

“**Controlo interno** - Processo concebido, implementado e mantido pelos encarregados da governação, gerência e outro pessoal para proporcionar segurança razoável acerca da consecução dos objetivos de uma entidade com respeito à fiabilidade do relato financeiro, eficácia e eficiência das operações e cumprimento das leis e regulamentos aplicáveis. O termo "controles" refere-se a qualquer aspecto de um ou mais dos componentes do controlo interno.”  
(ISA 315 - Identificar e Avaliar os Riscos de Distorção Material Através do Conhecimento da Entidade e do Seu Ambiente)

#### 4.1.3. Relevância do sistema de controlo interno para a auditoria

A obtenção de conhecimento sobre o CI da entidade auditada é essencial para a realização de uma auditoria, constituindo

mesmo um dever profissional consagrado em várias ISA, designadamente na *ISA 200 - Objectivos Gerais do Auditor Independente e Condução de uma Auditoria de Acordo com as Normas Internacionais de Auditoria*:

“(...) 7. (...) As ISA exigem que o auditor exerça julgamento profissional e mantenha ceticismo profissional durante o planeamento e a execução da auditoria e, entre outras coisas:

- Identifique e avalie os riscos de distorção material, quer devido a fraude quer a erro, com base no conhecimento da entidade e do seu ambiente, incluindo o **seu controlo interno**. (...)”

Este dever profissional fundamenta-se no facto de ser essencial para o auditor, quando planeia uma auditoria, conhecer o CI da empresa, saber se é ou não eficaz, dado que, conforme já foi referido no capítulo anterior

- **Se CI for satisfatório**

⇒ risco de controlo baixo ⇒ menor probabilidade de existirem distorções materiais nas DF ⇒ o trabalho do auditor não carece de ser tão extenso e aprofundado

- **Se CI não for satisfatório**

⇒ risco de controlo alto ⇒ maior probabilidade de existirem distorções materiais nas DF ⇒ o trabalho do auditor pode exigir máxima extensão e profundidade

#### 4.1.4. Finalidades do controlo interno

De acordo com o COSO os objetivos do CI são contribuir para que sejam atingidos com razoável grau de segurança:

- a eficácia e eficiência das operações (*effectiveness and efficiency of operations*);
- a confiança na informação financeira divulgada publicamente (*reliability of financial reporting*);
- o cumprimento das leis e regulamentos aplicáveis (*compliance with applicable laws and regulations*).



Fonte: COSO

Neste contexto, cabem no conceito de CI atividades tão díspares e de complexidade tão diferenciada como, por exemplo,

- tomar medidas para assegurar a aderência às políticas da gestão cimeira
- implementar procedimentos para proteção dos ativos
- instalar software e/ou dispositivos destinados a dissuadir ou detetar a prática de fraudes e erros
- por em vigor regras que assegurem o rigor e a plenitude dos registos contabilísticos
- estabelecer calendários de entrega centralizada da informação financeira deslocalizada tendo em vista a sua preparação tempestiva e competente divulgação pública
- acompanhar a produção legislativa e regulamentar por forma a assegurar o respetivo cumprimento.

Em consequência do exposto tem de concluir-se que a responsabilidade pela implantação e funcionamento do sistema de controlo interno (SCI) em qualquer organização é da competência da respetiva administração/gerência.

#### 4.1.5. Componentes do sistema de controlo interno

De acordo com o COSO, um SCI deve ser constituído por 5 componentes:

- Ambiente de controlo (*Control Environment*)
- Avaliação do risco (*Risk Assessment*)
- Atividades de controlo (*Control Activities*)
- Informação e comunicação (*Information and Communication*)
- Acompanhamento / Monitorização (*Monitoring*)



Fonte: COSO

##### a) Ambiente de controlo

O ambiente de controlo existente numa organização representa o contexto em que se exerce o processo de controlo

interno e constitui um componente básico para garantir a sua eficiência e eficácia. É habitual reconhecer na caracterização do ambiente de controlo tópicos tão diferenciados como:

- Filosofia e estilo de gestão: compromisso com o controlo
- Integridade e valores éticos da Gestão cimeira
- Competência e eficiência da Gestão cimeira: implantação de métodos modernos de gestão com mecanismos de controlo adequados - gestão orçamental, auditoria interna
- Adequação da estrutura organizativa às atividades desenvolvidas, com definição clara da autoridade delegada, das responsabilidades de cada elemento e dos objetivos a atingir
- Intervenção ativa dos órgãos de fiscalização das entidades (Conselho Fiscal ou Comissão de Auditoria)
- Política de recursos humanos com impacto no controlo: qualificação e remuneração

Sem um ambiente de controlo apropriado, o sistema de controlo interno não tem condições para se desenvolver e funcionar adequadamente

## b) Avaliação do risco

As organizações enfrentam múltiplos riscos que afetam ou podem vir a influenciar os objetivos a atingir aos diferentes níveis. É essencial, por isso, que tendo em conta o ambiente

externo, os riscos associados ao alcance dos objetivos fixados sejam identificados e quantificado o seu impacto.

Conhecidos os riscos a enfrentar poderão ser concebidos os mecanismos de controlo destinados a evitá-los ou a minorar a sua ocorrência.

**Exemplos de riscos** (que podem ser ou não relevantes numa dada empresa):

- o risco na estimativa do justo valor de ativos,
- o risco de omissão de passivos,
- o risco de duplicação de pagamentos a fornecedores,
- o risco de realização de pagamentos de aquisições que não satisfizeram os requisitos internamente fixados, etc.

Compete, em primeiro lugar, à administração de cada empresa identificar os riscos relevantes a fim de estabelecer os controlos que os evitem.

### c) Atividades de controlo

Entende-se por atividades de controlo o conjunto de medidas e procedimentos implantados numa organização com o objetivo de assegurar que as orientações da gestão são executadas. São exemplos de atividades de controlo:

- Segregação de funções

Num mesmo circuito funcional (por exemplo, compras e pagamentos, vendas e recebimentos, etc.) **não devem ser concentradas numa só pessoa** as seguintes funções:

- Autorização das operações
- Registo das operações
- Custódia/guarda dos ativos



Deste modo, os diferentes intervenientes num dado circuito funcional verificam de forma independente o cumprimento dos requisitos internos, garantindo a respetiva regularidade.

No circuito de compras:

Quem **autoriza** uma compra não deve ter **acesso ao armazém**, nem deve dar **ordem de pagamento** à fatura do fornecedor ou pagá-la. A **contabilização** da operação deve caber também a outra pessoa. Os intervenientes nestas tarefas devem ser todos **diferentes**.

- Segurança na autorização das operações

O desenvolvimento de uma operação carece da autorização de um empregado com capacidade para o efeito

Numa empresa as compras só se realizam depois de autorizadas por quem tiver autoridade para o efeito. Assim, pode estar definido que o Diretor de compras tem competência para autorizar compras até 50.000 euros, mas sempre que a aquisição ultrapassar esta importância, cabe ao Conselho de Administração a respetiva autorização.

- Segurança no registo das operações

De entre os procedimentos que devem ser observados no processo de registo das operações tendo em vista a eficácia e a eficiência do SCI, indicam-se os seguintes, a título exemplificativo:

- os documentos vindos do exterior devem ser numerados e registados logo que deem entrada

- os registos contabilísticos devem ser claros, oportunos e apoiados em documentação válida
- a documentação, quer interna, quer proveniente do exterior, deve permitir evidenciar os sectores da empresa por onde circulou, bem como as indispensáveis conferências, autorizações e respetivas datas
- as alterações a registos anteriormente realizados carecem de autorização de empregado com capacidade para o efeito

Aquando da autorização para pagamento de uma compra ou da assinatura do correspondente cheque, deve proceder-se ao “cancelamento” dos respetivos documentos justificativos, através, por exemplo, da aposição imediata de um carimbo de “PAGO” nas faturas, o que evita a reutilização indevida da documentação suporte de uma aquisição, ou seja, a duplicação de pagamentos a fornecedores.

- Proteção dos ativos

Nesta área, alguns dos procedimentos a observar podem ser os seguintes:

- os valores em dinheiro devem ser restringidos ao mínimo possível e conservados em local apropriado
- os bens para venda devem ser conservados em instalações apropriadas: armazéns resguardados
- a transferência interna de ativos deve competir apenas a empregados autorizados
- a circulação de empregados não autorizados deve ser vedada em certos locais sensíveis

O método mais seguro para proteger o numerário consiste em depositar diariamente no banco todos os valores recebidos e simultaneamente realizar todos os pagamentos por cheque ou transferência bancária.

- Verificações periódicas

Para além dos procedimentos anteriormente referidos, importa realizar periodicamente verificações periódicas como as que se indicam em seguida:

- Realização de conferências periódicas de certas categorias de ativos (inventários, ativos fixos tangíveis)
- conferências periódicas de saldos de bancos e de terceiros (clientes, fornecedores) - reconciliações

A efetiva supervisão dos colaboradores pelos responsáveis das operações aos diferentes níveis – atividade muitas vezes descuidada por estes últimos – também constitui uma forma de verificar (acompanhar) o trabalho que vai sendo desenvolvido na empresa.

- Medidas de gestão do pessoal

De entre as atividades de controlo a implementar, algumas deverão ser introduzidas na área dos recursos humanos:

- seleção de pessoal que, para além de competente, disponha de integridade moral
- atribuição de remunerações adequadas ao nível de responsabilidade
- promoção, sempre que possível, de rotação de pessoal pelos vários serviços

- obrigatoriedade de todos os empregados em gozar as férias anuais
- não autorização, salvo em circunstâncias excepcionais, de acesso dos empregados às instalações em dias e horas de encerramento

As medidas acima indicadas – o gozo de férias anuais, por exemplo – estão fundamentadas numa perspectiva de controlo interno, embora a Direção de Recursos Humanos da empresa, que deve velar pelo bem-estar do pessoal, também advogue certamente a adoção desta medida.

#### d) Informação e comunicação

Outro dos componentes essenciais do SCI é a produção de informação fidedigna para a gestão (e utilizadores externos), bem como a sua divulgação oportuna aos responsáveis pela tomada de medidas destinadas a assegurar que os objetivos fixados sejam alcançados.

Essencial neste domínio é a qualidade do sistema contabilístico, o qual assegura o processamento contabilístico das operações.

- O Sistema contabilístico

Conjunto de métodos e processos de recolha, reconhecimento, mensuração, compilação e relato das transações com impacto financeiro realizadas por uma empresa. Na atualidade tudo se desenvolve em ambiente informático, o que implica dispor de software e hardware apropriado (*vide* esquema da página seguinte)

## A contabilidade como sistema de informação das organizações

### AMBIENTE

**comunidade**  
**gestores**  
**empregados/sindicatos**  
**bancos**  
**administração fiscal**  
**clientes**  
**acionistas**  
**fornecedores**  
**autoridade supervisão**  
**diversos**

Input	Processamento	Output
(transações) • Atividade operacional • Atividade de Financiamento • Atividade de Investimento	(de acordo com o referencial contabilístico aplicável *) • Reconhecimento • mensuração • classificação • registo • compilação	(Informação financeira) • Interna: controlo orçamental e de gestão • Externa: demonstrações financeiras

**comunidade**  
**gestores**  
**bancos**  
**administração fiscal**  
**clientes**  
**acionistas**  
**fornecedores**  
**sindicatos/empregados**  
**autoridade supervisão**  
**diversos**

\*referenciais contabilísticos aplicáveis em Portugal - SNC ou NIC

O sistema contabilístico gera

- ⇒ demonstrações financeiras destinadas ao exterior (investidores e outros interessados)
- ⇒ informação de gestão destinada aos responsáveis aos diferentes níveis da estrutura organizativa

O sistema contabilístico é um componente do sistema de informação de gestão de uma empresa (SIG), o qual recolhe e trata informação igualmente relevante para a gestão proveniente de outros subsistemas: comercial, logístico, operacional, de recursos humanos, patrimonial, de gestão financeira, etc.

#### e) Acompanhamento / Monitorização

Para garantir a qualidade do SCI é necessário que a organização também se preocupe em monitorizar o grau de execução do dispositivo de controlo. Não basta criar regras e procedimentos e ficar à espera que tudo funcione como previsto. É necessário, que cada empresa,

- documente os procedimentos de controlo interno em vigor (manual de procedimentos)
- realize, ela própria, testes periódicos ao cumprimento dos procedimentos de controlo instituídos, a efetuar pela Auditoria interna ou por empregados independentes, devendo os respetivos resultados ser arquivados para comprovação ulterior.

#### 4.1.6. O sistema de controlo interno e a dimensão das empresas

Tendo em conta os requisitos a satisfazer com vista à instituição de um SCI eficiente e eficaz, naturalmente que em muitas organizações não existirão os recursos e meios financeiros necessários a tal fim. De facto, a qualidade dos SCI está muito relacionada com a dimensão das organizações, já que, por exemplo, uma pequena empresa, pela sua própria natureza, não dispõe dos meios humanos, nem pode afetar ao CI meios financeiros que ponham em causa a sua continuidade – o seu controlo interno terá de ser frágil. Inversamente, um grupo empresarial de grande dimensão tem todas as condições – desde logo humanas e financeiras – para implantar um SCI de qualidade, pelo que, quando tal não sucede, a administração deve ser responsabilizada por esta fragilidade que pode ter graves repercussões na continuidade da organização.

- Empresas de pequena dimensão
  - ⇒ constrangimento na segregação de funções
  - ⇒ falta de formalização do SCI (não existe manual de procedimentos nem normas internas ou estas são muito limitadas)
  - ⇒ **fragilidade do controlo interno**
  
- Empresas de grande dimensão
  - ⇒ é essencial dispor de um SCI eficaz, com segregação de funções, dado o volume de informação processada

- ⇒ SCI deve estar formalizado através de manual de procedimentos
- ⇒ **sem controlo interno eficiente e eficaz é pouco provável que a informação financeira produzida pela grande empresa esteja isenta de deficiências**

Se a empresa de grande dimensão não estiver dotada de um sistema de controlo interno eficiente e eficaz, muito dificilmente o auditor estará em condições de emitir uma opinião sem reservas sobre as respetivas demonstrações financeiras.

#### 4.1.7. As limitações dos sistemas de controlo interno

Não obstante a constante procura por um SCI à prova de fraudes, por exemplo, também é incessante a busca de fragilidades nos sistemas implantados por parte dos que pretendem apropriar-se indevidamente do que não lhes pertence. **Não há, de facto, um SCI absolutamente seguro.** Para tal conclusão concorrem as seguintes razões principais:

- o incumprimento pela própria gestão cimeira dos procedimentos de controlo que instituiu
- o conluio entre empregados
- o custo incomportável de implantação e funcionamento de um sistema de controlo interno “totalmente” seguro face aos benefícios esperados



#### 4.1.8. O crescente reconhecimento da importância do CI

Embora sem ser admitido, durante muitos anos, as matérias relacionadas com o CI foram sempre secundarizadas pela gestão cimeira, que preferia dedicar a sua atenção a outros temas operacionais, comerciais e financeiros.

O impacto altamente negativo sobre os mercados de capitais - designadamente no tocante à falta de credibilidade da informação financeira divulgada – gerado pelas grandes falências ocorridas durante a 1ª década do século (ENRON, Parmalat, Lehman Brothers, etc.), foi o causador do atual reconhecimento da importância dos sistemas de controlo interno, quer por parte das próprias empresas, quer por parte dos legisladores e reguladores.

Em consequência, em 2002, o Congresso dos E.U.A. aprovou o *Sarbanes-Oxley Act*, que veio alterar substancialmente o quadro legal vigente em matéria de auditoria e informação financeira das *public companies* (sociedades com títulos transacionados em bolsa), tendo também produzido grande impacto em matéria de CI.

Assim, naquele país, as sociedades cotadas passaram a ser obrigadas a elaborar todos os anos e a juntar às demonstrações financeiras um “**Relatório da Administração sobre o controlo interno relativo à informação financeira** (Section 404)”

- Descrevendo a estrutura e os procedimentos de controlo interno relativos à informação financeira

- reconhecendo que é da sua responsabilidade a implementação e funcionamento de um sistema de controlo interno eficaz
- identificando os pontos fracos do sistema e as medidas a tomar para os eliminar.

De referir que, tal como dispõe o *Sarbanes-Oxley Act*, o sistema de controlo interno das *public companies*, para além de ser objeto do relatório da Administração acima identificado, passou a ser, **também, especificamente sujeito a exame pelo Auditor**, tendo em vista permitir-lhe atestar a qualidade do controlo interno relativo à informação financeira dessas sociedades.

A União Europeia e Portugal também tomaram medidas nesta matéria, sendo atualmente exigíveis, em algumas situações – instituições financeiras, fundos de investimento, etc. – a elaboração de relatórios sobre o controlo interno por parte das Administrações e a emissão de pareceres sobre os mesmos por parte dos Auditores.

## Aplicação Prática

A) Na empresa Beta estão em vigor os procedimentos de controlo que, em síntese, se descrevem seguidamente:

- 1) os cheques para pagamento a fornecedores só são emitidos depois de as faturas a que respeitam terem sido conferidas pelo Departamento de Contabilidade com base nas notas de encomenda que estiveram na sua origem;
- 2) os cheques têm de ser assinados por 2 administradores, o que implica que, no período de férias dos mesmos, ou um ou ambos têm de deixar alguns cheques assinados em branco a fim de a empresa poder fazer face a pagamentos inadiáveis;
- 3) para imprimir maior dinamismo à área comercial, as futuras vendas a crédito a clientes já existentes deixam de precisar de autorização superior, podendo ser concretizadas pelos vendedores de imediato; apenas no caso das vendas a novos clientes, o Departamento Financeiro terá de dar a sua aprovação prévia.

Pretende-se que: comente os procedimentos instituídos e, se assim o entender, sugira as alterações a introduzir.

B) A administração de uma empresa, através de carta anónima, tomou conhecimento de que o Diretor de Compras obteria secretamente comissões para seu benefício pessoal relativamente a todas as aquisições de materiais para escritório feitas a um certo fornecedor. O Diretor em causa é o único responsável pelas compras realizadas pela empresa, tendo-se verificado que todas as aquisições de materiais para escritório realizadas nos últimos 2 anos foram colocadas no fornecedor atrás referido.

Pretende-se que: indique um conjunto de procedimentos de controlo interno que poderiam ser adotados pela empresa com o objetivo de evitar a ocorrência desta situação.

## 4.2. Avaliação do risco e resposta ao risco avaliado

Para avaliar o risco de distorção material (risco inerente e de controlo) da empresa a auditar, a fim de ser determinado o risco de deteção a correr pelo auditor, é necessário que este (i) **conheça a empresa**, isto é, a sua natureza, o negócio que desenvolve, o sector em que se insere e a sua estrutura organizativa e humana, bem como (ii) o funcionamento do **sistema de controlo interno** implantado. Isso mesmo já foi constatado no começo deste capítulo, quando foi reproduzido um excerto da *ISA 200*:

“(...) 7. (...) As ISA exigem que o auditor exerça julgamento profissional e mantenha cepticismo profissional durante o planeamento e a execução da auditoria e, entre outras coisas:

- Identifique e avalie os riscos de distorção material, quer devido a fraude quer a erro, com base no **conhecimento da entidade e do seu ambiente**, incluindo o **seu controlo interno**. (...)”

A *ISA 315 - Identificar e Avaliar os Riscos de Distorção Material Através do Conhecimento da Entidade e do Seu Ambiente* contém as orientações específicas a seguir pelos auditores nesta matéria.

### 4.2.1. Obtenção de conhecimento sobre o cliente

O conhecimento que o auditor deve obter sobre o seu cliente – a empresa a auditar – comporta as diversas vertentes essenciais para a caracterização deste, a saber:

- Conhecimento sobre o ambiente externo
  - Contexto económico nacional e internacional, geral e sectorial
  - Legislação específica do sector
  - Práticas contabilísticas e comerciais do sector
  - Informação sobre características dos fornecedores e clientes, etc.
  
- Conhecimento sobre o ambiente interno
  - Sede e instalações produtivas
  - Capacidade produtiva e sua utilização
  - Capacidade de gestão
  - Resultados obtidos no passado e perspectivas
  - Estrutura organizativa
  - Procedimentos internos
  - Sistemas de controlo das operações
  - Plano de contas
  - Restrições impostas por endividamento, etc.

A consulta a documentação facultada pelo cliente ou obtida junto de diversas fontes credíveis, cada vez mais facilitada através do recurso à internet, permite obter a informação necessária ao conhecimento do cliente. As principais fontes informativas costumam ser as seguintes:

- Estudos e estatísticas sobre a economia nacional e internacional
- Estudos e estatísticas sectoriais
- Bases de dados legais
- Relatórios de gestão e demonstrações financeiras dos últimos exercícios
- Planos de contas próprios
- Organograma

- Manual de procedimentos
- *Curricula* dos administradores e principais responsáveis

#### 4.2.2. Obtenção de conhecimento sobre o sistema de controlo interno do cliente

Para obter conhecimento sobre o SCI do cliente as principais fontes informativas internas são:

- Manual de procedimentos
- Ordens de serviço ou regras de funcionamento sobre certos processos internos (compras, vendas, etc.)
- Organograma, etc.

Para completar o seu conhecimento sobre o SCI o auditor recorrerá a diversos métodos, tais como:

##### a) Preenchimento de questionários padronizados (*check lists*)

São questionários **pré-preparados** pelos auditores por forma a orientar o trabalho de recolha de informações sobre o controlo interno, permitindo a cobertura dos aspetos essenciais. Geralmente, existe um questionário padronizado para cada fluxo de operações, ou seja: recebimentos, pagamentos, compras, processamentos ao pessoal, etc.

A utilização de *check-lists* pelo auditor apresentam vantagens e inconvenientes. De entre as primeiras salientam-se:

- dirigem o trabalho do auditor para aspetos considerados essenciais no controlo interno em qualquer empresa
- facilitam a revisão do trabalho de auditoria pelos responsáveis cimeiros

Os principais inconvenientes da utilização de *check-lists* são:

- não estão adequados à realidade de cada empresa
- não permitem concluir diretamente, isto é, sem análise pelo auditor, sobre se o controlo interno é forte ou fraco (embora o questionário possa ser concebido por forma a que as respostas “não” constituam “pontos fracos”)

As normas técnicas de auditoria não contêm um modelo de questionário de aplicação obrigatória, pelo que cada auditor utiliza o que se lhe afigura mais apropriado. Na página seguinte apresenta-se, a título ilustrativo, um *check-list* que pode ser usado por um auditor para fazer o levantamento dos procedimentos internos adotados nas operações de pagamentos por cheque. Sempre que mais do que uma pessoa participa num processo interno, o questionário pode ser aplicado a todos ou alguns dos respetivos intervenientes, o que possibilita, muitas vezes, a deteção de contradições entre as respostas obtidas.

#### b) Elaboração de memórias narrativas

São descrições escritas dos fluxos de informação, com a indicação dos departamentos e empregados que realizam as diferentes tarefas, dos documentos elaborados e do destino que lhes é dado, dos registos realizados, etc.

## Exemplo de Questionário padronizado (Check list) para a área de pagamentos por cheque

	SIM	NÃO	N/A	PONTO FRACOS		Observações
				Relevante	Não relevante	
<b>Pagamentos por cheque</b>						
1. Juntamente com cada cheque é apresentada a respetiva autorização de pagamento (AP) e a documentação de suporte?	✓					
2. Os cheques são emitidos por ordem sequencial?	✓					
3. Os cheques por emitir são guardados em local seguro?	✓					No cofre do Tesoureiro
4. Estão definidas as pessoas e os requisitos para assinatura de cheques?	✓					Ver Ordem de Serviço 8/14
5. Quem assina os cheques verifica se os mesmos estão de acordo com a AP e a documentação de suporte?	✓					
6. A AP e a documentação de suporte são “canceladas” depois da assinatura do cheque?	✓					É carimbado “PAGO” na AP e na documentação de suporte
7. Quem aprova os pagamentos e quem assina os cheques são pessoas diferentes?	✓					
8. Quem assina os cheques e quem os contabiliza são pessoas diferentes?	✓					
9. As contas bancárias são reconciliadas periodicamente por alguém independente?	✓					Mensalmente pela auditoria interna
10. É feita uma verificação diária independente entre o total dos cheques emitidos e o registo contabilístico dos pagamentos por cheque?		✓		✓		A verificação é feita pelo Tesouraria. Recomenda-se que seja feita pela auditoria interna



### **Exemplo de memória narrativa sobre o fluxo de Compras**

1. Quando o Armazém precisa de uma determinada mercadoria, prepara uma Requisição, com duas vias. Uma das vias é enviada para a Contabilidade (sector de contas a pagar) e a outra para o Departamento de compras.
2. Ao receber a requisição, o Departamento de Compras, procede a consultas junto de fornecedores, e decide junto de qual irá colocar a encomenda, para o que emite uma Ordem de Encomenda (OE) com 5 cópias.
3. Uma cópia da OE é remetida para o Armazém, a fim de serem verificadas as quantidades e descrições das mercadorias.
4. Duas das cópias da OE são enviadas para a Contabilidade (sector de contas a pagar) e para a Receção de Mercadorias tendo em vista notificá-los da realização da encomenda.
5. As restantes duas cópias são enviadas ao Fornecedor, o qual dá conhecimento da receção da encomenda devolvendo uma delas ao Departamento de Compras.
6. O Fornecedor expede a mercadoria, a qual é acolhida na Receção de Mercadorias, sector onde se procede à respetiva contagem e se elabora a Nota de Entrada em Armazém, com 3 cópias.
7. Depois de verificada e contada, a mercadoria dá entrada no Armazém, juntamente com 2 cópias da Nota de Entrada em Armazém. Aqui a mercadoria é comparada com o conteúdo da Nota de Entrada em Armazém, seguindo uma cópia deste documento para a Contabilidade (sector de contas a pagar).
8. A restante cópia da Nota de Entrada em Armazém é enviada pela Receção de Mercadorias para o Departamento de Compras como notificação do recebimento da mercadoria.
9. O Fornecedor envia a Fatura em duplicado para o Departamento de Compras, o qual retém a cópia e envia o original para a Contabilidade (sector de contas a pagar).
10. A contabilidade (sector de contas a pagar) compara a Requisição, a Nota de Encomenda, a Nota de Entrada em Armazém e a Fatura, e, depois de conferi-los, arquiva-os conjuntamente para documentar a compra.

### **c) Preparação de fluxogramas**

São descrições gráficas dos fluxos de informação e das operações e controlos implantados num sistema ou parte dele.

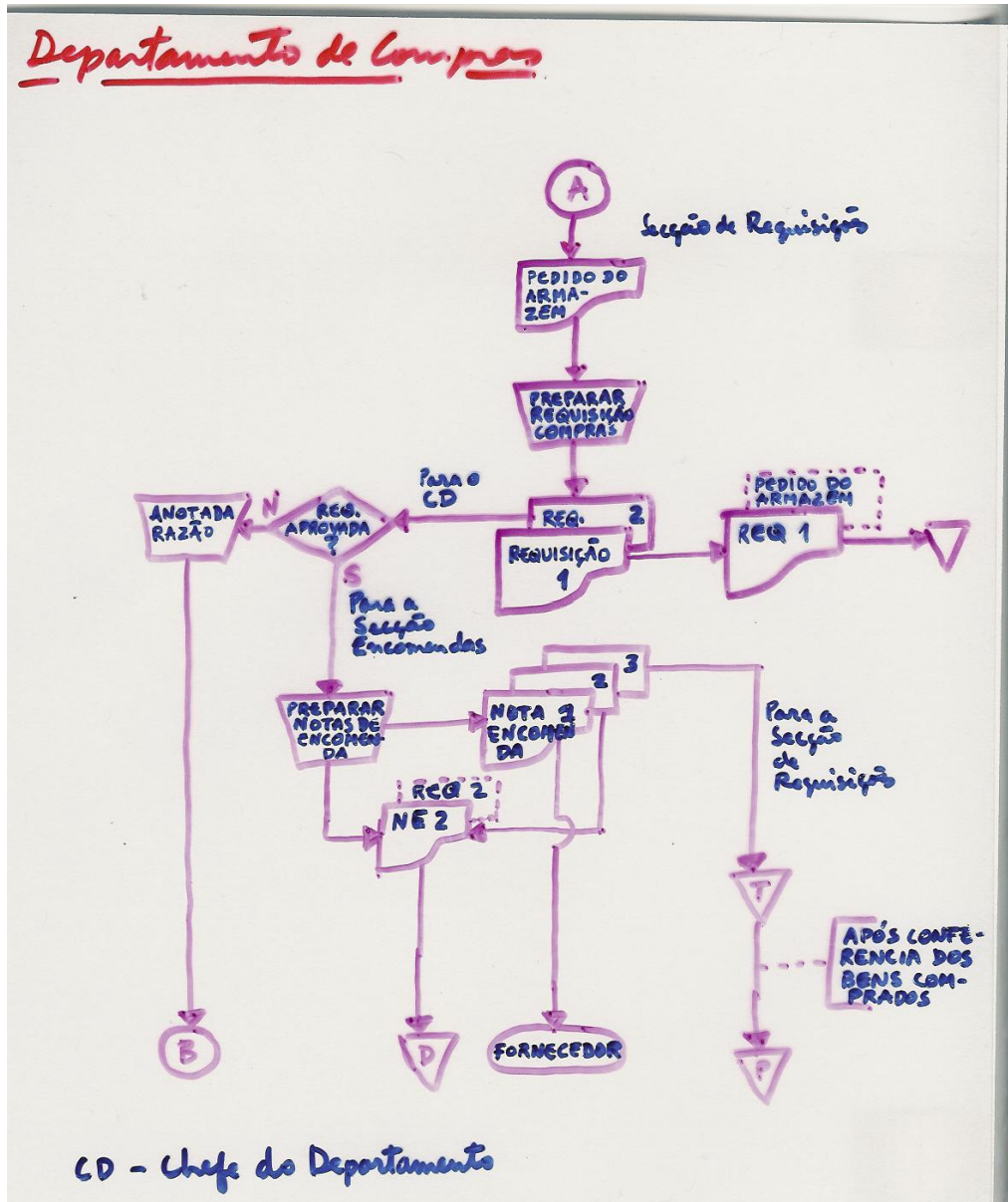
De entre as vantagens obtidas com a sua utilização salientam-se:

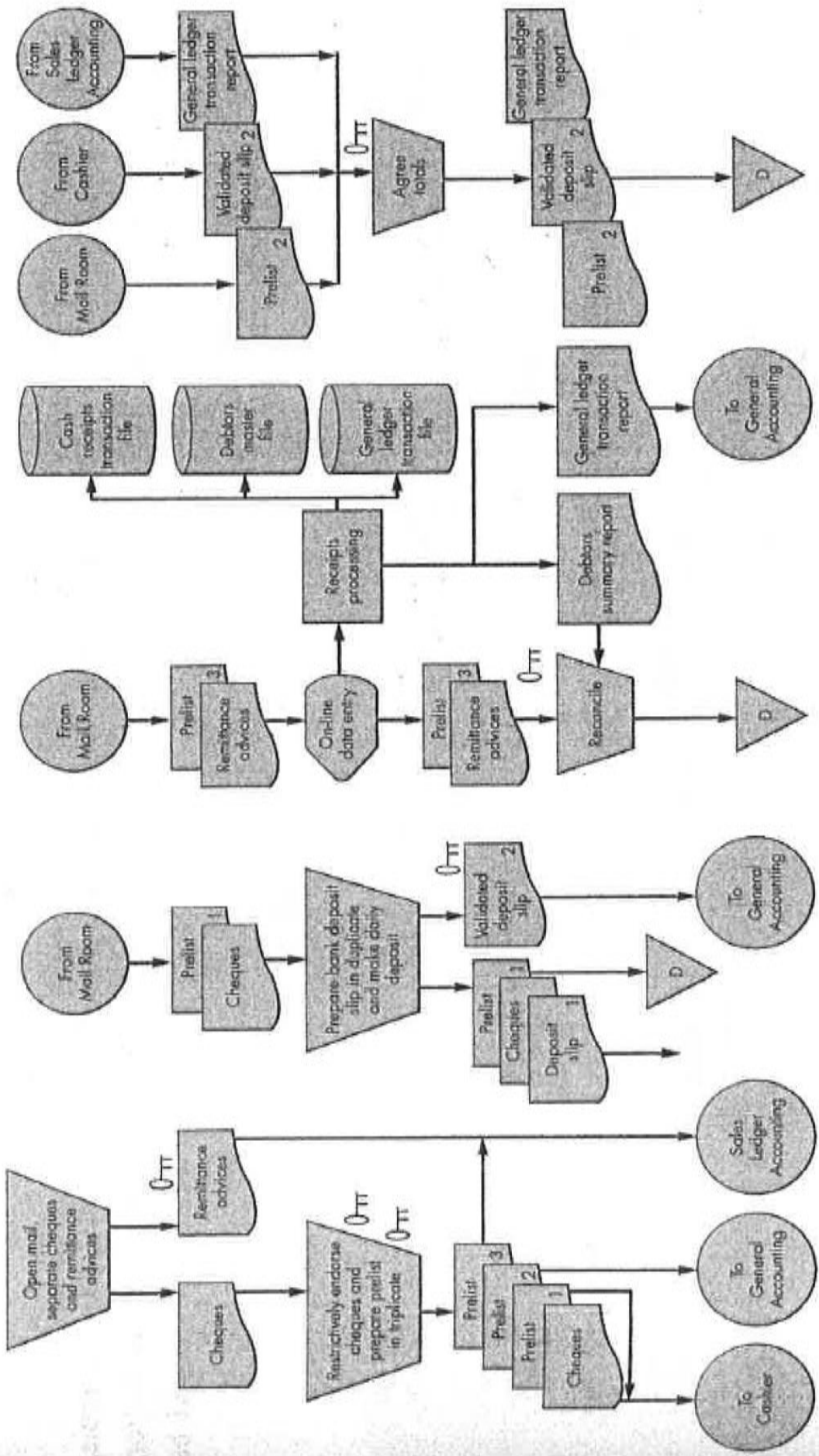
- permite visualizar os fluxos de informação e controlos
- facilita a revisão do trabalho de auditoria pelo responsável cimeiro

Como principal inconveniente é costume referir que a simples observação do fluxograma não conduz diretamente à conclusão sobre se o controlo interno é forte ou fraco.

Nas páginas seguintes apresentam-se exemplos de fluxogramas utilizados por auditores. O primeiro caso é a reprodução de um papel de trabalho preparado pelo próprio auditor para documentar o processo de compras de uma empresa, uma vez que esta não o tinha formalizado. O exemplo subsequente corresponde a um fluxograma preparado pela empresa auditada e que o auditor pode utilizar para testar o cumprimento dos procedimentos previstos na área de recebimentos de vendas. (Fonte: *Modern Auditing – Cosserat, Graham W.; Rodda, Neil*)

Exemplo de fluxograma preparado pelo próprio auditor





### 4.2.3. Identificação dos riscos de distorção material

Com base no conhecimento adquirido sobre a empresa a auditar e sobre o seu SCI, o auditor vai então procurar identificar os riscos inerentes e de controlo do cliente, também designados conjuntamente por **riscos de distorção material (RDM)**.

Estes RDM podem afetar as demonstrações financeiras como um todo ou apenas certas transações, saldos de algumas contas ou a apresentação das demonstrações financeiras.

#### a) Riscos de distorção material que afetam as DF como um todo

Estão relacionados normalmente com as características do negócio ou sector da empresa, a competência e integridade da sua administração ou a qualidade do sistema de controlo interno, não sendo diretamente identificáveis as operações em que podem ocorrer.

Como já vimos no capítulo 3, o risco inerente (um dos componentes do RDM) é elevado se o auditor considerar que a integridade, experiência e/ou competência dos administradores podem afetar a veracidade das DF como um todo; de igual modo, o risco de controlo é elevado se a inexistência de procedimentos básicos de controlo – por exemplo, falta de segregação de funções ou de controlo de acessos a terminais – põem em causa o SCI e as DF na sua globalidade.

b) Riscos de distorção material que afetam aspetos parcelares das DF

Os RDM na maior parte das vezes afetam diretamente certas transações, saldos de algumas contas ou a apresentação das demonstrações financeiras.

Por exemplo, nas vendas realizadas em lojas, muitas vezes, corre-se o risco de as mesmas poderem não ser todas registadas ou haver um erro na introdução do valor da transação (com a correspondente distorção do resultado líquido e do ativo); no cálculo das depreciações, se o programa informático que o realiza, não estiver bem concebido e testado, podem ser obtidos valores errados, o que distorce o valor do ativo fixo tangível, e do resultado líquido.

Neste contexto, o auditor depois de identificar os diferentes RDM potenciais na empresa que está a auditar, analisa e testa a eficiência dos controlos internos instituídos para os eliminar ou minimizar.

4.2.4. Obtenção de prova sobre a qualidade do SCI – testes aos controlos

Mesmo nas áreas em que o sistema de controlo interno parece ser satisfatório – pelo menos teoricamente, por exemplo, através da análise ao manual de procedimentos - o auditor tem de **obter prova** sobre a sua efetiva qualidade em termos de funcionamento. Com essa finalidade, deve realizar um conjunto de procedimentos nos diferentes fluxos operacionais, os quais são designados genericamente por “testes aos controlos”.

Os **testes aos controlos** são procedimentos de auditoria realizados pelo auditor com o objetivo de **apreciar a eficiência dos controlos** implantados pela empresa. Podem assumir diversas formas:

- Entrevistas aos empregados
- Verificação de documentos e relatórios
- Observação da aplicação dos controlos
- *Walkthrough* (*tracing* e *vouching*)
- Reprocessamento dos controlos, etc.

Os procedimentos genericamente designados pela expressão inglesa “*walkthrough*” consistem no rastreamento pelo auditor da aplicação efetiva dos procedimentos instituídos.

- O **tracing** envolve a seleção de documentos gerados por operações realizadas pela empresa – notas de encomenda, faturas de venda, etc. – e a comprovação da observância (ou não) das normas instituídas ao longo do processo seguido até serem registados contabilisticamente;
- O **vouching** segue o sentido contrário, isto é, a partir dos registos contabilísticos – amostras selecionadas pelo auditor de registos de recebimentos de clientes ou de pagamentos a fornecedores, por exemplo – vai procurar confirmar a regularidade do processo desde o seu início.

No manual de procedimentos consta que as compras acima de 50.000 euros carecem de autorização do Conselho de Administração, podendo as de valor inferior ser aprovadas pelo Diretor de Compras.

O auditor deve testar o cumprimento desta regra, através de apropriados testes aos controlos, tais como:



- questionários preenchidos com as respostas dadas pelos intervenientes no processo de compras, tendo em vista comprovar se os mesmos têm conhecimento desta norma e se a mesma é geralmente aplicada;
- análise às autorizações de compra relativas a uma amostra a seleccionar de registos contabilísticos de pagamentos a fornecedores superiores a €50.000.

#### 4.2.5. Avaliação dos riscos de distorção material

Como resultado dos testes aos controlos realizados, o auditor conclui a sua avaliação sobre o risco de distorção material do cliente, isto é, sobre o risco inerente e o risco de controlo que lhe estão associados. Em consequência, se concluir que o RDM é elevado terá de correr um risco de deteção baixo por forma a que o risco de auditoria seja aceitável. Conclusão inversa – pode correr um risco de deteção alto – será retirada quando o RDM for considerado baixo.

- risco de distorção material elevado (sistema de controlo interno insatisfatório e/ou risco inerente elevado) ⇒
  - ⇒ risco de deteção baixo ⇒
  - ⇒ Estender e aprofundar os procedimentos de auditoria a realizar
- risco de distorção material baixo (sistema de controlo interno satisfatório e/ou risco inerente baixo) ⇒
  - ⇒ risco de deteção alto ⇒
  - ⇒ Abrandar a extensão e profundidade dos procedimentos de auditoria a realizar



#### 4.2.6. Recomendações do auditor sobre o controlo interno

No decurso do seu trabalho de auditoria, o auditor procedeu não só à avaliação dos riscos, mas também ao levantamento e avaliação do SCI da empresa, podendo ter obtido prova sobre a existência de deficiências com impacto negativo na eficiência operacional e na qualidade das demonstrações financeiras.

Revestem-se, por isso, do maior interesse para as empresas os relatórios com **recomendações para o aperfeiçoamento do SCI** que os auditores, paralelamente aos relatórios de auditoria, entregam aos seus clientes no final do trabalho. No nosso País, para além da Certificação Legal das Contas - isto é, do relatório da auditoria imposto por lei, divulgado publicamente e que contém a opinião do ROC sobre as demonstrações financeiras - os Revisores Oficiais de Contas geralmente entregam às empresas auditadas outro relatório autónomo, destinado apenas a utilização interna e designado por **Relatório de Recomendações**, no qual, dão conta das deficiências de controlo interno detetadas e recomendam as práticas necessárias à sua eliminação.

#### **Normas profissionais sobre controlo interno**

- ISA 315 (Clarificada) - Identificar e Avaliar os Riscos de Distorção por Meio da Compreensão da Entidade e do Seu Ambiente

### 4.3. Controlo interno em ambientes informatizados

A utilização de meios informáticos pelas empresas tem vindo a vulgarizar-se de tal maneira que, hoje em dia, rara é a organização que não disponha de apoio informático nas áreas administrativas e financeiras, comerciais e produtivas.

#### 4.3.1. A evolução tecnológica e o seu impacto no controlo das organizações

A vulgarização da atividade informática em tempo real (*on line*) e a proliferação de terminais pelas organizações trouxe imensos benefícios em termos de atualização da informação e sua divulgação, mas está na origem de graves riscos de ocorrência de fraudes e erros.

No passado, o risco de desvio de dinheiro, por exemplo, envolvia a sua apropriação física; nos tempos atuais, em que o numerário está desmaterializado nas contas bancárias, esse risco diminuiu, mas o crime informático praticado por *hackers* pode tornar mais vulneráveis os acessos aos saldos de depósitos à ordem, exigindo o reforço e sofisticação da sua proteção.

#### 4.3.2. Procedimentos de controlo em ambiente informatizado

Em ambiente informatizado o SCI de uma organização deve estar dotada de dois tipos de procedimentos:

- Procedimentos de controlo gerais  
São procedimentos de âmbito geral que são essenciais para que as aplicações informáticas não sejam afetadas por ameaças exteriores ou internas
- Procedimentos de controlo das aplicações  
São os que visam proporcionar uma garantia razoável de que a introdução, processamento e distribuição dos resultados das aplicações informáticas decorreu de forma apropriada

a) Procedimentos de controlo gerais

De entre os procedimentos de controlo gerais mais relevantes salientam-se os seguintes

- **segregação de funções**

Tal como referido em 4.2., a segregação de funções é um princípio essencial de controlo que, também em ambiente informatizado, encontra o seu espaço de adoção. As funções de autorização, registo e guarda não devem competir a uma mesma pessoa, pelo que deve ser interdito ao pessoal informático o acesso a operações correntes, tais como, transferências bancárias, processamentos de vencimentos, ordens de expedição, etc.

O pessoal do departamento de informática **não deve ser autorizado a:**

- aprovar transações
- corrigir erros nas transações
- introduzir dados
- ter bens ou valores à sua guarda

na **organização interna do departamento de informática**, devem ser observadas as seguintes regras:

- o pessoal que concebe e escreve os programas não deve estar encarregado da operação do computador
- deve existir rotação entre os operadores informáticos
- o pessoal do departamento de informática deve gozar férias anualmente

- **Exigência de documentação das aplicações**

Quer sejam adquiridas ou desenvolvidas internamente, deve haver a preocupação de exigir documentação referente às aplicações, designadamente:

- fluxogramas
- descrições de ficheiros
- manual de operação
- listagens dos erros previstos, etc.

Sem esta preocupação, a manutenção das aplicações, sobretudo as desenvolvidas internamente, pode ser muito afetada devido ao desconhecimento da lógica que presidiu ao seu desenvolvimento.

- **Controlo da alteração das aplicações**

A área das alterações às aplicações está muito sujeita à prática de atos interditos, pelo que merecer especial atenção no que respeita ao SCI, designadamente exigindo o registo da finalidade de qualquer alteração e a identificação de quem a realizou.

- **Limitação de acessos**

A multiplicidade de acessos aos sistemas deve ser controlada por diversas formas:

- *password*: atribuída tendo em conta o perfil do utilizador e sujeita a alteração periódica
- listagens informáticas de tentativas de acesso falhadas, a fim de analisar os casos de tentativa múltipla

- **Segurança e fiabilidade na transmissão de dados**

Dada a importância que assume a transmissão de dados através de redes de telecomunicações, internet e redes internas, é necessário estabelecer controlos que impeçam o acesso indevido ou a deturpação de dados, tais como:

- encriptação de dados, isto é, o envio da informação codificada
- utilização de linhas privadas, o que assegura maior segurança e fiabilidade na transmissão

- *parity check*: introdução de parity bits redundantes para confirmar a receção da totalidade da mensagem
- **Segurança física de instalações, equipamentos e ficheiros**
  - Condicionamento de entradas no centro informático
  - Realização periódica de cópias de segurança dos ficheiros (backups)
  - cofres à prova de fogo
  - conservação de *backups* em local diferente do centro informático

#### b) Procedimentos de controlo das aplicações

Estes procedimentos, para serem eficazes, pressupõem a existência dos procedimentos de controlo gerais e visam proporcionar uma garantia razoável de que a introdução, processamento e distribuição dos resultados das aplicações informáticas decorreu de forma apropriada.

- **controlo da introdução de dados (input)**

O objetivo destes controlos é o de assegurar a integralidade, exatidão e validade dos dados introduzidos nas aplicações

- integralidade: foram introduzidos todos os documentos autorizados
- exatidão: todos os documentos autorizados foram introduzidos corretamente
- validade: nenhum documento não autorizado foi introduzido

Com esta finalidade podem ser adotados procedimentos como os seguintes:

- controlo da utilização por *password* e *log* da atividade realizada
- *check-digit* (número redundante de controlo)
- totais de controlo: usados nos processamentos por *batch*, de forma a controlar que o processamento englobou todos os dados
- teste de razoabilidade: controla os dados introduzidos durante o processamento com base em limites pré-definidos ou outros indicadores (IVA e vendas, Segurança Social e remunerações)
- testes de validação *on line*: o sistema não aceita dados incompletos (campos em branco) ou dados numéricos em campos alfabéticos, etc.

- **controlo do processamento de dados**

O objetivo destes controlos é assegurar a regularidade do processamento dos dados introduzidos nas aplicações. Se não foram realizados na fase do *input*, devem ser efetuados durante o processamento diversos procedimentos, tais como,

- testes de validação, tal como atrás referidos;
- testes de razoabilidade, *idem*

- teste de sequência: ou seja, controlar que os dados foram tratados pela ordem prevista
- etiquetagem dos suportes: discos, diskettes, DVD

- **controlo da distribuição dos resultados (*output*)**

O objetivo destes controlos é assegurar que os resultados das aplicações estão corretos e são distribuídos apenas pelas pessoas autorizadas

- controlo da utilização por *password* e *log* da atividade realizada
- revisão periódica das autorizações de acesso à informação
- reconciliação dos dados do input com os do *output*

#### 4.3.3. Identificação dos riscos de distorção material, obtenção de prova e avaliação do SCI em ambiente informatizado

Os princípios anteriormente apresentados (vide 4.2) sobre a identificação dos riscos de distorção material, a obtenção de prova e a avaliação pelo auditor da eficiência e eficácia do SCI, mantêm-se válidos, na sua essência, no contexto do ambiente informatizado.

Assim, deverá o auditor:



- Obter e documentar o conhecimento adquirido do sistema informático através de fluxogramas, memórias narrativas, etc.;
- Identificar os riscos significativos que possam afetar o seu funcionamento
- Realizar testes aos controlos destinados a comprovar o funcionamento do sistema, recorrendo a reprocessamentos, testes paralelos e outras técnicas específicas
- Avaliar o sistema e o correspondente risco de controlo em função dos resultados obtidos nos testes aos controlos

Nesta fase do trabalho de auditoria é usual recorrer a especialistas com **competência específica** em assuntos de natureza **informática** para que os resultados obtidos nesta área da auditoria possam ser aceites com confiança pelo auditor.

## **Normas de auditoria aplicáveis**

ISA 315 (Clarificada) - Identificar e Avaliar os Riscos de Distorção por Meio da Compreensão da Entidade e do Seu Ambiente

## 4.4. Fraudes e erros

### 4.4.1. Conceito jurídico de fraude vs. conceito de auditoria

O conceito de fraude em auditoria não coincide com a sua noção jurídica, a qual varia de país para país em função dos respetivos quadros legais.

Em Portugal se consultarmos a legislação vigente à procura das normas jurídicas tutelares do conceito de “fraude” depararemos com a seguinte situação:

- Código Penal português
  - ⇒ são vários os crimes que atentam direta ou indiretamente contra a propriedade e o património que estão previstos no Código Penal (*vide* Anexo), mas não está tipificado qualquer crime designado por “fraude”.
- Regime Geral das Infrações Tributárias
  - ⇒ Tipificados os crimes de “fraude”, “fraude qualificada” e de “fraude contra a segurança social”

### **Regime Geral das Infrações Tributárias**

*“art.º 103º  
FRAUDE*

*1 - Constituem fraude fiscal, punível com pena de prisão até três anos ou multa até 360 dias, as condutas ilegítimas tipificadas no presente artigo que visem a não liquidação, entrega ou pagamento*

*da prestação tributária ou a obtenção indevida de benefícios fiscais, reembolsos ou outras vantagens patrimoniais susceptíveis de causarem diminuição das receitas tributárias. A fraude fiscal pode ter lugar por:*

*a) Ocultação ou alteração de factos ou valores que devam constar dos livros de contabilidade ou escrituração, ou das declarações apresentadas ou prestadas a fim de que a administração fiscal especificamente fiscalize, determine, avalie ou controle a matéria colectável;*

*b) Ocultação de factos ou valores não declarados e que devam ser revelados à administração tributária;*

*c) Celebração de negócio simulado, quer quanto ao valor, quer quanto à natureza, quer por interposição, omissão ou substituição de pessoas.*

*2 - Os factos previstos nos números anteriores não são puníveis se a vantagem patrimonial ilegítima for inferior a 15.000 euros.*

*3 - Para efeitos do disposto nos números anteriores, os valores a considerar são os que, nos termos da legislação aplicável, devam constar de cada declaração a apresentar à administração tributária.”*

#### *“Artigo 104.º*

#### *FRAUDE QUALIFICADA*

*1 - Os factos previstos no artigo anterior são puníveis com prisão de um a cinco anos para as pessoas singulares e multa de 240 a 1200 dias para as pessoas colectivas quando se verificar a acumulação de mais de uma das seguintes circunstâncias:*

*a) O agente se tiver conluiado com terceiros que estejam sujeitos a obrigações acessórias para efeitos de fiscalização tributária;*

*b) O agente for funcionário público e tiver abusado gravemente das suas funções;*

*c) O agente se tiver socorrido do auxílio do funcionário público com grave abuso das suas funções;*

*d) O agente falsificar ou viciar, ocultar, destruir, inutilizar ou recusar entregar, exhibir ou apresentar livros, programas ou ficheiros*

*informáticos e quaisquer outros documentos ou elementos probatórios exigidos pela lei tributária;*

*e) O agente usar os livros ou quaisquer outros elementos referidos no número anterior sabendo-os falsificados ou viciados por terceiro;*

*f) Tiver sido utilizada a interposição de pessoas singulares ou colectivas residentes fora do território português e aí submetidas a um regime fiscal claramente mais favorável;*

*g) O agente se tiver conluiado com terceiros com os quais esteja em situação de relações especiais.*

*2 - A mesma pena é aplicável quando:*

*a) A fraude tiver lugar mediante a utilização de facturas ou documentos equivalentes por operações inexistentes ou por valores diferentes ou ainda com a intervenção de pessoas ou entidades diversas das da operação subjacente; ou*

*b) A vantagem patrimonial for de valor superior a € 50.000.*

*3 - Se a vantagem patrimonial for de valor superior a € 200.000, a pena é a de prisão de 2 a 8 anos para as pessoas singulares e a de multa de 480 a 1920 dias para as pessoas colectivas.*

*4 - Os factos previstos nas alíneas d) e e) do n.º 1 do presente preceito com o fim definido no n.º 1 do artigo 103.º não são puníveis autonomamente, salvo se pena mais grave lhes couber.”*

### *“Artigo 106.º*

#### *FRAUDE CONTRA A SEGURANÇA SOCIAL*

*1 - Constituem fraude contra a segurança social as condutas das entidades empregadoras, dos trabalhadores independentes e dos beneficiários que visem a não liquidação, entrega ou pagamento, total ou parcial, ou o recebimento indevido, total ou parcial, de prestações de segurança social com intenção de obter para si ou para outrem vantagem ilegítima de valor superior a € 7500.*

*2 - É aplicável à fraude contra a segurança social a pena prevista no n.º 1 do artigo 103.º e o disposto nas alíneas a) a c) do n.º 1 e no n.º 3 do mesmo artigo.*

3 - *É igualmente aplicável às condutas previstas no n.º 1 deste artigo o disposto no artigo 104.º*

4 - *Para efeito deste artigo também se consideram prestação da segurança social os benefícios previstos na legislação da segurança social.”*

- **Lei Geral Tributária**

⇒ Tipificado o crime de “fraude no transporte de mercadorias em regime suspensivo”

### ***Lei Geral Tributária***

*“Artigo 95.º*

*Fraude no transporte de mercadorias em regime*

*1 - Quem, por qualquer meio, no decurso do transporte de mercadorias em regime suspensivo:*

*a) Subtrair ou substituir mercadorias transportadas em tal regime;*

*b) Alterar ou tornar ineficazes os meios de selagem, de segurança ou de identificação aduaneira, com o fim de subtrair ou de substituir mercadorias;*

*c) Não observar os itinerários fixados, com o fim de se furtar à fiscalização;*

*d) Não apresentar as mercadorias nas estâncias aduaneiras de destino;*

*é punido com pena de prisão até 3 anos ou com pena de multa até 360 dias, se o valor da prestação tributária em falta for superior a € 15.000 ou, não havendo lugar a prestação tributária, a mercadoria objeto da infracção for de valor aduaneiro superior a € 50.000.(...)”*

O conceito de **fraude em auditoria** é diverso do que vem definido na legislação portuguesa.

Nas **normas internacionais de auditoria do IAASB**, consultando o Glossário, encontramos as seguintes definições:

***“Fraude***

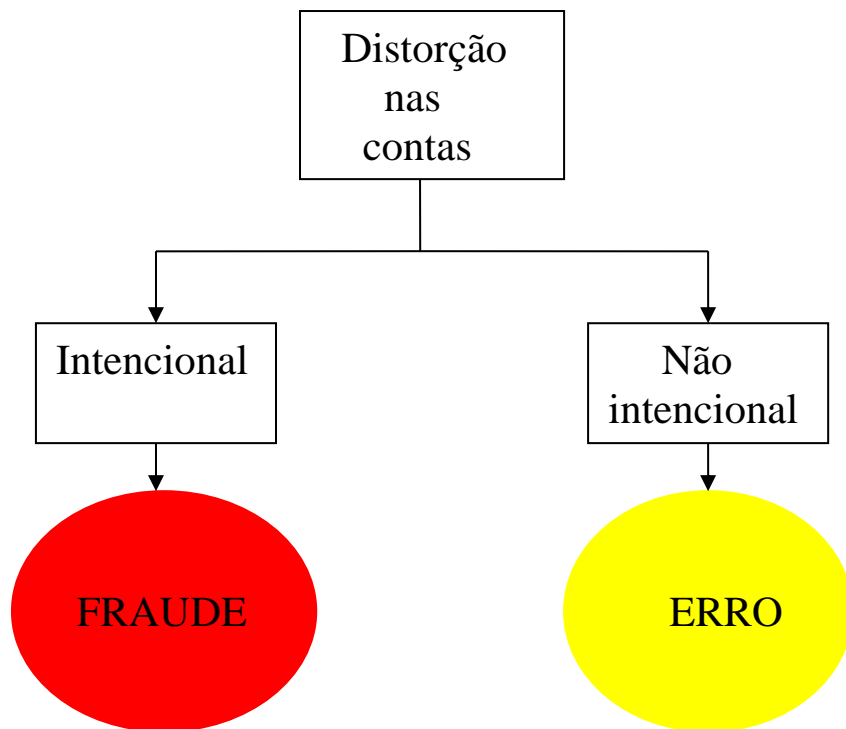
*Um acto intencional praticado por um ou mais indivíduos, de entre a gerência, encarregados da governação, empregados, ou terceiros, envolvendo o uso propositado de falsidades para obter uma vantagem injusta ou ilegal.”*

***“Erro***

*Uma distorção não intencional nas demonstrações financeiras, incluindo a omissão de uma quantia ou de uma divulgação.”*

O nº 2 da *ISA 240 - As Responsabilidades do Auditor Relativas a Fraude numa Auditoria de Demonstrações Financeiras* sintetiza:

**“As distorções nas demonstrações financeiras podem resultar de fraude ou de erro. O que distingue a fraude do erro é se a ação subjacente que resulta na distorção das demonstrações financeiras foi **intencional ou não intencional**”**



- distorção da informação com apropriação indevida de valores

- distorção da informação com propósito manipulador

- Erro de princípio

- Erro de aplicação  
(omissão ou inclusão desacertada)

#### 4.4.2. Tipos de fraude mais comuns

A prática de fraudes, cujo objetivo último é a obtenção de benefícios indevidos por quem nela se envolve, visa normalmente:

- a apropriação indevida de valores
- a manipulação da informação para ludibriar os investidores ou outros terceiros

##### **a) Fraude para apropriação indevida de valores**

- Desfalque  
Ou seja, apropriação indevida de **dinheiro** ou valores equivalentes por empregados com acesso ao cofre ou mediante pagamentos fictícios a terceiros, com encobrimento através de falsificação dos registos
- Desvio de bens  
tais como inventários e outros ativos, com a correspondente manipulação dos registos contabilísticos
- Fraude envolvendo corrupção  
Isto é, com a participação de um empregado em posição de influenciar as decisões de uma empresa, tendo em vista a obtenção de benefícios pessoais em prejuízo desta (diminuindo-lhe os ganhos ou aumentando-lhe os custos). Pode assumir diversas formas:



- Conflitos de interesses  
Quando, por exemplo, o diretor de compras de uma empresa é sócio de outra (“*silent partner*”) que é fornecedora da primeira
  
  - Suborno,  
consubstancia-se na prática de atos prejudiciais à empresa por um empregado em posição de decidir, em troca de dinheiro ou favores a pagar pelo interessado na decisão
  
  - Extorsão  
prática de atos prejudiciais à empresa por um empregado em posição de decidir, sujeito a qualquer forma de ameaça por um terceiro interessado na decisão
- Utilização indevida de ativos  
nomeadamente para benefício pessoal de gestores cimeiros e empregados (automóveis, casas, barcos, etc.)

## **b) Fraude para manipulação da informação**

O objetivo da fraude é dar uma imagem diferente da real (para melhor ou pior), consoante o interesse de quem a perpetrou. Para isso, vários são os “métodos” mais frequentemente utilizados:

- Falsificação ou alteração de registos contabilísticos e da documentação
- Deturpação ou omissão de factos ou transações

- Aplicação errónea intencional dos princípios contabilísticos

Em consequência, se, por exemplo, o objetivo da fraude for o de “melhorar” as DF tendo em vista vender a empresa por um preço superior ao apropriado, os atos fraudulentos a praticar poderão conduzir à

- Sobrevalorização dos ativos
  - Inventários
  - Ativo fixo tangível
  - Dívidas a receber (por exemplo, não registando as perdas de valor ou os riscos de falta de cobrança)
- Diminuição dos gastos reais
  - Especialização inadequada
  - Capitalização inapropriada
  - Falta de depreciações e amortizações
  - Estimativas deficientes
- Empolamento dos proveitos reais
  - Especialização inadequada
  - Vendas fictícias
  - Promoções especiais para aumentar as vendas
  - Vendas intra-grupo (nas contas individuais)
- Redução de passivos
  - Omissão de responsabilidades

#### 4.4.3. Responsabilidade pela deteção e prevenção de fraudes

A **Administração/Gerência** da empresa é quem tem a responsabilidade por instituir e por a funcionar um SCI interno que minimize o risco de ocorrência de fraudes e erros.

A ISA 240, nos seus parágrafos 5 e 6, salienta que “dadas as limitações inerentes de uma auditoria, existe um risco inevitável de que algumas distorções materiais das demonstrações financeiras (particularmente significativo no caso de distorção resultante de fraude) possam não ser detetadas, embora a auditoria seja devidamente planeada e executada de acordo com as ISA.”

De facto, pelo seu próprio método, devido à intervenção humana que sempre envolve e, normalmente, ao recurso à amostragem - mesmo que criteriosamente aplicada – uma auditoria comporta sempre um **risco** de que possam não ser detetadas distorções materialmente relevantes nas demonstrações financeiras.

A descoberta de uma fraude numa empresa sem que a mesma tenha sido detetada pelo auditor, não indica, por si só, que este realizou o seu trabalho de forma negligente. Desde que, através da exibição dos seus papéis de trabalho, o **auditor demonstre que cumpriu as normas de auditoria aplicáveis** – designadamente em matéria de consideração da fraude -, não pode ser considerado responsável pela não deteção da fraude em causa.

#### 4.4.4. A identificação e avaliação do risco de fraude pelo auditor

A *ISA 240*, a que já fizemos referência, atribui ao auditor a responsabilidade por “obter garantia razoável de fiabilidade de que as demonstrações financeiras tomadas como um todo estão isentas de distorção material causada por fraude ou por erro”(§5).

Por isso, na fase de identificação dos riscos de distorção material, o auditor normalmente considera que alguns destes RDM podem ter a sua origem na provável ocorrência de atos fraudulentos. Este trabalho exige que o auditor atue com **ceticismo profissional**, ou seja, que não deixe de admitir a possibilidade de que possa existir uma distorção material devido a fraude, não obstante a sua experiência passada positiva quanto à honestidade e integridade dos responsáveis e generalidade do pessoal da entidade auditada.

De acordo com a *ISA 240* deve ser sempre realizada na fase inicial da auditoria uma **reunião entre os membros da equipa de trabalho** sobre a sensibilidade das DF a distorções materiais causadas por fraude e como esta se poderá concretizar. Esta reunião, segundo a *ISA 240* “deve ter lugar pondo de parte as eventuais convicções dos membros da equipa de trabalho quanto à honestidade e à integridade da gerência e dos encarregados da governação”(§15). Este procedimento visa enfatizar a importância da deteção da fraude no âmbito da auditoria e insere-se na postura cética que o auditor deve adotar.

Depois de identificar os riscos de fraude e de realizar os testes aos controlos destinados a comprovar se os controlos em

vigor são eficazes, o auditor avaliá-los-á e os riscos que vier a considerar de fraude deverão ser objeto de **procedimentos substantivos específicos no plano de auditoria** visando obter segurança adicional sobre a regularidade das situações em causa.

#### 4.4.5. Probabilidade de ocorrência de fraudes e erros

Não há sistemas de controlo interno completamente seguros em matéria de prevenção e deteção de fraudes e erros.

Não são só as fraudes que são importantes em auditoria. Um **erro com materialidade** pode ter grande relevância dado tratar-se de uma distorção nas contas que pode influenciar o processo de decisão do utente da informação financeira. Não obstante, uma **fraude sem materialidade cometida pela Administração** e detetada pelo auditor pode, no entanto, constituir um indicador para ser intensificado o programa de verificações de auditoria, dado o acréscimo de risco que a situação comporta em termos de falta de integridade do órgão de gestão.

Existe maior probabilidade de serem praticadas fraudes em empresas nas quais, para além de um **sistema de controlo interno insatisfatório**, sejam detetados os seguintes condicionalismos:

- dúvidas acerca da integridade ou competência da administração
- a própria administração derroque habitualmente os controlos por esta instituídos

- atribuição de incentivos financeiros baseados em dados constantes das DF (resultados, vendas, etc.)
- pressões fora do habitual sobre dirigentes e gestores da empresa (atingir orçamentos, final de mandato, etc.);
- registo de transações não usuais
- perceção da inexistência ou falta de eficácia dos controlos em certas áreas/operações
- dificuldades em obter colaboração na obtenção da prova do trabalho de auditoria

#### 4.4.6. Dificuldade na deteção de fraudes e erros e redução do risco de ocorrência de fraudes e erros

O risco de que uma distorção material não seja detetada é mais elevado em caso de fraude do que em caso de erro, dado que, no primeiro caso, quem a comete, visa a sua ocultação e pode recorrer a métodos sofisticados e criminosos (falsificação, etc.).

O risco de o auditor não detetar uma distorção material resultante de fraude cometida pela Administração é maior do que para uma fraude praticada pelos empregados, em virtude do maior poder de que dispõem os primeiros e do menor escrutínio a que normalmente estão sujeitos os seus atos.

Particularmente difíceis de detetar são as fraudes que envolvem **conluio** entre empregados, uma vez que tornam aparente a segregação de funções que só nominalmente está implantada.

Para reduzir o risco de ocorrência de fraudes e erros, as empresas devem:

- implantar um sistema de controlo interno eficaz
- criar ou desenvolver a eficácia de um Departamento de auditoria interna

#### 4.4.7. Deveres do ROC/auditor no caso de detetar uma fraude

A atuação subsequente do ROC após ter detetado a prática de uma fraude no decurso da auditoria varia de país para país em função do respetivo enquadramento legal.

Na maioria dos países, os auditores estão obrigados ao sigilo profissional, ao abrigo do qual lhes é vedado dar conhecimento dos factos de que tomam conhecimento no exercício das suas funções. Este sigilo profissional não é, normalmente, absoluto, isto é, a lei protege-o dentro de certos limites. É o que se passa em Portugal, tal como decorre do Estatuto da Ordem dos Revisores Oficiais de Contas, cujo art.º 72º se reproduz na seguidamente:

**“Artigo 72.º  
Sigilo profissional**

1 - Os revisores oficiais de contas não podem prestar a empresas ou outras entidades públicas ou privadas quaisquer informações relativas a factos, documentos ou outras de que tenham tomado conhecimento por motivo de prestação dos seus serviços, **excepto quando a lei o imponha ou quando tal seja autorizado por escrito pela entidade a que diga respeito. (...)**”.

Neste contexto, atendendo ao disposto no n.º 3 do art.º 422º do Código das Sociedades Comerciais – que abaixo também se reproduz - os Revisores Oficiais de Contas devem comunicar às autoridades os **crimes públicos** de que tenham tomado conhecimento no exercício das suas funções.

**“Artigo 422.º**

**Deveres do fiscal único e dos membros do conselho fiscal**

1 – (...)

2 – (...)

3 - O fiscal único, o revisor oficial de contas e os membros do conselho fiscal devem participar ao Ministério Público os factos delituosos de que tenham tomado conhecimento e que constituam crimes públicos.”

Para além ter de comunicar às autoridades as fraudes que constituam crimes públicos, o ROC agirá em função das características dos atos fraudulentos detetados. Assim,

- Se a fraude for cometida por empregados da empresa, o ROC deve informar dos factos a Administração
- quando as fraudes são cometidas pela própria Administração, o ROC deve informar o Presidente da Assembleia Geral e dar-lhe conta do ocorrido, por forma a que os sócios/acionistas sejam informados dos factos em Assembleia Geral ou através da Certificação Legal das Contas.

**Normas de auditoria aplicáveis**

ISA 240 - A Responsabilidade do Auditor ao Considerar a Fraude numa Auditoria de Demonstrações Financeiras