Fernando Rodrigues

Fernando Rodrigues é doutorado em Informática e Gestão de Empresas com especialização em Gestão por Processos de Negócio. Mestre em Modelos de Avaliação de Desempenho. Licenciado em Informática de Gestão pela UAL. É docente de carreira do ISCAL estando integrado na Área Departamental de Ciências da Informação e Comunicação (CIC), onde leciona unidades curriculares de licenciatura e mestrado.
Com um percurso militar iniciado em 1983, no posto de Tenente foi integrado em ações de Defesa Nacional na Força Aérea Portuguesa. Iniciou em 1989 a sua experiência profissional em empresas privadas nacionais e multinacionais, sempre na área dos Sistemas/Tecnologias de Informação. Foi formador no INA na Formação de Dirigentes e acompanhou dezenas de projetos aplicados por todo o país, fazendo parte de júris de avaliação no final dos cursos CAGEP, CADAP e FORGEP.
Tem a certificação CBPP® (*Certified Business Process Professional*) atribuída pela ABPMP. Para além deste livro é também coautor do BPM CBOK Version 4.0: *Association of Business Process Management Professionals International* (*Portuguese Edition*).

A decisão de fazer um Mestrado em Auditoria é sempre um desafio pessoal e profissional de enorme responsabilidade, tanto mais porque a maioria dos estudantes e profissionais que frequentam as aulas sentem que determinadas matérias têm uma elevada potencialidade de aprendizagem, torna o seu dia-a-dia mais fácil e sobretudo, acrescentam valor no mercado de trabalho.
Este é um livro de consulta e estudo obrigatório para compreensão do que significa ASITA aplicada a uma solução de auditoria que o ISCAL protocolou para ser possível assegurar as aulas práticas. Em rigor, a aposta em aprender praticando é o desejo de todos os que pretendem obter o grau de Mestre.
A definição dos trabalhos em auditoria implica adquirir conhecimentos iniciais e básicos de uma Gestão por Processos de Negócio. Compreendendo o que significam os conceitos ao nível da notação BPMN 2.0 é possível apresentar, definir, discutir, propor e acrescentar valor junto dos Clientes que anseiam e exigem explicações sucintas junto das equipas de auditoria sobre os trabalhos realizados no terreno.
A visão e comunicação interna e externa com que as empresas hoje se debatem passa por contratar profissionais certificados para efetuar transformações digitais e liderar com processos e pessoas, não com tecnologia. Este desígnio é sempre referido a todo o momento, até porque os conteúdos técnicos mais significativos e que são ministrados durante o curso noutras unidades curriculares, reforçam a importância dos sistemas de informação, embora a área financeira seja a mais densa em termos de compreensão.
Neste contexto, o livro está orientado ao que se desenvolve na UC ASITA do ISCAL e serve de apoio à matéria que decorre das aulas práticas. O leitor poderá abordar as matérias e os exercícios práticos propostos de duas formas: ordenada e sequencialmente, partindo do início, ou pesquisando diretamente e de livre vontade o que considera ser mais apropriado, aprofundando o conhecimento dos conteúdos com recurso a práticas de *Design Thinking*.
O pensar "fora da caixa" poderá melhor reproduzir o(s) problema(s) que pretende resolver e começar a sua imersão de conceitos, propondo a si próprios casos práticos que podem até vir a ser testados. Procura-se deste modo estimular a vivência em ambiente de "laboratório" tendo em vista a aplicação prática da matéria lecionada e validada perante desafios do mundo real.

Exemplos e perguntas de revisão para:
- Gerir melhor os dados e informação crítica para tomar decisões
- Aumentar o conhecimento de conceitos utilizados no mercado
- Potenciar uma aprendizagem digital a novos modelos de negócio
- Planear uma aposta profissional que garante resultados a curto prazo
- Explorar se a atividade estimula a importância das certificações

9 789893 515839

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

POLITÉCNICO DE LISBOA

FERNANDO RODRIGUES

COLEÇÃO **CAMINHOS DO CONHECIMENTO**

AUDITORIA A SISTEMAS DE INFORMAÇÃO E TECNOLOGIAS APLICADAS (ASITA)

FERNANDO RODRIGUES

AUDITORIA A SISTEMAS DE INFORMAÇÃO E TECNOLOGIAS APLICADAS

FERNANDO RODRIGUES

COLEÇÃO **CAMINHOS DO CONHECIMENTO**

AUDITORIA A SISTEMAS DE INFORMAÇÃO E TECNOLOGIAS APLICADAS (ASITA)

AUDITORIA A SISTEMAS DE INFORMAÇÃO E TECNOLOGIAS APLICADAS

Fernando Rodrigues

AUDITORIA A SISTEMAS DE INFORMAÇÃO E TECNOLOGIAS APLICADAS

(ASITA)

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON

TÍTULO
Auditoria a Sistemas de Informação e Tecnologias Aplicadas

AUTOR
Fernando Rodrigues

EDITOR
Instituto Politécnico de Lisboa

DESIGN DA CAPA
Pedro Antunes

EXECUÇÃO GRÁFICA
Gráfica 99

Fevereiro de 2025

ISBN 978-989-35158-3-9

DEP. LEGAL N.º 544265/25

Agradecimentos

Este livro reúne todo o programa da Unidade Curricular (UC) de Auditoria a Sistemas de Informação e Tecnologias Aplicadas (ASITA), resultante dos últimos 7 anos de aulas ministradas no Mestrado em Auditoria do ISCAL.

Procura-se respeitar o conteúdo programático e temáticas relacionadas com o que é relevante numa clara orientação a futuros mestres em auditoria. Neste contexto, quero agradecer a todos os docentes que diariamente contribuem e desenvolvem documentação pertinente para a aprendizagem nas diversas áreas científicas, que além do autor, merecem ser referenciados globalmente. A todos eles o meu obrigado.

Os possíveis erros, incorreções e omissões que o leitor possa encontrar neste livro são naturalmente da minha total responsabilidade.

Nota Introdutória

Este é um livro de consulta e estudo obrigatório para compreensão do que significa ASITA aplicada a uma solução de auditoria que o ISCAL protocolou para ser possível assegurar as aulas práticas. A definição dos trabalhos em auditoria implica adquirir conhecimentos iniciais e básicos de uma Gestão por Processos de Negócio.

Compreendendo o que significam os conceitos ao nível da notação BPMN 2.0 é possível apresentar, definir, discutir, propor e acrescentar valor junto dos Clientes que anseiam e exigem explicações sucintas junto das equipas de auditoria sobre os trabalhos realizados no terreno.

A visão e comunicação interna e externa com que as empresas hoje se debatem passa por contratar profissionais certificados para efetuar transformações digitais e liderar com processos e pessoas, não com tecnologia.

Neste contexto, o livro está orientado ao que se desenvolve na UC ASITA do ISCAL e serve de apoio à matéria que decorre das aulas práticas. Os alunos devem complementar as matérias deste livro com os exercícios práticos desenvolvidos ao longo das aulas e aprofundar o conhecimento dos conteúdos com recurso a outros materiais de apoio que são distribuídos e recomendados durante a aprendizagem. Procura-se estimular a vivência em ambiente de "laboratório" tendo em vista a aplicação prática da matéria lecionada e validada perante desafios do mundo real.

ÍNDICE

Parte II

Parte III
Glossário

S

T

Índice de Ilustrações

FIGURAS

QUADROS

Introdução

Em contexto de mestrado, os alunos do ISCAL são muito exigentes do ponto de vista pedagógico, no sentido de cada conteúdo poder ser maximizado em termos de aprendizagem, com recurso a casos práticos vivenciados em sala de aula, permitindo a sua resolução direta e discussão para compreensão partilhada utilizando diversas ferramentas de produtividade. Os auditores perante a dificuldade de solucionar problemas em ambiente real com os quais são frequentemente confrontados nas suas atividades e tarefas, optam pela aprendizagem prática.

Este livro permite abordar de forma sucinta a realidade da auditoria quando é confrontada com desafios em ambiente tecnológico. Compreender Processos, as Pessoas e a Tecnologia é algo que no ISCAL é desenvolvido no âmbito de um Projeto Empresarial Aplicado (PEA).

O PEA tem como propósito desenvolver competências em ASITA orientada a indivíduos ou equipas. Existe uma articulação direta entre o PEA e os seguintes *Learning Outcomes*:

- conhecer os papéis de trabalho gerais com documentos de auditoria que podem ser usados e relativos ao impacto das questões tecnológicas em ambiente empresarial, com enfoque especial na atividade de Auditoria a SI;
- compreender os princípios básicos de um arquivo geral completo com documentos e contas, revisão analítica só para números, importação de dados em qualquer formato, diários contabilísticos com a máxima rapidez e nível de detalhe;

- pugnar pelo cumprimento do cibercrime e proteção de dados no que concerne aos SI das organizações, compreender a problemática do investimento em IT, atentar aos aspetos de segurança de IT, desenvolver soluções de análise de dados de informação empresarial, planear e executar testes de auditoria com recurso às TI;
- saber identificar comportamentos de risco na utilização de sistemas e os princípios gerais de segurança, identificar problemas organizacionais resolúveis por ferramentas existentes ou por si construídas;
- programar soluções de análise dos dados e informação plenamente funcionais para resolver os problemas de auditoria verificados.

Nas aulas é estimulado um raciocínio tipo cognitivo permitindo discussões em grupo, pesquisas livres com recurso a novas formas de investigar, recolher dados e informação relevante, que inúmeras vezes está distorcida da realidade e tem de ser validada.

O objetivo geral da UC ASITA é aprofundar o entendimento do que muitos já conhecem em termos profissionais, conhecer as principais realidades e dotar o aluno de meios próprios para desenvolver o conhecimento prático na sua atividade de auditor com as técnicas de modelação, análise e desenho de processos, orientação feita através da solução SAP Signavio.

Os objetivos específicos de aprendizagem passam por conseguir motivar os alunos para a compreensão das realidades e constrangimentos da utilização das tecnologias de informação nos trabalhos de auditoria.

Simultaneamente pretende-se aumentar o nível de autonomia do valor individual de produtividade, retirando valor acrescentado dessas mesmas tecnologias para a realização de tarefas concretas na organização, bem como, a automatização de processos, atividades e tarefas.

Os conteúdos programáticos apresentados permitem, de forma simplificada, tipificar e modelar problemas organizacionais que tendem a consciencializar o aluno para a problemática de desenvolvimento de atividades e tarefas de apoio à auditoria e suas principais dificuldades técnicas, humanas e organizacionais.

Pretende-se que os alunos compreendam o papel da segurança dos SI nas organizações, identifiquem os riscos tecnológicos associados a um problema concreto, analisem dados e informação tendo em vista apresentar propostas concretas que incluem previsão de otimização de soluções. O livro encontra-se dividido em três partes.

A Parte I faz uma breve introdução aos SI, os conceitos chave que se consideram importantes, as tendências que estão a transformar a forma de trabalhar das pessoas e que fazem parte dos principais sistemas de informação aplicados a auditoria, compreendendo ao mesmo tempo sem ser exaustivo de que forma uma Gestão por Processos de Negócio está alinhada com uma solução final assente num relatório que se entrega ao Cliente após os serviços prestados. Incluem-se nesta parte exemplos de soluções com recurso a folha de cálculo, o que permite analisar dados, a sua estrutura e o que significa trabalhar com funcionalidades mais avançadas.

A Parte II utiliza um software específico para auditoria e análise financeira, de acordo com um protocolo assinado entre o ISCAL e a empresa detentora da licença para utilização académica.

Desde o início dos trabalhos de auditoria e atividades prévias, passando pelo planeamento baseado em riscos com execução dos trabalhos, finalização e emissão do relatório, conclusões e ajustamentos dos trabalhos realizados em auditoria, o que é importante clarificar nesta parte é validar o resultado final conseguido, ou seja, como fica a pasta de auditoria, declarações e comunicações trocadas entre as partes, relatórios, arquivo digital.

No final da Parte I e II para que a aprendizagem decorra sem sobressaltos, existem perguntas de revisão agrupadas por níveis para consolidar os conhecimentos.

A Parte III inclui um glossário simplista, mas não exaustivo, de conceitos e termos considerados fundamentais para exercer a profissão de auditor. É vivamente recomendado aos alunos que todos os anos proponham e acrescentem novos termos técnicos, pois esta parte é sempre passível de estar incompleta, em virtude das evoluções constantes que o mercado dita.

Em futuras edições, o autor pondera apresentar um conjunto de exercícios resolvidos e explicados em sala de aula, bem como, testes de avaliação com as respetivas soluções.

Esta mais-valia apenas poderá ser disponibilizada à comunidade em geral no seguimento da aceitação dos leitores a esta obra, tendo em vista a opção pelo método pedagógico que melhor satisfaça as necessidades de cada indivíduo. Toda e qualquer informação adicional, pedido de esclarecimentos ou resposta para as soluções apresentadas devem ser dirigidas ao autor através de correio eletrónico.

Este livro foi criado e escrito com o objetivo de ser útil e acrescentar valor a todos os alunos e comunidade académica em geral. Espero que cumpra esse desígnio.

O autor

Parte I

Conceitos Chave
Sistemas de Informação e Auditoria
Gestão por Processos de Negócio
Análise de Informação em Folha de Cálculo

Módulo 1. Conceitos Chave

O objetivo desta parte é clarificar os conceitos chave com base em exemplos.

1.1 Questões Introdutórias

1.1.1 Sistemas de Informação

Sistemas de Informação é uma expressão utilizada para descrever um Sistema seja ele automatizado (e que pode ser denominado de várias maneiras), seja semi-automatizado ou até mesmo manual, que abrange pessoas, máquinas e/ou métodos organizados para recolher, processar, transmitir e disseminar dados que representam informação para o utilizador e/ou para um Cliente.

Informações têm como base de leitura Dados (em contexto informático, podem ser zeros e uns) são elementos de leitura para qualquer pessoa que de uma forma significativa são úteis para os indivíduos.

Dados são conexões de artefactos em estado bruto que importam eventos que estão a acontecer nas organizações ou num ambiente físico, antes de terem sido organizados e manipulados de uma forma que as pessoas possam entender e utilizar.

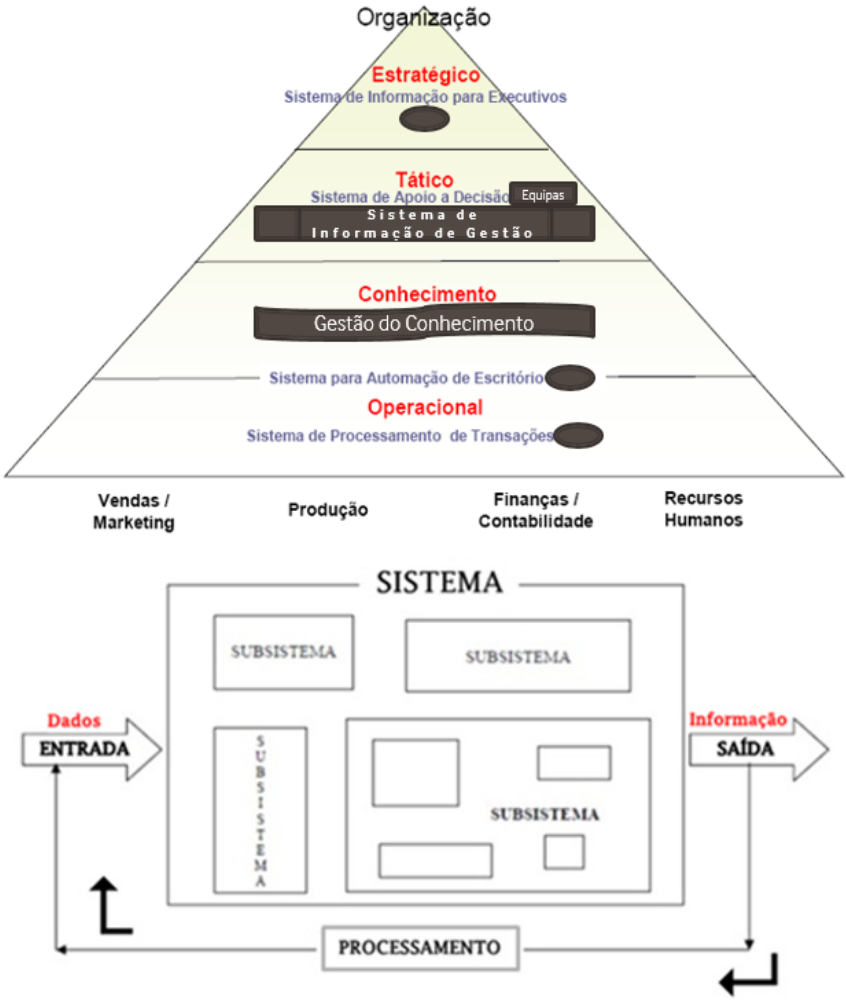


Figura 1. Sistemas de Informação

1.1.2 Tipos de Auditoria Existentes

Podemos definir auditoria como um exame metodológico de uma situação, atividade, função, programa ou sistema de uma determinada entidade, realizado por uma entidade independente e competente, com o objetivo de permitir assegurar a validade material dos elementos que devem ser controlados, verificar a conformidade do tratamento dos factos com as regras, as normas e os procedimentos do sistema de controlo interno, tendo em vista exprimir uma opinião.

Esta opinião é motivada pela conformidade global do objeto da auditoria com as normas legais e regulamentares, cujo resultado final é expressado com a entrega de um relatório.

Auditor é aquele que ouve. Trata-se de um profissional que assume o papel de ouvinte, o que permite no âmbito das suas funções gerar relatórios, corrigir, controlar, interpretar, fiscalizar, avaliar, planear, dar pareceres, fazer levantamentos e recolha de informação.

Podemos enumerar os seguintes tipos de auditoria existentes[1]:

- Externa
- Interna
- Operacional
- Financeira
- Gestão
- Qualidade
- Tecnológica
- Fraude
- Ambiental
- Estratégica
- Marketing
- Sistemas de Informação
- Informática

Entre outras, direta ou indiretamente relacionadas entre si.

Toda e qualquer auditoria serve para fundamentar a atividade e as tarefas realizadas – que uma vez reunidas, consistem na emissão de uma opinião profissional sobre o objeto de análise (**elementos fundamentais**) a fim de ser possível confirmar se estão cumpridas adequadamente as condições que lhe são exigidas.

A função auditoria a Sistemas de Informação (SI) passa pela realização de um exame crítico que tem a finalidade de avaliar a eficácia e a eficiência de dados, informação e conhecimento.

[1] Está disponível no final do livro um Glossário com uma caracterização sumário de conceitos.

1.2 A Função Auditoria a SI

A auditoria a SI implica a realização de um diagnóstico para identificar áreas problemáticas em termos de risco, incluindo a avaliação dos próprios sistemas informáticos, registos e fluxos de informação, organização dos SI, segurança informática, aplicações, sistemas integrados de gestão e programas diversificados.

O impacto desta função no auditor visa sobretudo elaborar sugestões para minimizar o risco, ameaças e vulnerabilidades, procurando maximizar o efeito dos controlos existentes.

Tem como objetivos:

- ✓ Mostrar e relacionar os elementos da função auditoria a SI;
- ✓ Caracterizar as funções e as qualificações técnicas do auditor em tecnologias;
- ✓ Relacionar a auditoria a SI com a função informática.

A razão para auditar SI reúne os seguintes elementos constituintes:

- ✓ No âmbito dos SI
  - o O planeamento estratégico;
  - o A arquitetura dos SI;
  - o As bases de dados e respetivos dicionários.

- ✓ A nível da infraestrutura e das plataformas tecnológicas
  - o As configurações, hardware diverso e as redes;
  - o Os sistemas centrais, departamentais e locais.

- ✓ A nível das ferramentas e aplicações informáticas
  - o Os sistemas de gestão de bases de dados;
  - o Os sistemas de apoio (softwares e aplicativos) geradores e editores de programas, ferramentas de produtividade, como sejam, processadores de texto, folhas de cálculo e afins;
  - o As aplicações de negócio (software aplicacional).

A auditoria a SI combina o que é (o próprio conceito de) auditoria, um complexo sistema gerador de dados e informações, todo um manancial de processamento eletrónico de conhecimento, com o objetivo de garantir vantagens competitivas na cadeia de valor de qualquer organização.

Para simplificar o contexto, dá-se em seguida exemplo de dois processos assentes em mapeamentos, numa visão de alto nível, procurando ilustrar atividades, tarefas, controlos e procedimentos.

1.2.1 Controlos e Segurança

Entende-se por **controlo,** o processo pelo qual se verifica se as atividades de uma organização estão de acordo com um plano de ação desejado e o plano está conforme as atividades dessa mesma organização. Razão pela qual mapear os processos é crítico.

É um processo que habilita o gestor a dirigir e monitorar as suas atividades, abrangendo a sua estrutura de controlo, a qual inclui a sua componente ambiental, os sistemas financeiro-operacionais, as políticas, objetivos, planos, padrões e procedimentos.

Este processo procura a delegação de autoridade para execução, quer no acompanhamento e avaliação contínuos a fim de identificar desvios do quadro traçado, quer ações corretivas para restaurar as operações de acordo com o previsto, quando necessário.

Já no que diz respeito ao **controlo cruzado**, trata-se de um controlo que abrange as operações, registos, documentos, entre outros, realizadas por mais do que uma entidade pública ou privada.

O aumento dos suportes tecnológicos que se baseiam em dados e processam informação, bem como, a complexidade dos mesmos perante cenários globais, permite-nos concluir que o trabalho de auditoria deve ser realizado por equipas que integrem auditores tradicionais e técnicos informáticos (equipas multidisciplinares).

O auditor clássico sem conhecimentos das novas tecnologias e SI fica isolado e terá muitas dificuldades em produzir conclusões suficientemente fundamentadas. Necessita de obter informação complementar, nomeadamente sobre:

- A conceção global do sistema de informação;
- A organização e gestão do departamento de informática;

- A arquitetura conceptual, lógica e física dos SI instalados compreendendo o equipamento, software, comunicações, dados, redes, ambientes de conexão orientados ao negócio;
- Os controlos relativos à operação dos computadores e do software do sistema;
- Os controlos e procedimentos de conceção e manutenção de software e de segurança relativos às diversas aplicações;
- Os procedimentos de entrada e saída de dados nas aplicações relevantes;
- Evolução prevista do sistema de tratamento da informação.

A **segurança** dos SI é um dos mais valiosos ativos e fatores críticos de sucesso das organizações (empresariais ou não empresariais).

Os dados e a informação, quer seja em ambiente internet quer em formato digital, devem ser corretamente protegidos. Na atualidade, todo e qualquer SI constitui um auxiliar importante na tomada de decisão e um meio para o desenvolvimento e suporte do negócio.

Trata-se de recursos estrategicamente determinantes.

No entanto, diversos especialistas chamam a atenção que esta questão ainda não é, nem parece constituir uma prioridade para os gestores e administradores das empresas.

Pode-se constatar que a atenção dispensada à segurança não é proporcional aos elevados riscos associados à perda, dano ou apropriação ilegítima de informação crucial para as organizações.

Existem inúmeros casos e estudos mundiais que evidenciam resultados preocupantes no aumento do número e da gravidade de ataques aos SI, aumento dos custos por incidente de perda ou roubo de dados e informação crítica, desatualização ou mesmo inexistência de planos de prevenção e segurança. São conhecidos os relatórios dos analistas de mercado.

Os processos ajudam a avaliar os custos inerentes à segurança e aos riscos que se pretendem minimizar. A segurança aos SI é uma das áreas mais relevantes para o controlo interno.

Perante dificuldades na mudança constante dos SI e tecnologias de informação cada vez mais evolutivas, a identificação de falhas no controlo e segurança deve ser sustentada por relacionamento entre processos que devem ter em conta a cultura organizacional.

Cabe ao auditor avaliar o ambiente existente, separar a informação concreta e relevante dos suportes tecnológicos que se relacionam.

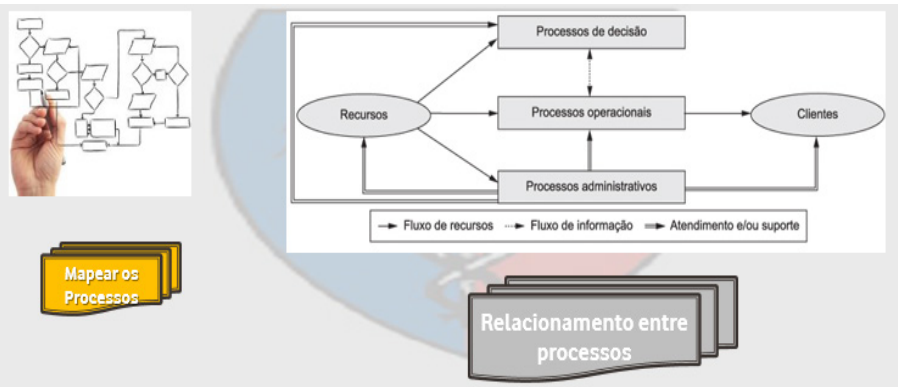


Figura 2 – Relacionamento entre Processos

1.2.2 Técnicas Existentes

Para realizar as suas funções, o auditor dispõe de um conjunto de técnicas adequadas. A sua aplicação implica que sejam considerados elementos como o parâmetro do controlo interno a ser analisado, as condições tecnológicas em que irá ser efetuada a aplicação e a natureza dinâmica (processos) ou estática (resultados) da situação e ambiente informático (digital).

Dependendo das situações de aplicação, as condições de auditoria têm de ser diferenciadas. A apresentação das técnicas considerará o objetivo de aplicação e também a caracterização de cada uma em cada situação da aplicação.

QUESTIONÁRIO

É habitual que o auditor comece por solicitar o preenchimento de questionários previamente impressos e enviados aos responsáveis das diversas áreas a auditar, bem como, a utilizadores relevantes de outros níveis. As respostas permitem uma análise inicial que, por sua vez, irá orientar o trabalho do auditor até à elaboração do seu relatório final.

ENTREVISTAS

É durante as entrevistas que o auditor recolhe informação que complementa a que lhe é facultada por outros meios puramente técnicos ou pelas respostas dos questionários. Deve ser seguida uma preparação muito cuidadosa e diferenciada de acordo com cada caso a analisar, sendo o objetivo alcançar conversações o menos tensas possíveis e respostas com simplicidade.

CHECKLIST

Durante conversas informais reúne-se informação dispersa que é uma excelente oportunidade para obter dados adicionais e que permitem cruzar questionários e entrevistas. Regra geral esta técnica deve ser respondida oralmente, pois a alternativa cómoda de serem enviadas perguntas por correio eletrónico, nem sempre é válida em termos de conteúdos, pontos fracos e pontos fortes.

A clareza das perguntas leva os auditados a responder a partir de pontos de vista muito diferentes, uma vez que estamos perante perfis técnicos e informáticos de profissão, sob o arbítrio do auditor.

Por esta razão é pouco prudente enviar toda e qualquer pergunta sem definir à partida um resumo do pretendido e personalização prévia, garantindo uma imagem de autoridade e de prestígio.

Neste contexto, é importante que existam conjuntos de perguntas organizadas e classificadas por temas, estruturas lógicas e físicas e a ordem da sua formulação técnica.

Por vezes é conveniente que sejam repetidas algumas das perguntas para cada área funcional com o objetivo de se poder comparar as respostas de diferentes fontes. Talvez se consigam descobrir questões contraditórias!

Os Questionários e Checklists podem ser avaliados por dois processos:

1. Checklist com escala de avaliação[2]
2. Checklist com perguntas fechadas[3]

[2] As perguntas devem ser colocadas aos auditados sem qualquer comentário às suas respostas para evitar problemas de fiabilidade e de enviesamento.

[3] Como se infere do nome, as respostas apenas podem ser do tipo “Sim” ou “Não”.

ANÁLISE DE RELATÓRIOS

Esta técnica é muito importante quando se procura avaliar o controlo interno, a eficácia dos SI e a eficiência na execução de atividades e tarefas por parte dos utilizadores, a sua maior ou menor confidencialidade e a utilização da informação que contêm.

Em ambientes tecnológicos e SI os principais pontos fracos dos relatórios passam por já não serem utilizados, a infraestrutura já não é adequada às finalidades pretendidas, não são distribuídos aos destinatários a quem poderia interessar, nem tão pouco é tido em conta o seu caráter confidencial.

ANÁLISE PRESENCIAL

A visita às instalações da organização a auditar é fundamental. Observar e mesmo **fazer em vez de observar** no que se refere a equipamentos, procedimentos e recursos técnicos é crítico.

Quando se pretende analisar vários pontos de controlo clássicos da auditoria e nem sempre os acessos, as rotinas de backup, ficheiros e dispositivos de arquivo (in)seguros, impõe-se uma análise técnica ao ambiente em operação (real e naquele instante).

TÉCNICAS DE ENSAIO COM SIMULAÇÃO

1. *TEST-DECK*

   Submetem-se um conjunto de dados de teste aos programas que vigoram no sistema ou a uma dada rotina relativamente à qual se pretende analisar a sua lógica de processamento.

   A aplicação desta técnica implica que o auditor tenha bons conhecimentos de análise de sistemas.

2. SIMULAÇÃO PARALELA

   O auditor começa por identificar as rotinas que devem ser auditadas 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.

ANÁLISE DO *LOG / ACCOUNTING*

Trata-se do arquivo onde se encontram registados os diversos passos provenientes da utilização do hardware e do software que integram o SI em ambiente tecnológico.

Os ficheiros *Log/Accounting* são anotações históricas que informam sobre as alterações que vão acontecendo e como aconteceram.

Permitem tirar conclusões sobre o software vigente, a sua utilização e dispositivos que integram determinadas configurações ou conjuntos digitais instalados, local ou remotamente.

Estas rotinas são utilizadas frequentemente por pessoal técnico em funções informáticas, sobretudo, relacionadas com segurança.

Na condução de uma auditoria a SI, esta técnica exige sólidos conhecimentos computacionais, além de linguagem apropriada.

MAPEAMENTO ESTATÍSTICO E LÓGICO

Obriga à utilização de ferramentas adequadas e orientadas a uma notação (por exemplo BPMN) tais como o Signavio.

PROGRAMAS ESPECÍFICOS DE AUDITORIA

No que se refere à análise de SI, os auditores utilizam métodos cruzados que confirmam ou não os valores atribuídos a cada um dos parâmetros mais importantes de um sistema.

Os valores desses parâmetros devem estar compreendidos num intervalo indicado pelo fabricante. Exemplos: CaseWare (IDEA) e ASD Auditor.

Existem dois tipos de programas usualmente utilizados:

1. RASTREIO DE PROGRAMAS
2. SOFTWARE PARA AUDITORIA.

Figura 3 – Programas Específicos de Auditoria

Perguntas de Revisão

1) Qual é a diferença entre Auditoria Informática (AI) e Auditoria a Tecnologias de Informação TI)?
   - AI trata de avaliar o próprio sistema informático. TI incide especialmente no sistema de controlo interno da organização auditada.
   - AI consiste na análise e avaliação sistemática das áreas operacionais de uma organização. TI incide na análise dos sistemas e ambiente informático de uma organização.
   - AI trata de avaliar o próprio sistema informático. TI incide na análise dos sistemas e ambiente informático de uma organização.
   - Todas as alternativas estão incorretas.

2) São exemplos práticos de aplicações informáticas:
   - É o processo através do qual é possível não só identificar os riscos relevantes para a concretização dos objetivos da organização como analisá-los.
   - Conjunto de softwares que permitem analisar as forças, fraquezas, ameaças e oportunidades.

- Programa ou conjunto de programas informáticos aplicados a um conjunto de utilizadores específicos.
- Sistemas de remuneração, sistema de processamento dos reembolsos de um imposto, sistema integrado de gestão (ERP), entre outros.

Módulo 2. Sistemas de Informação e Auditoria

2.1 Avaliação do Risco

Um auditor (interno) ao efetuar o levantamento preliminar de um Sistema de Informação (SI), tem necessariamente associada uma atividade/processo, deverá considerar os seguintes fatores:

1. Característica da empresa

   Cultura ética;
   Estrutura organizativa;
   Controlos implementados;
   Modelo de avaliação de desempenho;
   Estrutura de "*fringe benefits*";
   Pressão para atingir os objetivos;
   Conflito de interesses e procedimentos de controlo;
   Princípios de boa governação (*Corporate Governance*).

2. Mudanças recentes na gestão, nos SI e nos postos (áreas de negócio) operacionais

3. Os ativos existentes, os serviços vendidos e o seu impacto em irregularidades

4. Os controlos instituídos em operações chave

5. Os normativos e enquadramento regulador dos SI

6. O resultado de auditorias anteriores

7. O mercado em que a empresa opera

8. As recomendações dos consultores, por trabalhos contratados pela gestão

9. A tecnologia e a complexidade do hardware e software dos SI

10. A aquisição / desenvolvimento recente de software de importância estratégica para o negócio (Core Business)

11. A missão, visão, valores, lema, vetores estratégicos, objetivos, indicadores e iniciativas, incluindo os meios da Equipa de SI, se são (ou não) adequados ao negócio / atividade da empresa

12. Os orçamentos dos SI são devidamente estruturados e adequadamente objeto de controlo

13. Os contratos celebrados no âmbito dos SI e respetivos controlos instituídos

14. A existência de um Plano Estratégico de Informação

15. A existência de um Plano de Segurança (*Disaster Recovery*) com reporte adequado

16. A existência de um Departamento de Segurança da Informação

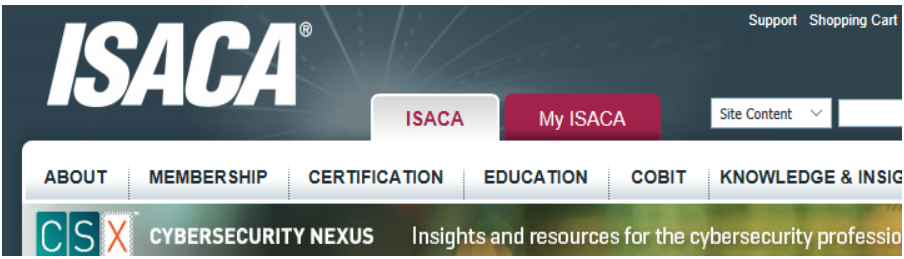
17. A existência de um plano de seguros para cobertura dos riscos

18. A existência de um plano de controlos de acessos lógicos, com especial relevância para a informação estratégica

19. O impacto da regulamentação e legislação aplicável aos SI da empresa

Entre outros…

2.2 Normas de Auditoria de SI (*standards for information systems auditing*)



010 – Departamento de auditoria de SI
020 – Independência
030 – Ética e Normas
040 – Competência
050 – Planeamento
060 – Avaliação da auditora
070 – Relatório
080 – Follow-up

2.3 Sistema Tecnológico da i 4.0

Ecossistema pode ser analisado em torno de 3 eixos, onde se evidenciam as tecnologias "core"

i. Sistemas avançados de informação

- Infraestrutura digital
- Inteligência artificial e algoritmos preditivos
- Análise avançada de dados
- *Cloud computing*
- Cibersegurança

ii. Conectividade entre sistemas, equipamentos, produtos e pessoas

- Sensores avançados e IoT
- Operação remota
- Realidade aumentada
- Máquinas inteligentes

iii. Sistemas avançados de produção

- Produtos e materiais avançados e conectados
- Operações modulares
- Produção aditiva
- Robôs autónomos

As empresas com maior sucesso não serão necessariamente as mais fortes à partida, mas as que demonstram maior agilidade e capacidade de adaptação.

2.4 Lei da Proteção de Dados Pessoais A Importância na existência de um Regulamento da Proteção de Dados para as Empresas

Enquadramento

A proteção de dados pessoais tem sido um tema importante na União Europeia desde há mais de 20 anos, cujo último desenvolvimento relevante foi a aprovação, pelo Parlamento Europeu, do novo Regulamento Geral de Proteção de Dados ("RGPD").

O RGPD entrou em vigor em maio de 2018. Qualquer empresa, ainda que não estabelecida na União Europeia, que recolha e trate dados pessoais de residentes num dos Estados-Membros deverá cumprir com as obrigações do RGPD.

As mudanças significativas que resultam do RGPD terão, como é evidente, um impacto diferente nas organizações, dependendo da sua natureza, área de atividade, dimensão e tipo de tratamento de dados que realizem.

No entanto, ainda que o impacto possa ser diferente, a generalidade das organizações terá de implementar medidas, em termos organizacionais e procedimentais, por um lado, e tecnológicos, por outro, por forma a se adaptarem ao RGPD.

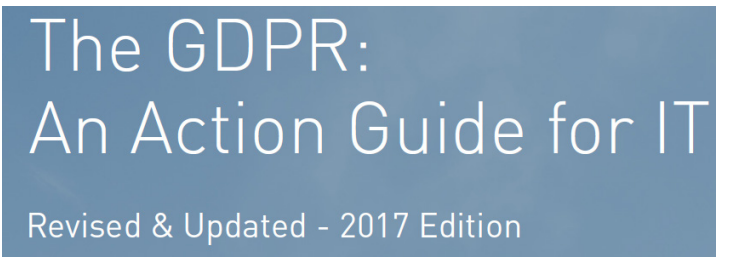
2.4.1 O Novo Regime Europeu da Proteção de Dados

O tratamento dos dados pessoais deve ser feito de forma transparente e com respeito pela reserva da vida privada, bem como salvaguardar os direitos, liberdades e garantias.

A globalização e evolução tecnológica trouxeram novos desafios, aos quais o novo RGPD está a tentar dar resposta, as normas são complexas e o seu incumprimento traz pesadas sanções.

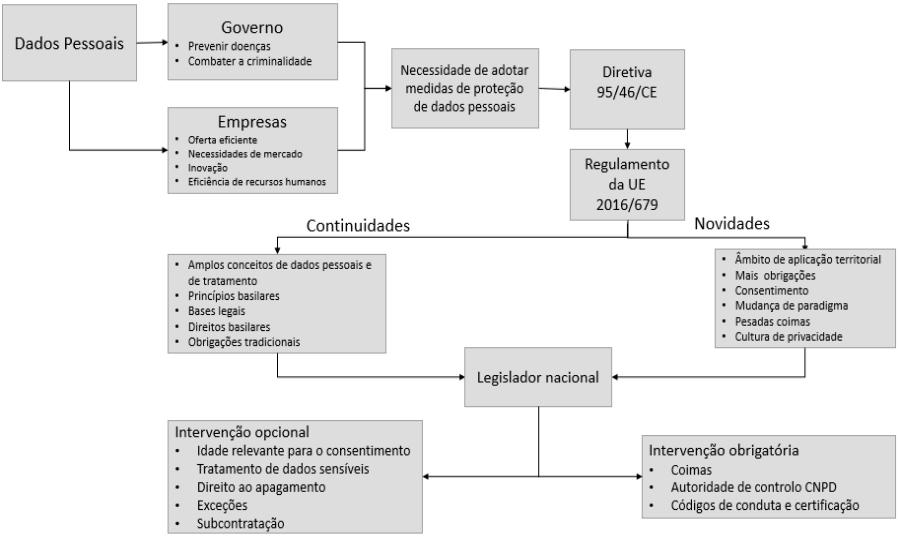
Entrou em vigor em maio de 2018 passou a vigorar nos 28 Estados Membros.

Mais informação deve ser consultada, interpretada e com leitura mais atenta, a quem se mostrar interessado, embora a presente recomendação seja feita a título particular e a nível de cultura geral. O leitor deve procurar em "GDPR_Action_Guide_eBook.pdf".



Apresenta-se em seguida um mapeamento exemplificativo da importância do RGPD.

2.4.2 Mapeamento da importância do RGPD



Quadro 1 – Mapeamento da Importância do RGPD

2.5 Lei do Cibercrime

O cibercrime é o nome atribuído aos crimes informáticos que envolvam qualquer atividade ou prática ilícita na rede pública global (conhecida por internet), isto é, infrações cometidas com o recurso aos sistemas eletrónicos e às novas tecnologias de informação.

Estes crimes podem envolver invasões de sistema, dissipação de vírus, roubo de dados pessoais, acesso a informações confidenciais, entre outras situações mais ou menos tecnologicamente evoluídas. Com a expansão das redes de comunicação, em especial a internet, cada vez mais as atividades económicas, financeiras e de negócio das sociedades modernas e do mundo globalizado dependem do uso dessas redes e das aplicações que nelas assentam.

Neste contexto, assumem crescente relevo, também, as atividades ilegais associadas às redes de comunicação, usando-as para efeitos criminosos e explorando as suas vulnerabilidades, o que torna a cibercriminalidade uma ameaça dos tempos modernos.

Portugal tem, desde 1991, um quadro normativo tendente a punir os então denominados "crimes informáticos" ("Lei da Criminalidade Informática"). Este diploma adequado à realidade que se destinava a regular à data da sua aprovação, tornou-se deficitário. Surgiram entretanto novas realidades que têm vindo a ser descritas e consideradas como crime por muitas outras legislações europeias e por instrumentos internacionais. Foi por isso necessário a revisão desta lei.

A nova lei, aprovada em 2005, relativa a ataques contra sistemas de informação, descreve comportamentos que deverão ser qualificados como crime, obrigando também à criação de normas conexas, relacionadas com tais comportamentos, relativos à instigação, auxílio, cumplicidade e tentativa, responsabilidade de pessoas coletivas, competência territorial e ainda intercâmbio de informações.

Características do Cibercrime

- É muitas vezes transnacional, o que dificulta as investigações;
- Com o aumento dos computadores pessoais, permite que qualquer pessoa no mundo possa realizar práticas criminosas a partir de qualquer lugar, hora ou zona geográfica.

Exemplos de Cibercrime

- Acesso ilegítimo a dados ou informações de outrem;
- Interceção e reprodução ilegítimas;
- Roubo de dados e informação;
- Pornografia infantil;
- Lavagem de dinheiro;
- Ciberterrorismo;
- Ciberativismo *

  *) atividade contra organizações que defendem determinadas causas.

Envolve o roubo de informações e manipulações das mesmas e a divulgação ao público. É uma prática que deixa as autoridades com dificuldades em punir os seus responsáveis, muitas vezes por falta de leis aplicáveis a determinado tipo de infrações.

Para prevenir estes crimes, os especialistas aconselham o máximo cuidado a ter na utilização frequente da internet, dando-se como exemplos, emails suspeitos recebidos e sites pouco conhecidos.

Legislação relativa ao Cibercrime

Lei n.º 109/2009, de 15 de setembro – Estabelece as disposições penais, materiais e processuais, relativa a ataques contra os sistemas de informação, adota a diretiva interna à Convenção sobre o Cibercrime do Conselho Europeu.

Surgiu no seguimento de uma outra lei já existente em Portugal desde 1991 e que acrescentou algumas ideias fundamentais sobre a prática do cibercrime.

Qual é a importância do Cibercrime na nossa vida?

A lei do cibercrime é importante na vida do cidadão no sentido em que:

- Condena a quem introduzir ou apagar dados informáticos produzindo dados não genuínos, quem tentar causar prejuízo a outro ou usar documentos; produzidos através de roubo de dados, ou a quem importar ou vender dados;
- Visa salvaguardar ao máximo os direitos fundamentais dos cidadãos, protegendo-nos contra o uso ilegal e não permitido da nossa informação pessoal;
- Responde a preocupações relevantes dos cidadãos e dá a quem tem a responsabilidade de enfrentar a cibercriminalidade novos e muito necessários instrumentos, para cujo bom uso são necessários meios adequados e estratégias concretas no plano nacional e internacional.

Esta lei dá-nos segurança contra crimes informáticos, visto que estes podem ser punidos. Antes desta legislação, crimes como a cópia de cartões de débito ou de crédito não eram penalizados, o acesso a computadores para obter qualquer tipo de informação não era sancionado, a criação e propagação de um vírus não era punível.

Assim, esta legislação vem sancionar os seguintes atos criminosos:

- Através da Lei do Cibercrime, a produção e a difusão de um vírus passam a ser punidas com uma pena que pode ir até 10 (dez) anos de prisão;
- Esta lei fornece ao sistema processual penal normas que permitem a obtenção de dados de tráfego e a realização de interceções de comunicações em investigações de crimes praticados no ambiente virtual;
- Esta lei considera todos os crimes informáticos graves.

A Lei do Cibercrime foi criada para combater e condenar os crimes informáticos. Esta lei foi imposta em parte devido à Convenção sobre Cibercrime do Conselho da Europa. Faz referência a diversos crimes que podem ser praticados na internet: como sejam:

- a interceção e adulteração de documentos ou dados;
- a "falsidade informática", dentro da qual nos podemos referir a burla informática e a usurpação de uma identidade online, também conhecida como fishing;
- pirataria informática também referida por "reprodução ilegítima de um programa protegido".

Para além disto permite, por exemplo, a recolha de endereços de Internet Protocol (IP) em caso de investigação de um crime.

É importante não esquecer o efeito que têm sobre as vítimas, começando pelo impacto a nível financeiro, tomando-se como exemplos adicionais os seguintes:

- o roubo de identidade;
- impacto legal, pois a vítima pode ser acusada de diversos crimes;
- o impacto emocional, nalguns casos leva inclusive à paranoia.

2.6 Segurança dos SI

Plano de Recuperação ou Continuidade do Negócio

Atividades a executar (5 fases)

I. Arranque
II. Redução de riscos e avaliação do impacto
III. Desenvolvimento do plano
IV. Implementação do plano
V. Manutenção e atualização

I. ARRANQUE DO PROJETO

- ❑ Objetivos, Âmbito, Pressupostos e Terminologia
- ❑ Modelo de Gestão do Projeto (segundo uma metodologia comprovada)
- ❑ Atividades
  - o Levantamento de Funções Críticas
  - o Tarefas
- ❑ Gestão de um Programa de Segurança

II. REDUÇÃO DE RISCOS E AVALIAÇÃO DO IMPACTO

- ❑ Criação de Medidas (que evitam tanto a ocorrência do desastre como danos significativos daí resultantes)
- ❑ Ato de Prevenção (ocorrências que antecedem o que origina o desastre)
- ❑ Mecanismos e Procedimentos
  - o Ocorrem tanto antes como depois do incidente
  - o Permitem limitar o impacto
  - o Medidas que são tomadas durante a contingência

- ❑ Contingência é composta por:
  - o Fases de recuperação e regresso à normalidade
  - o Casos em que o incidente provoque mais do que uma mera indisponibilidade do serviço ou da operação de negócio

II. REDUÇÃO DE RISCOS E AVALIAÇÃO DO IMPACTO

II. a) ANÁLISE DE RISCO

- ❑ Grau de risco efetivo (probabilidade de concretização de um ataque pela vulnerabilidade existente a esse ataque)
- ❑ Identificação das ameaças
- ❑ Determinar as vulnerabilidades
- ❑ Calcular a probabilidade de ocorrência (das ameaças identificadas face às vulnerabilidades detetadas)
- ❑ Controlo de riscos
- ❑ Análise de impacto no negócio

III. DESENVOLVIMENTO DO PLANO

- ❑ Documento único
- ❑ Plano ou Procedimento
- ❑ Flexibilidade e independência
- ❑ Plano alternativo (inflexibilidade, desadequação, esforços inúteis)
- ❑ Plano com pontos únicos de falha
- ❑ Estratégias de proteção (dados, informação, equipamentos, redes…)
- ❑ Criação de Medidas (que evitem tanto a ocorrência do desastre como danos significativos daí resultantes)

III. a) PLANO DE CONTINGÊNCIA

- ❑ Matriz de responsabilidades em contingência
- ❑ Plano de recuperação
- ❑ Plano de regresso à normalidade
- ❑ Plano de gestão de crise

IV. IMPLEMENTAÇÃO DO PLANO

- ❑ Aquisição de meios
- ❑ Plano de testes
- ❑ Sensibilização e formação

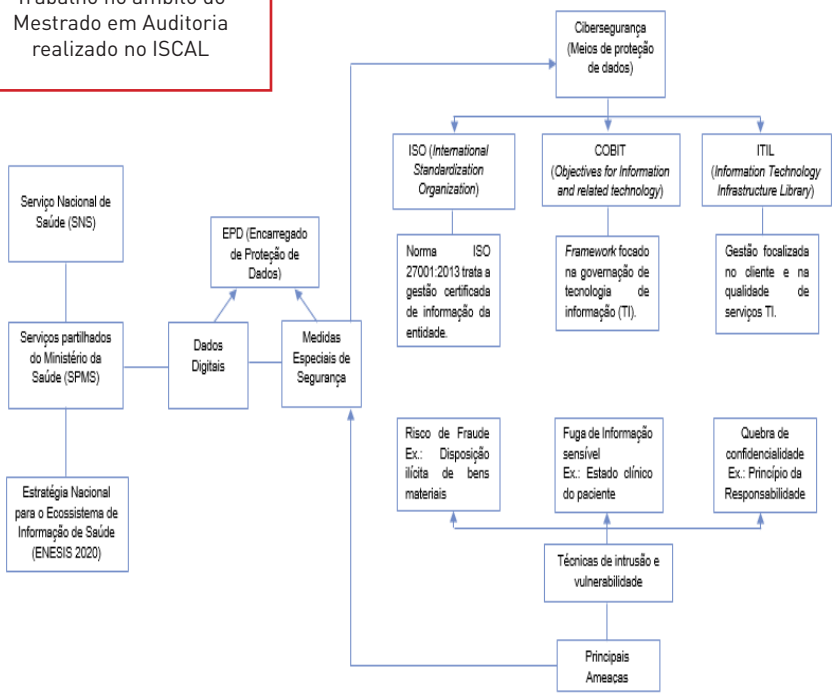
V. MANUTENÇÃO E ATUALIZAÇÃO

- ❑ Plano de exercícios e sensibilização
- ❑ Plano de atualização
- ❑ Frameworks, metodologias e técnicas existentes
- ❑ Orientação a uma Gestão por Processos de Negócio
- ❑ Considerações gerais e propostas de melhoria
- ❑ Aquisição de meios

Figura 4 – Plano de Recuperação ou Continuidade de Negócio

2.7 Mapeamento de Cibersegurança no SNS

Resultado final de um exercício prático desenvolvido em aula pelos diversos Grupos de Trabalho no âmbito do Mestrado em Auditoria realizado no ISCAL



Quadro 2 – Mapeamento de Cibersegurança no SNS

Tendo em vista a ratificação do Regulamento Geral da Proteção de Dados (RGPD), as entidades por este abrangidas adquiriram a necessidade não só de eleger um delegado responsável pela supervisão do sistema de controlo dos dados dos recursos humanos, como também de realizar frequentes auditorias à sua Organização.

Nesta medida, tanto o Auditor como o Encarregado da Proteção de Dados (EPD) têm funções fundamentais que, embora diferentes, procuram alcançar o mesmo propósito. Logo, é esperado que trabalhem em constante comunicação e conformidade.

Auditor	**EPD**
Auditorias regulares sobre o cumprimento das disposições do RGPD	Gerir a equipa: Contratar, Formar e Orientar
Contacto direto com o EPD	Realização de avaliações de risco (PIA)
Tentativa da eliminação dos riscos de fraude	Comunicação de falhas relativas à informação do utente
Garante a efetividade dos controlos organizacionais	Zelar pelo cumprimento da legislação (RGPD)
Auditoria Externa (Interesse público)	**Auditoria Interna (Interesse privado)**

Quadro 3 – Comparativo entre a posição do Auditor e do EPD

Após análise do quadro acima, é possível afirmar que a posição do Auditor e do EPD tem de ser exercida por pessoas distintas.

O EPD tem como função realizar uma auditoria interna e comunicar o seu resultado ao auditor externo, sendo que este desempenha um papel de interesse público, que recai sobre o Estado.

Em relação ao Modelo de Cibersegurança aplicado ao SNS, o Auditor, que representa uma entidade pública tem como obrigação reportar ao Conselho de Administração todas as irregularidades detetadas que o auditor interno não cumpra. Perante esta exigência, é estritamente necessário que o EPD exerça as suas obrigações e que as comunique ao Auditor.

Outros mapeamentos e exercícios foram e estão a ser resolvidos todos os anos letivos. Decerto mereceriam e irão ter uma leitura atenta e/ou atenção ao seu enunciado. Por manifesta ausência de espaço e oportunidade não os podemos listar.

2.8 A Importância da Auditoria a Sistemas de Informação

É importante clarificar a importância da Auditoria a Sistemas de Informação (ASI) no contexto do presente livro, uma vez que o leitor procura respostas às necessidades que são manifestadas por todos. O autor poderia desenvolver com mais profundidade este desígnio. Sucede que o ISCAL tem um Mestrado disponível no mercado e com elevada procura todos os anos.

Os alunos procuram através de casos práticos executar atividades e tarefas ao longo das aulas, utilizando os conhecimentos adquiridos por experiência e prática. Ao contrário de conhecimentos teóricos ou científicos, apresentam resoluções para problemas concretos, um pensamento crítico constante, em que o objetivo final é a discussão de soluções, evidenciando o Saber-Fazer.

Seria académica e manifestamente inviável listar todos os exemplos trabalhados, haveria por parte de alguns alunos envolvidos e pelos próprios grupos de trabalho, incompreensão, pelo facto da divulgação da sua propriedade intelectual estar a ser feita, sem o seu aval, consentimento e aprovação. Deste modo, o autor limita-se a resumir alguns pressupostos considerados relevantes para aumentar o interesse dos potenciais candidatos a Mestre em Auditoria, estando o ISCAL disponível para receber todos aqueles que se queiram candidatar e em condições de continuar a evoluir nestas áreas. Serão muito bem-vindos.

A este propósito o livro inclui diversas Referências Bibliográficas que podem ajudar a estimular o interesse em ASI, uma vez que todos os Mestres que foram orientados pelo autor até ao momento encontram-se referenciados, estando as suas obras disponíveis para consulta pública através do Repositório do IPL.

Importa ainda observar que a evolução exponencial da tecnologia, desde a criação de *robots* com sistemas de inteligência artificial até ao surgimento de aplicações que evidenciam novos conceitos, são sobretudo inovações, que no dia de hoje podem inclusive estar totalmente ultrapassadas. Um exemplo concreto e que tem causado alguma disrupção é o *blockchain*, também conhecido como *Distributed Ledger Technology*, o qual tem sido amplamente discutido e que tem provocado interesse a nível global.

Muito do que se ensina e promove tem de fazer sentido para acrescentar valor ao mercado. No caso concreto da ASI convidamos tod@s a ler os trabalhos publicados pelos nossos Mestres com inusitada orientação a tecnologia, pese embora sejam partes interessadas e estejam a desenvolver consultoria, integrados em projetos ou mesmo a liderar equipas, exercendo auditoria com uma forte componente contabilística e financeira, áreas de conhecimento onde o ISCAL por tradição é reconhecido desde a sua fundação.

2.8.1 A Auditoria em Portugal

Em Portugal, a Ordem dos Revisores Oficiais de Contas (OROC) é o organismo responsável pela representação e regulamentação da área de auditoria. Toda e qualquer matéria relativa à revisão legal das contas, auditoria às contas e/ou serviços relacionados estão sujeitas ao normativo deste órgão.

Neste enquadramento, quando se alguém se refere a "auditoria das demonstrações financeiras", pretende-se normalmente fazer referência à revisão legal das contas ou à auditoria às contas, atividades que, em Portugal, estão exclusivamente adstritas à profissão de Revisor Oficial de Contas (ROC) sujeitas à jurisdição da OROC.

Ao longo do tempo, o regimento na atividade de ROC em Portugal foi sofrendo diversas atualizações. Desde diversas regulamentações até à própria entrada como membro efetivo, cuja admissão na OROC é feita através de cursos de preparação para exame, extremamente exigentes e do ponto de vista técnico, algo complexos no sentido de o sucesso ser à partida garantido. Como tudo na vida o (in)sucesso faz parte do nosso quotidiano.

Apesar das dificuldades conhecidas, os alunos do ISCAL que conseguem vaga, que frequentam o curso e que finalizam o Mestrado, a grande maioria tem como objetivo, um dia, reunir as aptidões e os conhecimentos para fazer o exame de admissão à OROC. Nem todos são bem-sucedidos, mas é um excelente ponto de partida.

2.8.2 Processos de Negócio em Auditoria

Antes de iniciar os trabalhos, o auditor necessita de criar um processo principal de auditoria.

É necessário igualmente elaborar um plano adequado para o desenvolvimento dos trabalhos. Trata-se de uma operação contínua que implica refazer atividades e tarefas, bem como, avaliar provas com o intuito de formular julgamentos válidos e acertados.

A definição a nível operacional dos passos a seguir na realização de uma auditoria é essencial para precaver situações indesejadas e realizar um trabalho bem-sucedido, por forma a possibilitar uma tomada de decisão eficaz.

Como qualquer processo de negócio a auditoria também requer um fluxo de atividades e tarefas para garantir que são cumpridos todos os requisitos obrigatórios e que os procedimentos são realizados eficaz e eficientemente.

Em termos genéricos, os processos de negócio que envolvem auditoria, estão de acordo com diversos manuais de auditoria, o mais pesquisado e utilizado é o manual do Tribunal de Contas.

De acordo com as referências citadas, os processos de negócio desenvolvem-se em quatro fases distintas, conforme demonstrado na figura seguinte.

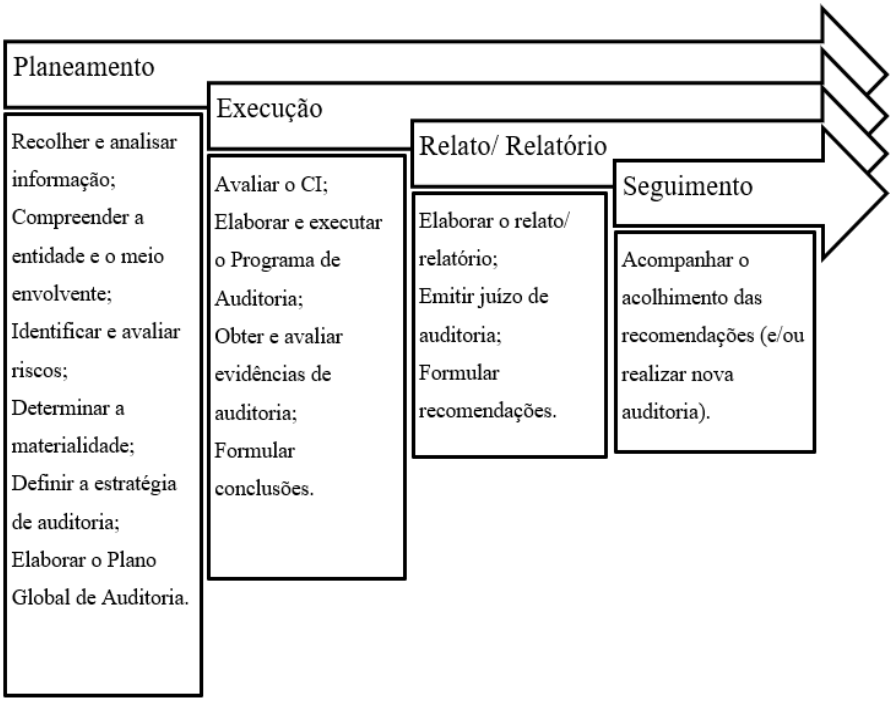


Figura 5 – Processo de Auditoria

Processos em auditoria são contínuos e dinâmicos, uma vez que existe a possibilidade de trabalhar em simultâneo em diferentes fases, conforme descrito na figura 6 e se necessário, à semelhança de qualquer planeamento, reajustar a estratégia.

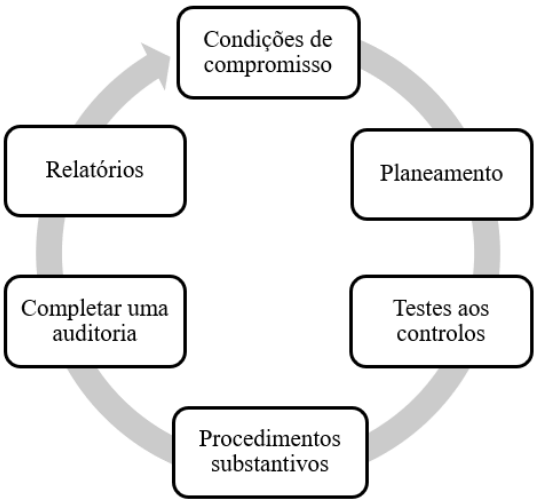


Figura 6 – Fases de uma Auditoria

Em seguida, resumem-se cada uma das fases indicadas na figura 6 para clarificar as operações.

Condições de compromisso

Esta é a primeira fase de uma auditoria e incide sobre a decisão acerca da aceitação (quando se trata de um Cliente novo) ou continuidade de um Cliente (retenção dos Clientes atuais). Trata-se de uma das decisões mais importantes a serem tomadas pelos auditores e cujo objetivo passa por fazer uma avaliação do risco profissional relativamente à associação a determinado Cliente.

Neste sentido, para garantir o cumprimento dos requisitos necessários de suporte à tomada de decisão de aceitar ou não um compromisso, as empresas de auditoria devem adotar um conjunto de procedimentos que proporcionem a obtenção de uma conclusão fiável abrangente a todos os intervenientes que vão participar na respetiva auditoria.

Planeamento

O planeamento constitui uma das etapas mais importantes de um trabalho de auditoria. Esta fase contempla a elaboração de uma estratégia de todos os procedimentos a serem cumpridos e é vital para uma Organização adequada do trabalho a desenvolver.

O desenvolvimento de um planeamento de auditoria pressupõe o estudo prévio de todas as etapas a realizar, com base no conhecimento obtido sobre a atividade da entidade auditada, os fatores económicos relevantes e a legislação aplicável. A elaboração de um efetivo planeamento possibilita à empresa de auditoria a obtenção de ganhos de eficiência e eficácia nos trabalhos, evitando desperdícios de tempo e uso de técnicas desajustadas.

Esta fase de planeamento é uma etapa imprescindível num trabalho de auditoria, uma vez que beneficia todo o processo em termos económicos e operativos e ao ser planeado todo o trabalho, permite garantir a competência e qualidade do trabalho ao menor custo possível, bem como, reduzir o risco de auditoria.

A figura seguinte sintetiza os diversos aspetos que um plano global de auditoria deve englobar.

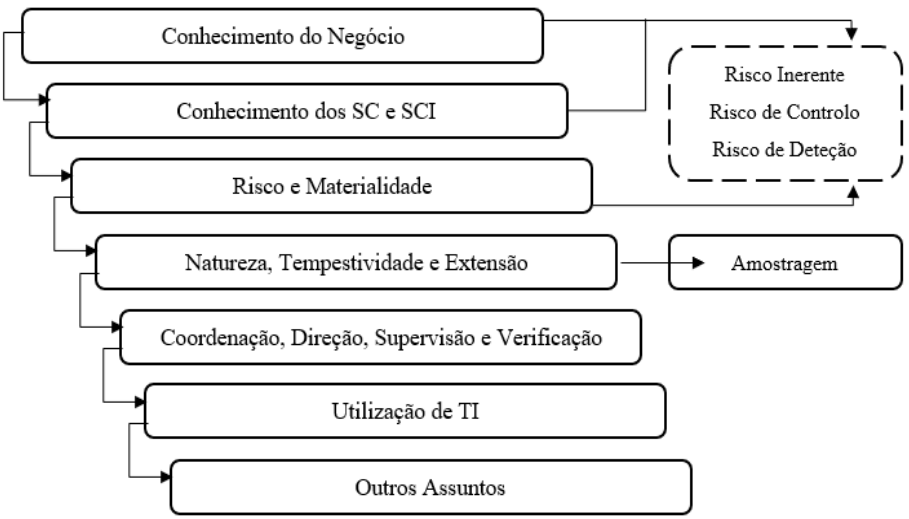


Figura 7 – Plano Global de Auditoria

Testes aos controlos

O conhecimento dos SI e de controlo interno é crucial para que o auditor possa identificar previamente os procedimentos e as normas contabilísticas adotadas pela entidade auditada, para poder validar a sua uniformidade e consistência.

Os testes aos controlos são procedimentos de auditoria desenvolvidos para avaliarem a eficácia operacional do controlo interno relativamente à eventualidade de existirem distorções materiais nas demonstrações financeiras. Estes procedimentos permitem prevenir, detetar e corrigir erros.

Procedimentos substantivos

Os procedimentos substantivos têm como principal finalidade a deteção de eventuais distorções materialmente relevantes sobre a matéria de auditoria cuja deteção não foi identificada pelo sistema de controlo interno.

Completar uma auditoria

Assegurar que a auditoria foi conduzida de forma eficiente e eficaz é um dos requisitos para que as expectativas dos utilizadores da informação financeira sejam alcançadas. Esta fase engloba a análise dos seguintes pontos:

- Continuidade da empresa
- Ajustamentos e reclassificações
- Divulgações
- Acontecimentos subsequentes

Relatórios

A missão primordial de um revisor/auditor é a de, após a realização da análise e avaliação das contas de uma empresa, emitir um documento que expresse uma opinião verdadeira e apropriada sobre as demonstrações financeiras. Esta constitui, portanto, a fase final de um trabalho de auditoria.

Em Portugal, este documento é denominado por Certificação Legal de Contas (CLC), o qual passou a ser de caráter obrigatório a partir de 1983, ano em que foram aprovadas as primeiras Normas Técnicas de Revisão Legal de Contas da OROC. Mais tarde, em 1993, no seguimento da aprovação do novo regime jurídico dos ROC, o modelo da CLC sofreu algumas alterações.

Qualquer trabalho de auditoria requer a realização de um conjunto de tarefas pertencentes a determinadas fases do processo, por forma a que o fluxo do trabalho corresponda ao que se pretende, bem como, para garantir que são cumpridos todos os requisitos obrigatórios.

A figura 8 na página seguinte sintetiza o processo principal global que uma auditoria apresenta.

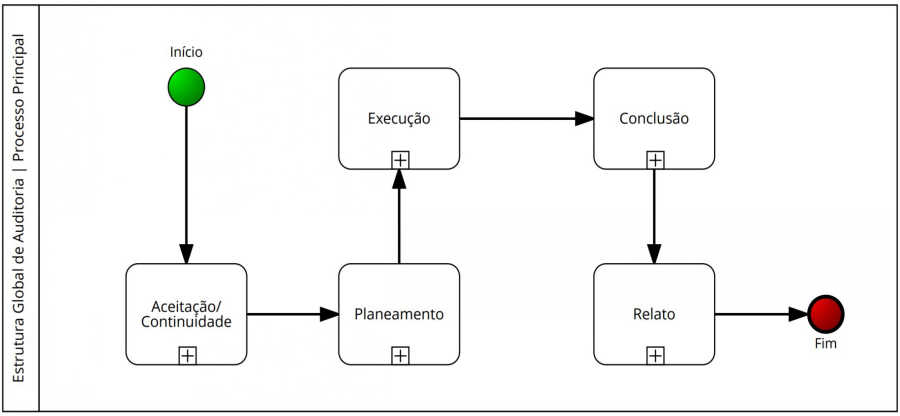


Figura 8 – Processo Principal de Auditoria

Cada uma das fases apresentadas, está representada por subprocessos cujo desenvolvimento é efetuado por atividades e tarefas que se subdividem por outros subprocessos.

2.8.3 As Limitações de um Trabalho de Auditoria

O desenvolvimento dos trabalhos em auditoria depende, em grande parte, da qualidade da informação financeira divulgada, a qual deverá ser fiável, relevante, precisa, comparável e por conseguinte, deverá refletir a imagem verdadeira e apropriada da Organização.

Neste contexto, a auditoria, por resultar numa opinião independente, baseada numa análise criteriosa e sustentada sobre todos os aspetos materialmente relevantes contidos nas demonstrações financeiras, representa uma componente importante no estabelecimento da confiança entre as partes relacionadas e interessadas de um negócio.

A execução de uma auditoria, pela sua abrangência e incidência, não permite analisar e verificar toda a documentação e transações que ocorreram. Neste sentido, existe uma noção tradicional conhecida por "*Audit Expectation Gap*" que se verifica relativamente à necessidade de *Compliance* e de uma gestão de risco efetiva.

Em suma, a atividade de auditoria apresenta diversas limitações, como por exemplo, o custo razoável, o período temporal, as estimativas e os critérios contabilísticos, a determinação da materialidade, o relatório de auditoria e o próprio risco de auditoria que resumidamente, representa "o risco de o auditor expressar uma opinião de auditoria inapropriada quando as demonstrações financeiras estão materialmente distorcidas" (de acordo com a ISA 320).

Segundo esta norma, os auditores limitam a sua responsabilidade à análise e avaliação da informação considerada materialmente relevante.

2.8.4 Relação entre Tecnologias de Informação e Auditoria

Perante o exigente desafio dos normativos e regras aplicáveis aos trabalhos que se executam, surgem as TI e a consequente contínua implementação de novos SI que têm afetado significativamente os ambientes corporativos em todas as áreas de negócio, da qual a auditoria não é exceção, reforçando a necessidade de automatização dos SI.

Apesar das TI terem influenciado significativamente a profissão de auditoria nas últimas décadas, o propósito para a realização de auditorias permanece igual. O que existe com mais complexidade é a necessidade de uma adaptação quanto aos procedimentos e métodos de que a auditoria se deve servir para se ajustar a novos contextos. Embora sejam utilizados diversos métodos e soluções suportadas por aplicações informáticas, o objetivo do trabalho de auditoria não se altera.

É neste desafio constante que a ASI deve ser ajustada para que seja possível desenvolver o trabalho necessário atendendo à complexidade dos SI de qualquer empresa. Dadas as circunstâncias atuais, é requerido aos auditores que expressem uma opinião verdadeira e apropriada baseada em elevados volumes de dados e informação, com uma estrutura de análise demasiado complexa. É através do recurso a soluções orientadas a auditoria que os profissionais conseguirão analisar o enorme volume de dados que têm pela frente.

Num contexto de mudança e melhoria contínua, a maior parte das empresas têm os seus processos razoavelmente informatizados, contribuindo para o desenvolvimento da ASI, quer para o aumento da sua sustentabilidade e suporte das operações, quer para a sua prospeção.

É nesta realidade que o funcionamento, o controlo e a fiabilidade dos processos existentes determinam a importância da ASI, pelo que a auditoria sem este conhecimento orientado ao negócio poderia tornar-se irrelevante e dispensável.

A ASI abrange um conjunto de mecanismos no que respeita à análise e controlo de sistemas de processamento de informação, à validação da implementação de novos sistemas e à avaliação da eficiência e eficácia da utilização dos recursos informáticos, criando, deste modo, uma convergência das necessidades da gestão ao nível empresarial com os SI.

O âmbito da ASI é claramente estabelecido pela necessidade de uma verificação contínua aos SI, por forma a providenciar uma garantia fiável acerca da eficácia dos mesmos, uma vez que os auditores são elementos independentes orientados para garantir a conformidade dos procedimentos necessários de acordo com as exigências legais, bem como, verificar a capacidade de respostas efetivas na eventual existência de falhas.

Um auditor de SI deve atestar a robustez e a conformidade dos controlos aplicáveis, bem como, a fiabilidade da informação por estes produzida, atendendo aos normativos legais em vigor, por forma a emitir a opinião acerca das contas da empresa em questão com base na recolha de evidências e garantindo que não existem riscos materiais passíveis de causar danos significativos, quer à Organização, quer às partes interessadas.

De um modo sintético, a principal responsabilidade da ASI prende-se com a análise e avaliação dos riscos significativos inerentes aos SI que suportam os processos de negócio desenvolvidos pela empresa/Organização.

Perante esta realidade, é evidente que um auditor de SI deve ser detentor de um conjunto de um conjunto de competências e conhecimento em áreas específicas que num dado momento se pensaria que são dispensáveis para a emissão da sua opinião.

Para que mantenha a sua competência, é fundamental desenvolver e dominar uma enorme quantidade de aptidões e novo conhecimento que lhe permitam trabalhar e compreender uma linguagem tecnológica que tem de dominar, em suportes digitais diversos e onde se encontra a realidade que não está nas pastas físicas, de modo a emitir o seu parecer com base num trabalho isento de erros e possíveis riscos.

A título de exemplo e para terminar, a ASI justifica-se desde logo pela existência de quase 3.000 programas certificados pela Autoridade Tributária. O cumprimento das obrigações fiscais veio acelerar a utilização de SI diversos e regular certificação prévia dos programas informáticos de faturação. Sucede que apesar das vantagens, introduz nos trabalhos de auditoria novos riscos em termos de controlo fiscal, pela possibilidade de subsequente adulteração dos dados registados, potenciando situações de evasão fiscal.

Existem milhares de declarações de IRS, IVA e IRC com as respetivas transações associadas. O autor conhecendo a realidade do mercado tem proposto novas linhas de investigação futuras em resultado das regras e modelos de negócio que estão continuadamente a acontecer.

Os textos anteriores foram escolhas de parte de conteúdos de dissertações e adaptadas ao contexto pretendido. O autor teve o privilégio de conduzir, orientar e supervisionar investigações que se encontram publicadas e estão devidamente referenciadas no livro. Optou-se por apresentar apenas breves resumos ao que a ASI diz respeito.

Um agradecimento especial às autoras Catarina Incozi (Mestre em Auditoria), Hélia Machel (Mestre e Auditora de SI em Moçambique) e Cláudia Moreira (Mestre em Controlo de Gestão e Avaliação de Desempenho) pelo mérito obtido, defesa oral e desempenho que manifestaram perante os júris no decorrer das provas públicas.

Perguntas de Revisão

1) Por que razão a segurança dos SI é um dos mais valiosos ativos e fatores críticos de sucesso das organizações?
   - Os dados e a informação, quer seja em ambiente internet, quer em formato digital, devem ser corretamente protegidos.
   - Trata-se de recursos estrategicamente determinantes.
   - Todo e qualquer SI constitui um auxiliar importante na tomada de decisão e um meio para o desenvolvimento e suporte do negócio.
   - Todas as alternativas são complementares.

2) A visita às instalações da organização a auditar é fundamental. Qual é a técnica que se aplica na prática de fazer em vez de observar?
   - Análise de Relatórios.
   - Análise Presencial.
   - Técnicas de Ensaio com Simulação.
   - Simulação Paralela.

3) O que se entende por Cibercrime?
   - É uma atividade criminosa baseada em sistemas eletrónicos e nas novas tecnologias de informação.
   - São crimes que podem envolver invasões de sistema, roubo de dados pessoais, acesso a informações não confidenciais, entre outras situações.
   - São infrações cometidas com o recurso a ferramentas eletrónicas e às novas tecnologias de informação.
   - Corresponde aos crimes praticados com recurso a computadores e/ou à Internet. Destaca-se o furto de identidade.

Módulo 3. Gestão por Processos de Negócio

O que são Processos de Negócio? De acordo com o CBOK 4.0. Guia de Conhecimento para uma Gestão por Processos de Negócio, existem três tipos diferentes de processos de negócio numa visão ponta a ponta:

- Processos Primários (frequentemente referidos como Processos Principais ou Macroprocessos)
- Processos de Suporte
- Processos de Gestão

Na maioria das Organizações, os processos primários constituem cerca de 20% das atividades corporativas, enquanto os processos de suporte constituem 70% e os processos de gestão, representam 10%.

Processos Primários (20%) – são processos ponta a ponta, interfuncionais, que entregam diretamente valor aos Clientes. São frequentemente referidos como processos principais, pois representam as atividades essenciais que uma Organização realiza para cumprir a sua missão em alinhamento com a estratégia definida.

Processos de Suporte (70%) – os processos de suporte são concebidos para apoiar os processos primários, muitas vezes através da gestão de recursos e/ou infraestrutura, exigidos pelos processos primários. A principal diferença entre processos de suporte e processos primários é que os processos de suporte não fornecem valor diretamente aos Clientes, enquanto os processos primários fornecem.

Processos de Gestão (10%) – os processos de gestão são utilizados para medir, monitorizar e controlar as atividades corporativas. Os processos de gestão garantem que um processo primário ou de suporte atenda aos objetivos operacionais, financeiros, regulatórios e legais. Em rigor não agregam valor diretamente aos Clientes, mas são necessários para garantir que a Organização opere de forma eficaz e eficiente.

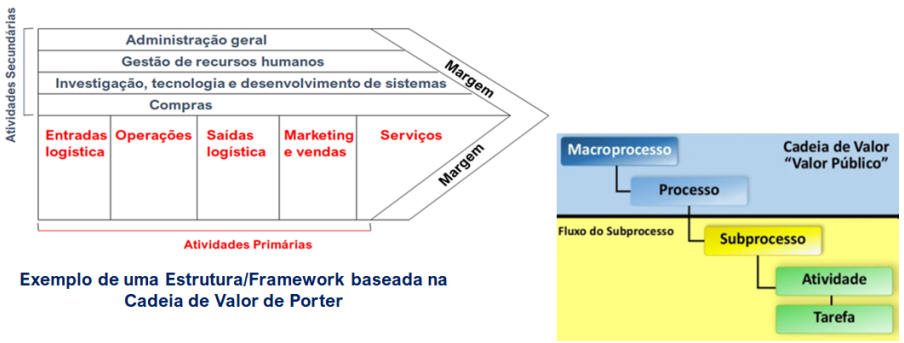
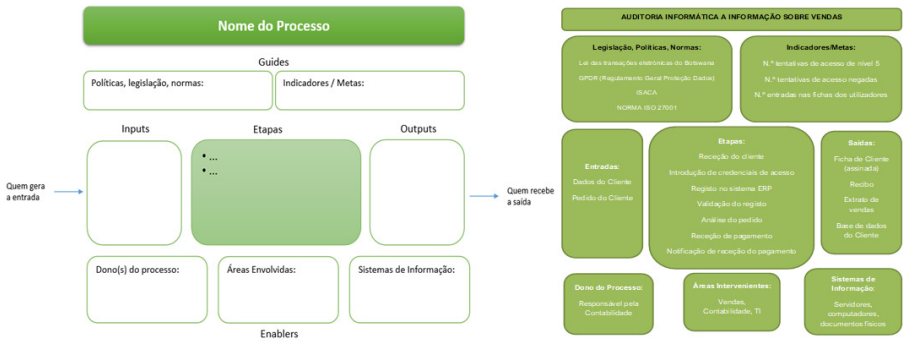


Figura 9 – Cadeia de Valor de Porter

3.1 Casos Práticos para Modelação de Processos

Proposta para uma iniciação a processos de forma básica sem recurso a fluxogramas:



Quadro 4 – Proposta iniciação a Processos sem recurso a Fluxogramas

Naturalmente que o leitor à medida que for desenvolvendo aptidões, competências e nível de compreensão em termos de negócio que realmente acrescente valor ao Cliente, é desafiado a modelar, analisar e desenhar processos, o que significa em termos de maturidade evoluir para a notação BPMN 2.0.

O *Business Process Model and Notation* 2.0 é um padrão criado pela *Business Process Management Initiative*, entretanto fundido com o *Object Management Group* (OMG), um grupo que define padrões de sistemas de informação.

O BPMN tem uma aceitação crescente como padrão sob várias perspetivas, o que resultou na sua inclusão em várias das ferramentas de modelação mais amplamente utilizadas. Fornece um conjunto robusto de símbolos para a modelação de diferentes aspetos dos processos de negócio.

Como a maioria das notações modernas, os símbolos descrevem relações definidas, tais como, fluxos de trabalho e ordem de precedência. A figura seguinte mostra um exemplo simples de um diagrama de processos em BPMN.

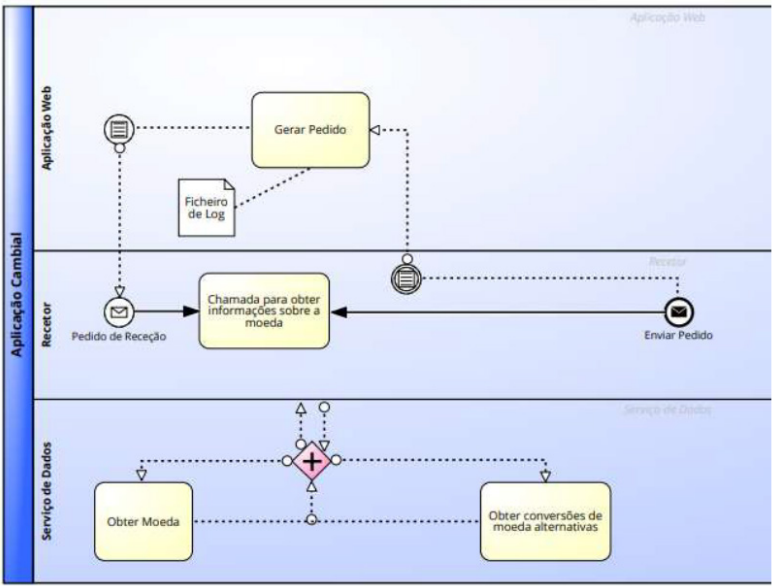


Figura 10 – Notação BPMN

Principais Características

- Versão 2 (BPMN 2.0) representa uma significativa maturação e solidificação da notação
- Mais de 100 ícones no total, organizados em conjuntos descritivos e analíticos para atender às diferentes necessidades dos utilizadores
- Notação muito precisa que indica:
  - o Eventos iniciais, intermediários e finais
  - o Atividades e fluxos de mensagens
  - o Comunicações intra corporativas e colaboração interempresarial
  - o Atividades e fluxos de dados

Quando devemos usar

- Para apresentar um modelo de um processo a múltiplos conjuntos de audiências
- Para simular um processo de negócio com um motor de processos
- Para executar um processo

Vantagens

- Utilização e compreensão generalizados; considerado por muitos como sendo o padrão de facto nos EUA e noutros países a nível global
- Utilização significativa no Departamento de Defesa americano e outras entidades governamentais
- Uma das notações mais poderosas e versáteis para identificar restrições de processos

Desvantagens

- Requer formação e experiência para usar corretamente todo o conjunto de símbolos
- É difícil ver as relações entre vários níveis de um processo
- Diferentes ferramentas de modelação podem suportar diferentes subconjuntos da notação

- As origens das TI inibem a sua utilização com outros membros da comunidade empresarial de algumas organizações.

Para mais informações, consultar:

- O site dedicado ao *Object Management Group* em www.bpmn.org
- Ficheiros de ajuda e amostras com modelos na maioria das principais ferramentas de modelação

Como observações finais sobre este módulo, importa clarificar que os alunos que frequentam a UC ASITA têm como base de entendimento outras abordagens quando chegam à sala de aula.

Estimulados com exercícios práticos e sem qualquer formação prévia orientada à notação BPMN, desenvolvem com enorme entusiasmo processos AS-IS e simulações TO-BE, com recurso a desenho técnico que é modelado, aplicado e explicado a problemas concretos em auditoria.

O resultado final de trabalhos realizados demonstra-se com exemplos. Obviamente que é uma simples amostra não exaustiva do esforço e dedicação que empregam perante os desafios colocados.

Exemplo 1 de um Processo de Auditoria a um SI

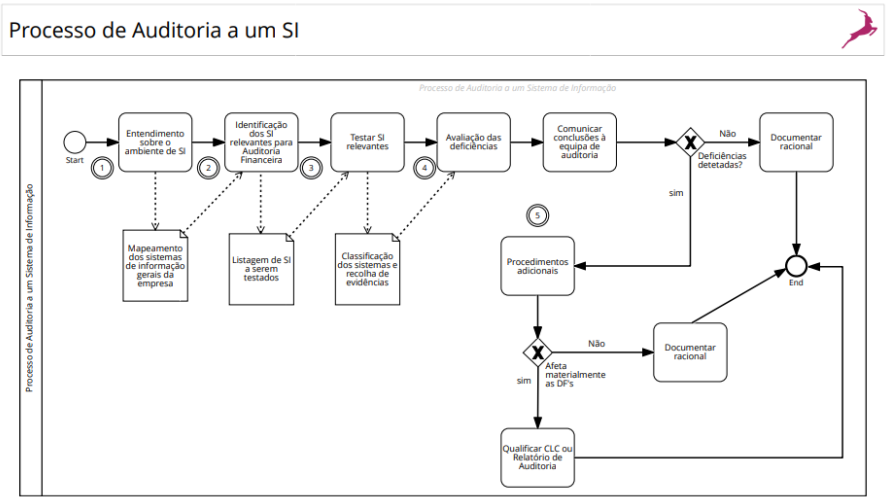


Figura 11 – Processo de Auditoria a um SI

Exemplo 2 de um Processo de Auditoria Financeira

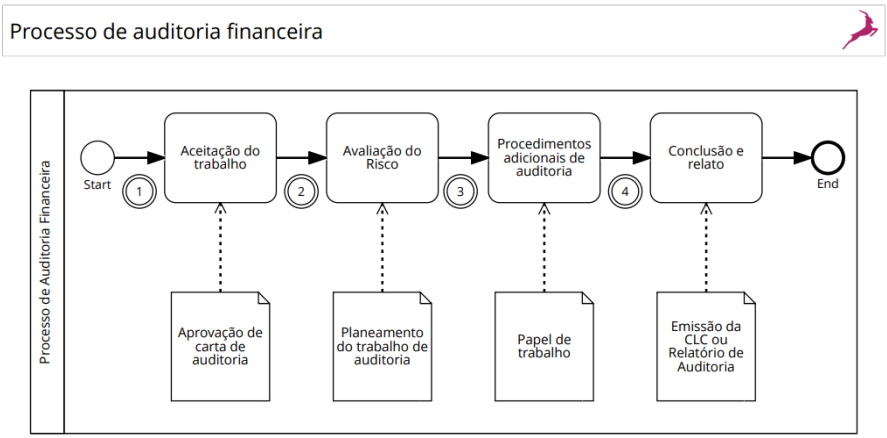


Figura 12 – Processo de Auditoria Financeira

O resultado final das figuras propostas permite clarificar**: Dados** não são Informação, **Informação** não é Conhecimento, **Conhecimento** não é Compreensão, **Compreensão** não é Sabedoria.

Proposta para iniciação a processos de forma profissional com recurso a notação BPMN 2.0:

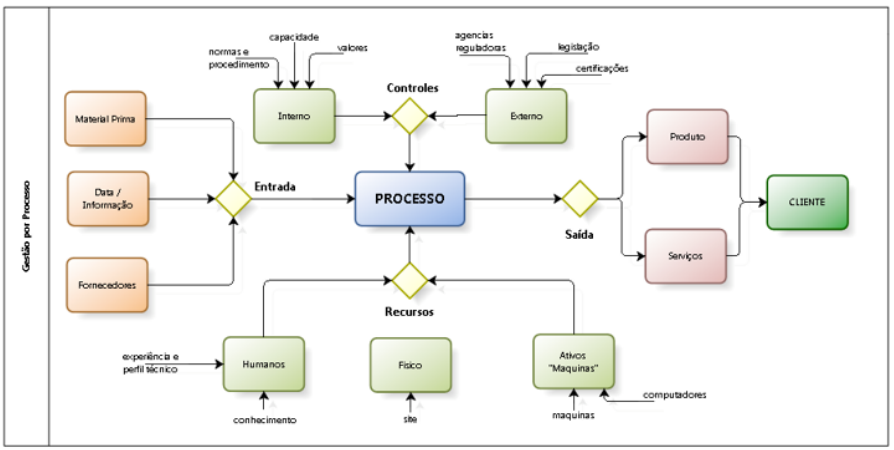


Figura 13 - Proposta para Iniciação a Processos

Em termos de estímulo para investigação e produção científica, a figura seguinte é partilhada com o leitor que por vezes tem dúvidas sobre as fases que uma dissertação ou tese significam.

Cabe aos orientadores acompanharem os seus alunos em todas as fases de investigação, sendo obrigatório um apoio permanente perante as dificuldades sentidas ao longo do tempo. No que diz respeito a lacunas de comunicação o exemplo seguinte ilustra o que realmente importa:

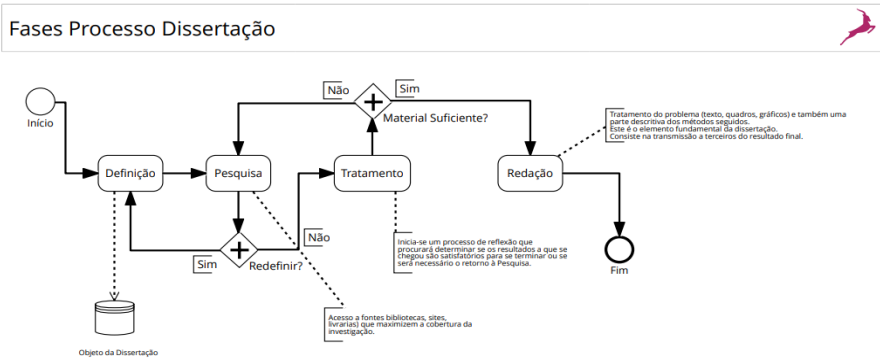


Figura 14 - Fases Processo Dissertação

Muito mais haveria para contextualizar, merecer uma leitura mais atenta com outros exemplos trabalhados sobre este módulo, mas devido a restrições de espaço e oportunidade o autor não os vai listar, o que não significa que em futuras edições não o possa fazer. Esta decisão será sempre reavaliada caso o leitor manifeste interesse em aprofundar estes conteúdos.

Perguntas de Revisão

1) Existem diversas notações que se podem utilizar em Processos. BPMN é das mais utilizadas. Qual é a melhor definição?
   - É uma notação que recorre a formas geométricas standardizadas para descrever um processo.
   - É uma notação que recorre a algoritmos que depois são traduzidos numa linguagem de programação.

- É uma mescla entre linguagem natural e linguagem formal.
- É uma forma de representar algoritmos evitando ambiguidades e redundância.

2) Por vezes o auditor é obrigado a utilizar ferramentas adequadas tais como o SAP Signavio. Em que técnica esta aplicação informática se aplica?
   - Análise de Processos.
   - Análise do Log / Accounting.
   - Programas Específicos de Auditoria.
   - Mapeamento Estatístico e Lógico.

3) Qual é a melhor definição para uma boa Governação orientada a Processos?
   - Um conjunto de processos e ferramentas de auditoria que são implementados para controlar uma organização.
   - Um conjunto de processos e modelos que os auditores trabalham com o objetivo de entregar o seu Plano de Auditoria.
   - Um conjunto de processos e técnicas que uma vez implementados permitem ajustamentos e reclassificações.
   - Um conjunto de processos e estruturas que são implementados para dirigir uma organização.

Módulo 4. Análise de Informação em Folha de Cálculo

Este módulo inicia uma abordagem a tabelas e gráficos dinâmicos. O seu conteúdo é trabalhado em sala de aula, no entanto não é matéria que faça parte integrante dos testes que se realizam.

A sua pertinência e exemplificação prática diz-nos que são provavelmente dois dos melhores exemplos de ferramentas informáticas que os auditores utilizam e que demonstram as enormes potencialidades do *Excel* para tratar, resumir e analisar grandes quantidades de dados.

Uma *Pivot Table* é uma tabela interativa que automaticamente cruza a informação de vários campos (colunas) de uma tabela de dados e em função desse cruzamento apresenta determinados resumos ou cálculos. Uma das características interessantes das *Pivot Tables* reside no facto da sua estrutura ser facilmente alterada através da inclusão, rotação ou reconfiguração dos campos utilizados nas suas linhas e colunas, permitindo a observação de diferentes resultados e informação.

A partir de dados recolhidos no terreno existe alguma dificuldade em obter exemplos com informação que seja útil e que acrescente valor a todos os alunos. Deste modo é durante as aulas que os Grupos de Trabalho (GT) escolhem os seus próprios dados que podem ser recolhidos em qualquer Empresa/Organização na qual já estiveram envolvidos em projetos, que deverão ser processados, estruturados ou organizados na perspetiva de uma investigação já realizada.

O objetivo final deste primeiro exercício será:

- Construir tabelas criadas por cada GT que representam vendas mensais numa empresa;

- Transformar a tabela estática em tabela dinâmica de acordo com o modelo exemplo;
- Aplicar filtros sobre os rótulos (áreas das linhas e colunas);
- Criar gráficos dinâmicos que combinem e demonstrem resumos interativos;
- Outras funcionalidades avançadas para justificar os dados obtidos e gerar um relatório.

Exercício 1. *Pivot Tables* – Proposta com Valor Acrescentado

O modelo exemplo que se segue permite iniciar uma abordagem possível a desenvolver.

	A	B	C	D
1	Mês	Custos		%
2		Mensais	Acumulados	
3	Fev	989,98 €	989,98 €	9%
4	Mar	1 774,82 €	2 764,80 €	24%
5	Abr	1 249,64 €	4 014,44 €	35%
6	Mai	2 239,42 €	6 253,86 €	54%
7	Jun	3 249,40 €	9 503,26 €	82%
8	Jul	1 209,50 €	10 712,75 €	93%
9	Ago	839,66 €	11 552,42 €	100%
10	Total	11 552,42 €		

Quadro 5 – Iniciar Pivot Tables

No modelo anterior a coluna C foi construída com a fórmula =SOMA (B$3: B3) e a coluna D foi calculada a partir da coluna B (=B3 / B$10). Para o total, média e outros valores a considerar, o autor não aprofunda a forma como se executam os cálculos, dado que no ISCAL os alunos iniciam este tipo de exercícios e têm prática reconhecida logo no 1.º ciclo de estudos.

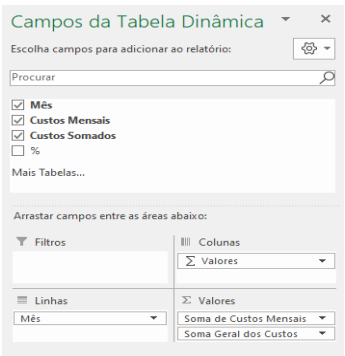
Exercício 2. *Pivot Tables* – Metodologia(s) a Implementar

O leitor deve genericamente criar uma tabela dinâmica que realize os seguintes passos:

1. Selecione uma célula da tabela de origem;

2. No separador **Inserir**, grupo **Tabelas**, selecionar o comando **Tabela Dinâmica**;
3. Completar a caixa de diálogo "**Criar Tabela Dinâmica**" (figura modelo seguinte) tendo em consideração as seguintes opções:
   - Escolha os dados que pretende analisar;
     - Selecionar uma tabela ou intervalo;
     - Utilizar uma origem de dados externa;
     - Utilizar o Modelo de Dados deste livro.
   - Escolha onde pretende colocar o relatório da Tabela Dinâmica.

Meses	Soma de Custos Mensais	Soma Geral dos Custos
Fev	989,98 €	989,98 €
Mar	1 774,82 €	2 764,80 €
Abr	1 249,64 €	4 014,44 €
Mai	2 239,42 €	6 253,86 €
Jun	3 249,40 €	9 503,26 €
Jul	1 209,50 €	10 712,75 €
Ago	839,66 €	11 552,42 €
Média	1 650,35 €	
Total	11 552,42 €	
(em branco)		
Total Geral	**24 755,18 €**	**45 791,49 €**



Quadro 6 – Como é criada uma Pivot Table

Exercício 3. *Pivot Tables* – Gráficos Dinâmicos

Em sala de aula e livremente, cada GT faz as suas recomendações de acordo com o gráfico escolhido, que irá combinar o resumo interativo fornecido pela tabela dinâmica criada.

Terminada a parte de *Pivot Tables* seguimos para uma análise de informação mais robusta, em que o seu conteúdo é igualmente trabalhado em sala de aula, sendo que podem ser cenários de ambiente real vivenciados nas empresas. Os resultados são discutidos entre todos os GT. Esta matéria também não faz parte dos testes que se realizam em regime de avaliação contínua.

Exercício 4. Simulações e Processos de Previsão (Resultados)

Este exercício tem duas partes que são complementares. A Parte I é de Nível Intermédio. A Parte II é de Nível Avançado. As técnicas de simulações de dados dão suporte às atividades de apoio à decisão e também aos processos de previsão.

O objetivo final deste exercício será:

- Criar uma tabela de simulação a uma variável;
- Criar uma simulação a duas variáveis;
- Aplicar os conhecimentos adquiridos na execução de um exercício prático;
- Criar uma previsão de resultados (cenários) através de *What-If Analysis*;
- Analisar os processos e criar gráficos dinâmicos que validem os resultados.

Parte I – Simulação a uma e a duas variáveis

Para criar uma tabela de simulação, deve o leitor seguir as instruções seguintes que permitem compreender o que se pretende. Podem existir outras abordagens possíveis e aplicação prática.

Exercício 4 – Simulação a uma variável

Criar um conjunto dados que simule preços de venda do "Artigo Lx-122", por alteração das margens de lucro para os valores de 5%, 10%, 15% e 20%.

	A	B	C	D
34				
35		Simulação por alteração da % lucro		
36		Artigo Lx-122	Margem	Preço venda
37			5%	21,68 €
38			10%	22,72 €
39			15%	23,75 €
40			20%	24,78 €
41				

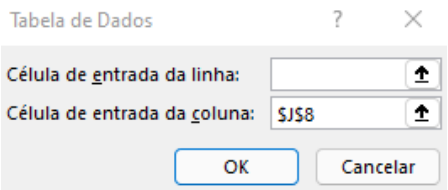
Quadro 7 – Simulação a uma Variável

O preço final de cada artigo depende da margem de lucro definida. Poderá ser eventualmente útil avaliar o impacto da alteração do valor dessa margem no preço final de um determinado artigo. O leitor deve construir por sua iniciativa, baseado no Quadro 7 e em Excel, a partir da célula B35, as diferentes percentagens de lucro possíveis de acordo com o exemplo. Os valores para os preços serão objeto de cálculo.

Em seguida, posicionar o cursor na célula D37 e inserir a fórmula para o cálculo do preço de venda para o Artigo Lx-122. Dá-se como exemplo:

```
D37 = E11 + E11 * J8          'Resultado: 21,68 €
```

Devolve a margem de lucro calculada de 5%, conteúdo da célula J8, sobre o preço de custo.



Exercício 5. Simulação a uma variável – Metodologia(s) a Implementar

Para simular os preços de venda, de acordo com as diferentes margens de lucro, selecionar a área C37:D40 do Quadro 7 escolher a opção "Análise de Hipóteses/Tabela de Dados [*What-If Analysis/Data Table*] do agrupamento "Previsão" do Separador Dados [*Data*]. Surge a seguinte caixa de diálogo:

Os valores estão dispostos sob a forma de coluna, pelo que unicamente se deve preencher o segundo parâmetro correspondente à "Célula de entrada da coluna" como mostra a caixa de diálogo anterior.

Exercício 6. Simulação a duas variáveis

Criar um conjunto de dados que simule preços de venda do "Artigo Lx-122", por alteração das margens de lucro para os valores de 5%, 10% e 15% e do preço de custo para 20,65 €, 19,30 €, 21,10 € e 18,00 €.

Simulação por alteração da % lucro e preço custo				
Artigo Lx-122	21,68 €	5%	10%	15%
	20,65 €	21,68 €	22,72 €	23,75 €
	19,30 €	20,27 €	21,23 €	22,20 €
	21,10 €	22,16 €	23,21 €	24,27 €
	18,00 €	18,90 €	19,80 €	20,70 €

Quadro 8 – Simulação a duas Variáveis

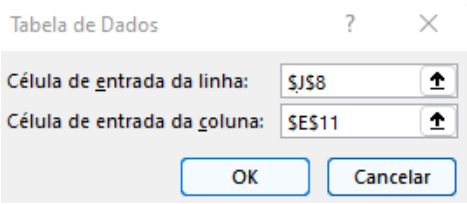
Para simular os diferentes preços de venda, ajustando os diferentes preços de custo e margens de lucro, é necessário construir uma nova simulação que está representada no Quadro 8.

Na primeira célula G36, deve-se calcular o preço de venda de acordo com os dados iniciais:

```
G36 = E11 + E11 * J8          'Resultado: 21,68 €
```

Sendo o resultado exatamente igual ao anterior agora é necessário prever os resultados por alteração da percentagem de lucro e também dos preços de custo.

Selecionar a área G36:J40 do Quadro 8 e escolher a opção "Análise de Hipóteses/Tabela de Dados [*What-If Analysis/Data Table*] do agrupamento "Previsão" do Separador Dados [*Data*]. Definir como variante de linhas, as margens de lucro, célula J8 e das colunas, os preços de custo, célula E11. Surge a seguinte caixa de diálogo:



Ao pressionar OK, automaticamente o conjunto de dados da simulação ficará completo.

Convém referir que os valores ficam agrupados e todos eles, contêm a fórmula {= TABLE(J8;E11)}, o que significa que nenhum poderá ser editado individualmente, ou seja, devem ser tratados como um todo.

Exercício 7. Simulação de Dados

Vamos agora aplicar os conhecimentos adquiridos na execução de um exercício prático.

Criar no Excel, um ficheiro que permita simular um empréstimo bancário. As condições iniciais definem um financiamento de 120.000 € para uma moradia avaliada em 150.120 € a pagar durante 30 anos sobre uma taxa de 5% ao ano num pagamento mensal de 644,19 €.

Efetuar uma simulação para determinar o valor mensal a pagar, por alteração do período de empréstimo para 25, 35 e 40 anos. Posteriormente pretende-se também avaliar o efeito no pagamento mensal por alteração do valor do financiamento para 100.000, 135.000 e 150.120 €.

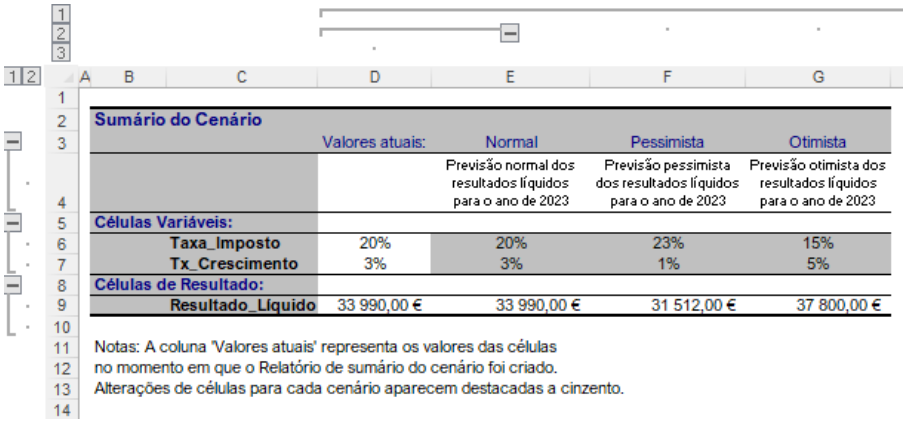
O leitor deve gravar o ficheiro com o nome "Exercicio_Parte_I".

Fim da Parte I

Parte II – Previsão de Resultados (Cenários)

Efetuar uma previsão dos resultados líquidos para o próximo ano de uma determinada empresa, com base nas taxas de imposto e crescimento previsíveis num cenário normal (taxa = 20% e crescimento = 4%) pessimista (taxa = 23% e crescimento = 1%) e otimista (taxa = 15 % e crescimento = 5%).

O resultado final pretendido é apresentado de seguida (Figura 15).



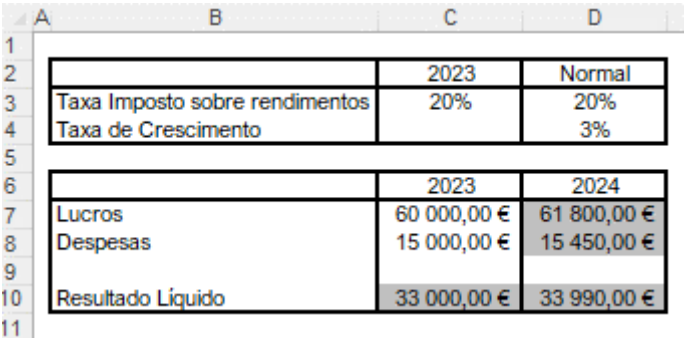
Sumário do Cenário	Valores atuais:	Normal	Pessimista	Otimista
		Previsão normal dos resultados líquidos para o ano de 2023	Previsão pessimista dos resultados líquidos para o ano de 2023	Previsão otimista dos resultados líquidos para o ano de 2023
Células Variáveis:				
Taxa_Imposto	20%	20%	23%	15%
Tx_Crescimento	3%	3%	1%	5%
Células de Resultado:				
Resultado_Líquido	33 990,00 €	33 990,00 €	31 512,00 €	37 800,00 €

Notas: A coluna 'Valores atuais' representa os valores das células no momento em que o Relatório de sumário do cenário foi criado. Alterações de células para cada cenário aparecem destacadas a cinzento.

Figura 15 – Sumário de um Gestor de Cenários

Para quem nunca tomou a iniciativa de fazer uma análise de dados ou tem pouca experiência no Excel, existem diferentes interpretações, razão pela qual é importante construir cenários.

Comecemos por definir uma nova folha de cálculo, criada com o nome "Cenários" com os seguintes quadros de previsões, taxa de imposto e crescimento:



	2023	Normal
Taxa Imposto sobre rendimentos	20%	20%
Taxa de Crescimento		3%

	2023	2024
Lucros	60 000,00 €	61 800,00 €
Despesas	15 000,00 €	15 450,00 €
Resultado Líquido	33 000,00 €	33 990,00 €

Figura 16 – Criação de um Cenário

Os valores das células a sombreado resultam da aplicação de fórmulas. Analisemos que no ano de 2023 a empresa declarou um lucro de 60.000,00 € e uma despesa de 15.000,00 €.

O cálculo do resultado líquido do ano de 2023 deve obedecer à fórmula:

Resultado Líquido = Lucros – (Lucros x Tx Imposto + Despesa)
C10 = C7 – (C7* C3 + C8) 'Resultado: 33.000,00 €

Num cenário normal para o ano de 2024, prevê-se que a taxa de imposto sobre os rendimentos se mantenha estável nos 20% e que se verifique um crescimento económico na ordem dos 3%.

Com base nesta informação obtém-se um eventual lucro para 2024 no valor de 61.800,00 € que resulta da multiplicação dos lucros obtidos no ano anterior pela taxa de crescimento previsível. Inserir na célula D7 a fórmula:

D7 = C7 + C7 * D4 'Resultado: 61.800,00 €

De acordo com o cenário esperado o valor das despesas será de 15.450,00 € que resulta da multiplicação das despesas do ano anterior, pela taxa de crescimento. Inserir na célula D8:

D8 = C8 + C8 * D4 'Resultado: 15.450,00 €

O resultado líquido neste cenário normal é de 33.990,00 €. Este valor é obtido na subtração dos lucros pelo valor da taxa de imposto sobre os rendimentos (D7 * D3) e pelo valor das despesas efetuadas, célula D8. Inserir na célula D10, a seguinte fórmula:

D10 = D7 – (D7 * D3 + D8) 'Resultado: 33.990,00 €

As fórmulas aplicadas permitiram o desenho de um cenário para os resultados líquidos a obter no ano seguinte, num limite de razoabilidade. Para criar os restantes cenários, pessimista e otimista, ver figura 17, devemos aceder à opção Análise de Hipóteses/Gestor de Cenários [*What-If Analysis/Scenario Manager*] do agrupamento "Previsão" do Separador Dados [*Data*].

Surge a seguinte caixa de diálogo (Figura 17):

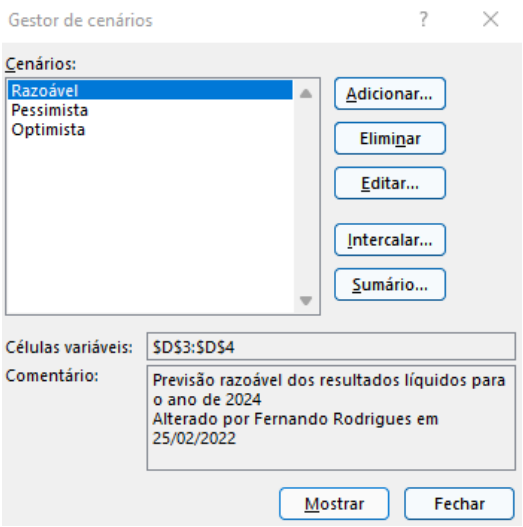


Figura 17 – Caixa de Diálogo (Gestor de Cenários)

Com o propósito de facilitar uma análise comparativa e apoiar a tomada de decisão, o passo seguinte é pressionar o botão Adicionar [*Add*] para criar os três cenários possíveis.

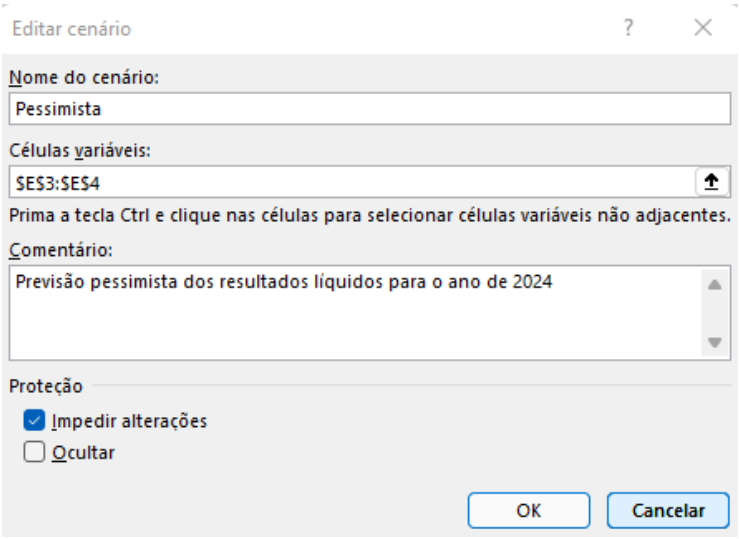


Figura 18 – Editar Cenário

Caso se pretendam alterar os valores e simular através das células variáveis a criação de cenários alternativos, pressionamos o botão Editar (Figura 18) e em seguida fazemos OK.

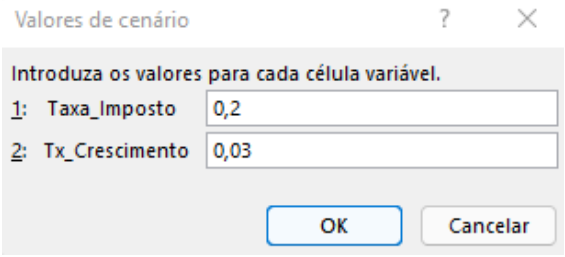


Figura 19 – Valores de Cenário

Os parâmetros da caixa de diálogo (Figura 19) surgem automaticamente preenchido com o valor das células D3 e D4. O Excel utiliza o endereço das células para a atribuição dos nomes.

Podemos alterar esse valor com o propósito de facilitar a compreensão dos cálculos e dos resultados. Por exemplo de acordo com a figura 20. é permitido alterar o nome das células D3, D4 e D10 para "Taxa_Imposto", "Tx_Crescimento" ou "Resultado_Liquido". Para isto acontecer, devemos ativar o menu de contexto e selecionar a opção "Definir Nome [*Define Name*], selecionando o menu Inserir [*Insert*] e no sub-menu Nome [*Name*] a opção Definir [*Define*].

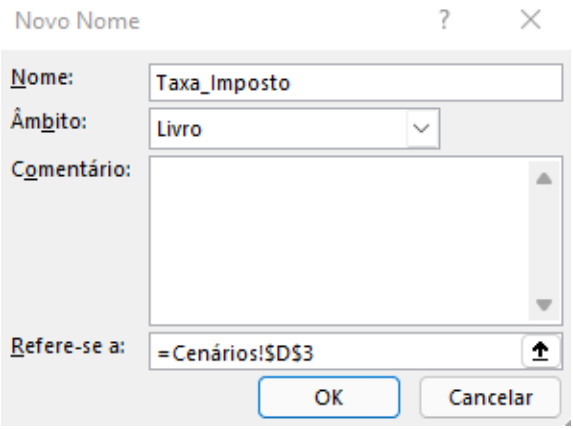


Figura 20 - Definir Novo Nome num Cenário

Dica: a alteração do nome das células pode também ser efetuada diretamente através das caixas de nomes da barra de fórmulas. Os nomes para as células não podem conter espaços!

Após termos os três cenários desenhados, escolher a opção Sumário [*Summary*] par emitir o relatório final. Deverá aparecer a figura 21.

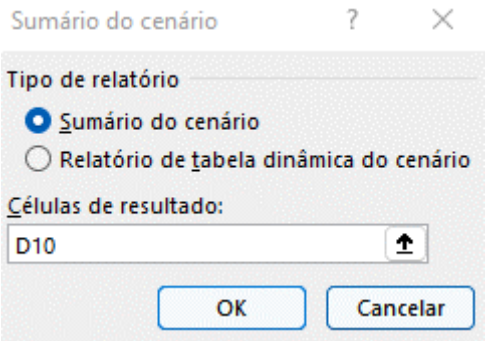


Figura 21 - Sumário do Cenário

Podemos sempre optar por criar Gráficos Dinâmicos [*Scenario Pivot Table Report*] que são úteis no cruzamento de dados. Após a conclusão do relatório do cenário é possível alterar as suas formatações e a visualização de dados.

Todas as formatações pré-definidas, tais como, cores, os alinhamentos, os limites, conteúdo do texto, de qualquer célula pertencente ao relatório, podem ser alteradas por decisão do leitor.

Gravar o Livro [*Workbook*] com todas as folhas geradas e atribuir-lhe um nome, por exemplo, "Processos_Auditoria".

Fim da Parte II

Entende-se que as simulações e processos de previsão tendo em vista resultados concretos para analisar informação recolhida, são o início de discussão com o Cliente, tendo em conta a complexidade que cada realidade com que as equipas de auditoria se confrontam.

No âmbito do Mestrado em Auditoria a frequência das aulas implica a resolução de exercícios mais complexos, como por exemplo, a prática de "Atingir Objetivo/*Goal Seek*" e problemas de otimização com recurso ao Solver.

Por manifesta falta de oportunidade e contexto atual os mesmos não serão apresentados. Fica desde já o leitor convidado a manifestar o seu interesse nesses exercícios, procurar inscrever-se em futuras edições dos cursos existentes no ISCAL e/ou dirigir ao autor pedidos de resposta através de correio eletrónico.

Parte II

Soluções Práticas Aplicadas a Auditoria

Módulo 5. Soluções Práticas Aplicadas a Auditoria

O objetivo deste módulo é que o leitor compreenda como se podem iniciar os trabalhos com um software específico para a atividade de auditoria.

É importante clarificar que não é propósito deste livro disseminar junto do mercado ou sequer publicitar de qualquer forma a empresa de software que estabeleceu um protocolo com o ISCAL para a livre utilização académica por parte dos alunos. Em contraponto, importa evidenciar a disponibilidade desde a primeira hora e apoio permanente que o autor teve junto da empresa, inclusive a manifestação de interesse de alunos em Portugal e Moçambique para desenvolverem as suas investigações com base nos conteúdos que a solução apresenta ao mercado.

É um módulo em constante evolução razão pela qual não será muito detalhado em termos de aprendizagem, conteúdos e explicação por parte do autor.

Figura 22 – Solução ASD Auditor

Tópicos gerais sobre a utilização do software

Abertura do Trabalho

– Aceitação do trabalho e respetiva documentação; Carregamento de dados (intercalares) a partir de um SAFT ou extratos; Criação automática das áreas de trabalho

Planeamento

– Avaliação de Riscos Distorção Material (Risco Inerente, Risco de Controlo, Risco Fraude); Avaliação de Risco de Revisão Analítica; Materialidade; Plano de Auditoria e Programas de Trabalho

Execução

– Seleção de amostra para testes detalhe e circularização; Provas analíticas substantivas; Análise de saldos e movimentos e registo dos erros identificados

Preliminares

– Importação do diário definitivo e impacto no trabalho desenvolvido; Recálculo da materialidade e impacto no planeamento; Revisão analítica final

Conclusão

– Recolha e tratamento dos ajustamentos de auditoria; Recolha de notas e incidências identificadas; Conclusões para relatório; Pasta final.

Funcionalidades do software

- ✓ Plano de Auditoria e criação dos riscos no trabalho de auditoria;
- ✓ Riscos distorção material (RDM) das demonstrações financeiras;
- ✓ Risco de Negócio + Risco de Controlo Interno;
- ✓ Existe um livro azul que OROC traduziu – Normas Internacionais de Auditoria (IFAC US);
- ✓ A ISA 315 é a que tipifica os riscos (Páginas 285 até 342);
- ✓ Arquivo Geral completo com toda a documentação necessária para realizarem a vossa auditoria (modelos, questionários, minutas…);
- ✓ Papéis de Trabalho gerais com documentos de auditoria que podem ser usados
  (o próprio software já traz de base).

Amostragem para auditoria

- ✓ É impossível analisar todas (corremos um risco de 10%) as contas financeiras;
- ✓ Existem dois tipos de Materialidade: a Normal (Demonstrações Financeiras) e a de Execução (por exemplo, pegar na Normal e baixarmos a Materialidade global para muito ou pouco);
- ✓ Calcular o "Intervalo de Amostragem" (trata-se de uma fórmula que apura a materialidade de execução a dividir pelo coeficiente da tabela estatística (U.M.);
- ✓ Documentos e Contas (existem dois tipos de circularização);
- ✓ Explorar as potentes ferramentas de revisão analítica: tipologias de lançamentos, antiguidade de saldos, correspondências fiscais, evolução mensal e anual, entre outras.

Página de Entrada

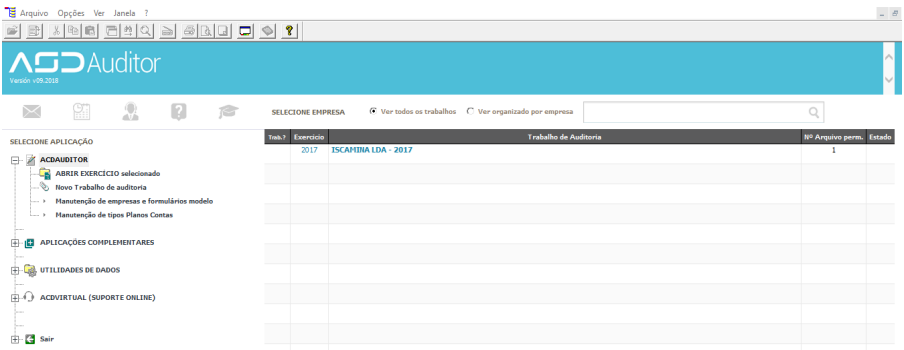


Figura 23 – Página Entrada ASD Auditor

Exemplo de uma empresa XYZ, Lda

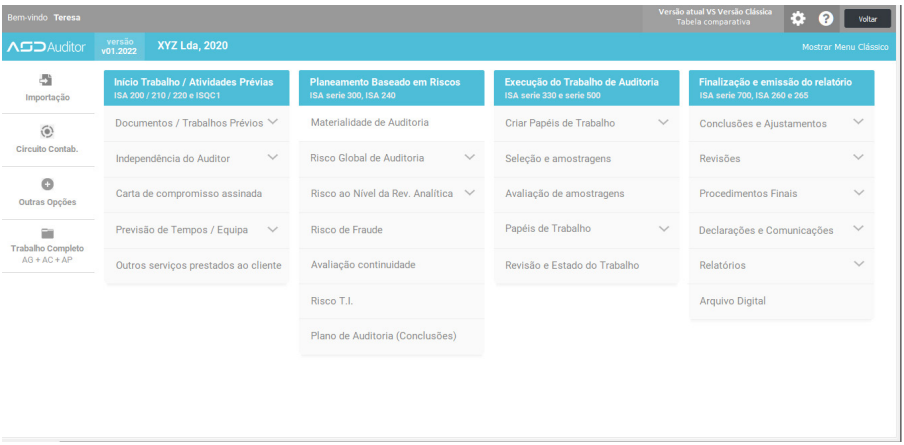


Figura 24 – Exemplo Empresa

Exemplo do Menu de Ajuda

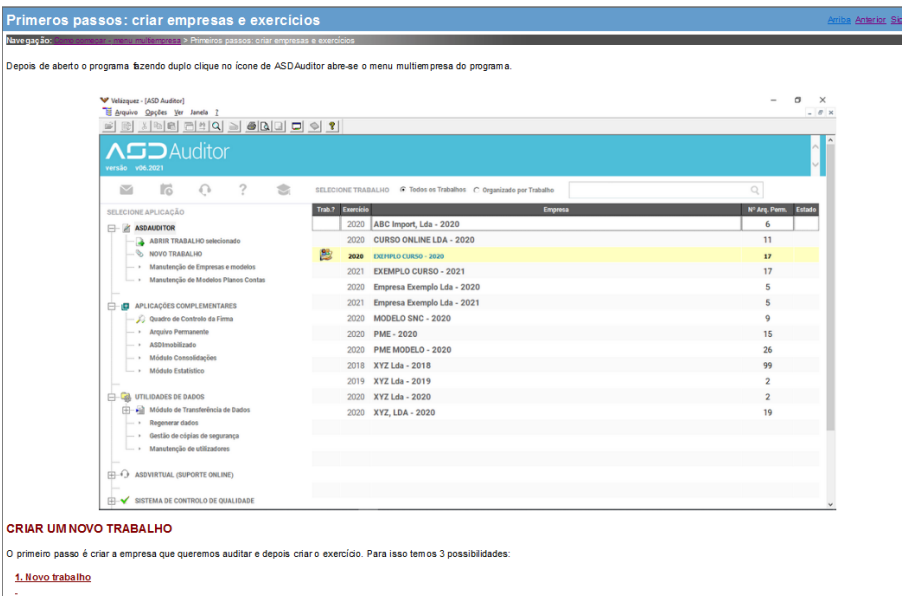


Figura 25 – Exemplo Menu Ajuda

Abertura do Trabalho

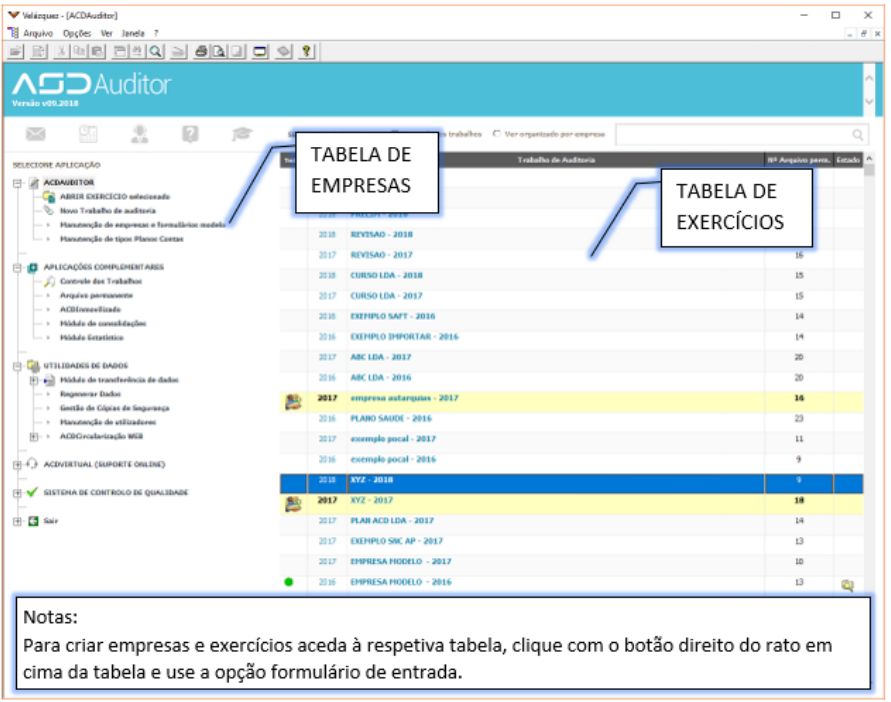


Figura 26 – Abertura do Trabalho

Reiterando que não é propósito deste livro publicitar de alguma forma empresas de software, clarificamos que a Ordem dos Revisores Oficiais de Contas (OROC) divulga três softwares de auditoria:

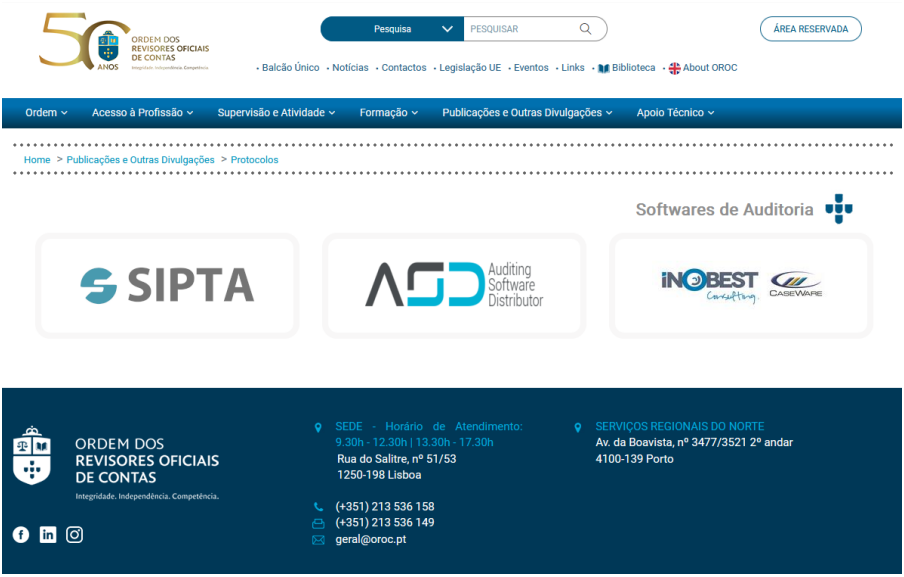


Figura 27 – OROC Divulga Softwares Auditoria

Tendo o ISCAL um Protocolo assinado com a empresa SIPTA a divulgação desta alternativa em detrimento de outras não é exaustiva. Porém, por razões concorrenciais, apresentamos esta solução tal como a OROC igualmente a promove.

O SIPTA é um software desenvolvido e comercializado em Portugal, pela empresa WIS4 – Web Integrated Systems, Lda. e em países de língua oficial portuguesa.

O ACD é um software desenvolvido em Espanha, comercializado pela empresa ASD – Auditing Software Distributor em Portugal.

O Caseware é um software desenvolvido no Canadá, comercializado pela empresa INOBEST Consulting em Portugal.

O SIPTA sendo um produto nacional e que se encontra em constante evolução, poderá vir a ser em breve disponibilizado igualmente em termos de aprendizagem, pelo que se apresentam em seguida alguns conteúdos e uma explicação por parte do autor.

Quanto ao Caseware não existiu por parte do distribuidor qualquer contacto ou manifestação de interesse em incluir informação para fins académicos.

Figura 28 – Página Entrada SIPTA

O **SIPTA** – Sistema Informático de Papéis de Trabalho de Auditoria – é um software que funciona online, que integra diversas ferramentas e técnicas de auditoria, permitindo um trabalho colaborativo das equipas, independentemente do seu local, computador ou dispositivo móvel.

Sendo uma ferramenta intuitiva, responde aos normativos internacionais de auditoria, e permite adaptar-se à organização de auditoria (nacional ou internacional), dado que pode ser estruturada e adaptada a diversas realidades.

Funcionalidades principais SIPTA e integradas na solução:

- ONLINE E INTEGRADO
- TODAS AS ETAPAS DA AUDITORIA
- MAPAS DE TRABALHO AUTOMÁTICOS
- AMOSTRAGEM
- APP SIPTA MOBILE
- PLATAFORMA DE CIRCULARIZAÇÃO
- GESTÃO DA QUALIDADE (ISQM)
- DF'S E RÁCIOS AUTOMÁTICOS
- AUTORIDADE TRIBUTÁRIA
- INTERAÇÃO COM A ENTIDADE AUDITADA

Exemplo de menu de evolução dos trabalhos do SIPTA, por etapa e fase de auditoria:

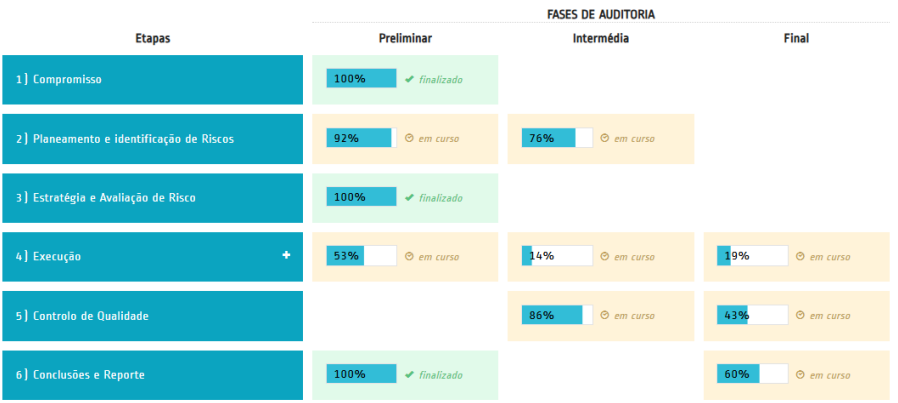


Figura 29 – Menu Evolução Trabalhos

Exemplo de um formulário do SIPTA de mapas de trabalho:

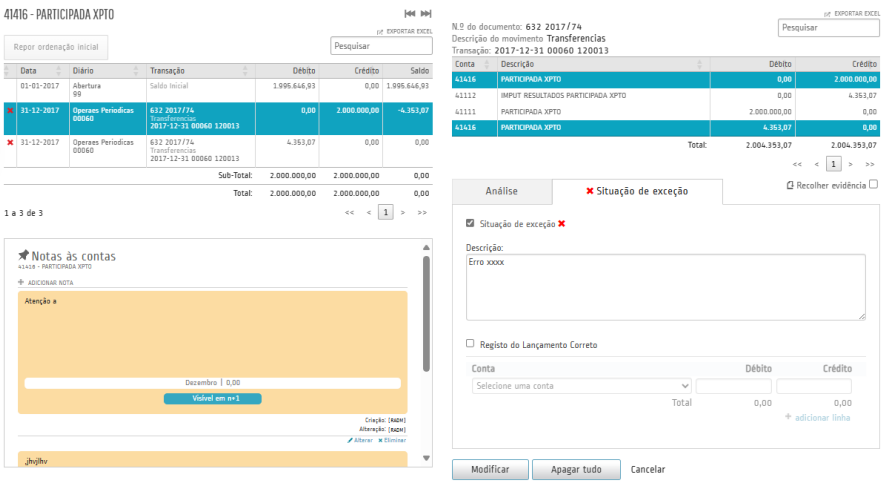


Figura 30 – Formulário SIPTA

Exemplo do SIPTA de validação das Demonstrações Financeiras:

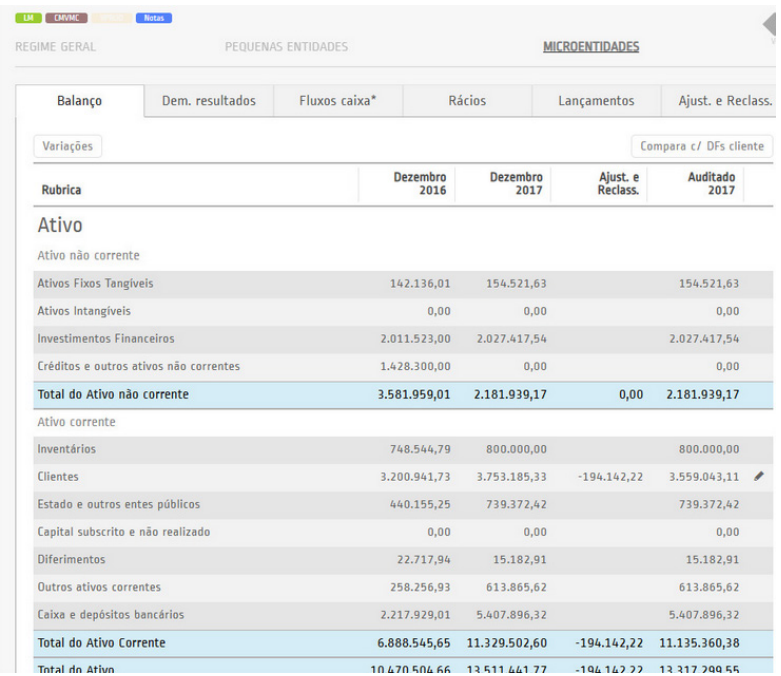


Figura 31 – Validação Demonstrações Financeiras

Figura 32 - Solução SIPTA

Em futuras edições, em resultado da colaboração com as empresas e ainda no pressuposto do contexto atual permitir dar continuidade ao trabalho que o autor tem desenvolvido, tendo em vista a investigação, maior apoio e reconhecimento na produção científica que tem sido realizada, poderá o autor vir a aprofundar novos conteúdos deste módulo.

Por limitações diversas, respeitando-se a garantia da representatividade de diferentes soluções existentes no mercado (e não apenas as que estão referenciadas no presente módulo), dando a oportunidade para evitar estereótipos e preconceitos ao serem abordados conteúdos sobre marcas e empresas, o autor disponibiliza-se para oferecer oportunidades de participação e colaboração de outras alternativas, promovendo a diversidade de perspetivas e experiências.

A adoção de boas práticas, linguagem inclusiva e acessível para todos os leitores é o desígnio deste livro, sendo possível criar no futuro ambientes concorrenciais para os mesmos objetivos.

Se for esta a resposta que a comunidade académica exigir cá estaremos para cumprir.

Referências Bibliográficas

Agostinho, P. (2019). *A auditoria interna no desenvolvimento da indústria 4.0 em Portugal*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/handle/10400.21/12171

Almeida, B. (2022). *Manual de auditoria financeira: Uma análise integrada baseada no risco* (4.ª Edição revista e atualizada). Lisboa: Escolar Editora. **ISBN: 978-972-592-593-5**

Alves, J. (2015). *Princípios e prática de auditoria e revisão de contas*. Lisboa: Edições Sílabo. **ISBN: 978-972-618-821-6**

Amaral, L. & Varajão. J. (2007). *Planeamento de Sistemas de Informação (4.ª Edição atualizada e aumentada)*. Lisboa: FCA Editora. **ISBN: 978-972-722-579-8**

António, P. (2015). *Informática e tecnologias da informação*. Lisboa: Edições Sílabo. **ISBN: 978-972-618-784-4**

Antunes, L. (2019). *Tecnologia blockchain e criptomoedas*. Lisboa: Plátano Editora. **ISBN: 978-989-760-227-6**

Antunes. M. & Rodrigues, B. (2018). *Introdução à Cibersegurança – A internet, os aspetos legais e a análise digital forense*. Lisboa: FCA Editora. **ISBN: 978-972-722-861-4**

Arens, A. *et al*. (2023). *Auditing and Assurance Services (18th Edition)*. Michigan State University & North Carolina State University, USA: Pearson Education Limited. **ISBN: 978-129-244-898-5**

Attie, W. (2018). *Auditoria – Conceitos e aplicações* (7.ª Ed.). São Paulo, Brasil: Editora Atlas. **ISBN: 978-859-701-710-6**

Aziz, O. (2019). *Auditoria aos Sistemas de Informação com base no Control Objectives for Information and Related Technology (COBIT)*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/handle/10400.21/14775

Barcelos, H. & Rodrigues, F. (2024). *Módulos Automatizados em Software de Auditoria para Procedimentos Analíticos*. In: XXIIIGrudisDC2024. Universidade de Aveiro (ISCA), Portugal, Fevereiro 2-3, 2024. Ver programa da conferência <<aqui>>.

Bashir, I. (2020). *Mastering blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more* (*3rd Edition*). Birmingham, UK: Packt Publishing. **ISBN: 976-183-921-319-9**

Bonyuet, D. (2020). *Overview and impact of blockchain on auditing*. *The International Journal of Digital Accounting Research*, 20, 31-43. Oklahoma State University, USA. Disponível em: http://www.uhu.es/ijdar/10.4192/1577--8517-v20_2.pdf. **DOI: 10.4192/1577-8517-v20_2**

Borralho, C. (2023). *Sistemas de planeamento e controlo de gestão*. (2.ª Edição revista e atualizada). Lisboa: Edições Sílabo. **ISBN: 978-989-561-274-1**

Bruno, D. (2021). *Auditoria de Planos de Continuidade de Negócio no âmbito dos Sistemas de Informação*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https:// repositorio.ipl.pt/handle/10400.21/13267

Bruno, D., Costa M., & Rodrigues, F. (2020). *Auditoria a Planos de Continuidade de Negócio*. In: Bastos, M. A., Marques, R. P., Peguinho, C., & Caçador, S. (eds.). *Proceedings of the 1st International Conference in Accounting and Finance Innovation: business innovation and digital transformation*, Universidade de Aveiro, Portugal, November 12-13, 2020. pp. 83-93. **ISBN: 978-972-789-665-3. DOI: 10.34624/1r78-9p55**.

Cangemi, M. & Brennan, G. (2019). *Blockchain Auditing – Accelerating the Need For Automated Audits! Journal EDPACS, The EDP Audit, Control, and Security Newsletter*, *5*, 1-11. London, UK. Disponível em https://www.tandfonline.com/doi/full/10.1080/07366981.2019.1615176. **DOI: 10.1080/07366981.2019.1615176**

Carvalho, L., *et al*. (2021). *Gestão das organizações – Uma abordagem integrada e prospetiva (4.ª Ed.)*. Lisboa: Edições Sílabo. **ISBN: 978-989-561-316-8**

Coderre, D. (2009). *Computer-Aided Fraud Prevention and Detection: A step--by-step guide (1st Edition)*. University of South Florida, USA: John Wiley & Sons. **ISBN: 978-047-039-243-0**

Collings, S. (2011). *Interpretation and Application of International Standards on Auditing*. Manchester, UK: John Wiley & Sons. **ISBN: 978-047-066-112-3**

Costa, C. (2023). *Auditoria financeira – Teoria e prática (13.ª Ed.)*. Lisboa: Editora Rei dos Livros. **ISBN: 978-989-565-081-1**

Costa, M. (2021). *Auditoria a Processos e Sistemas: um Mapa do Percurso do Cliente*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/ handle/10400.21/13266

Costa M., Bruno, D., & Rodrigues, F. (2020). *Auditoria a Processos e Sistemas: Um Mapa do Percurso do Cliente*. In: Bastos, M. A., Marques, R. P., Peguinho, C., & Caçador, S. (eds.). *Proceedings of the 1st International Conference in Accounting and Finance Innovation: business innovation and digital*

transformation, Universidade de Aveiro, Portugal, November 12-13, 2020. pp. 121-133. ISBN: 978-972-789-665-3. **DOI: 10.34624/1r78-9p55**

Dutta, S. (2013). *Statistical Techniques for Forensic Accounting: Understanding the Theory and Application of Data Analysis*. New Jersey, USA: Pearson Education Limited. **ISBN: 978-013-313-381-3**

Freire, J. (2021). *Blockchain e smart contracts – Implicações jurídicas*. Lisboa: Almedina. **ISBN: 978-972-409-688-9**

Guy, D. *et al*. (2002). *Auditing Sampling – An Introduction to statistical sampling in auditing (5th Edition)*. Manchester, UK: John Wiley & Sons, Inc. **ISBN: 978-047-137-590-6**

Helbig, J. (2022). *Da blockchain ao criptoinvestidor*. Lisboa: Editorial Presença. **ISBN: 978-972-236-825-4**

Henriques T. (2019). Gestão de sistemas de informação: Pessoas, equipas e mudança organizacional. Lisboa: FCA Editora. **ISBN: 978-972-722-903-1**

Imoniana, J. (2016). *Auditoria de sistemas de informação*. São Paulo, Brasil: Editora Atlas. **ISBN: 978-859-700-311-6**

Incozi, C. (2022). *A Problemática dos Sistemas de Informação na Contabilidade e Auditoria*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/handle/10400.21/14952

Incozi, C. & Rodrigues, F. (2021). *Understanding the role of Information Systems in Accounting*. In: ECMLG 2021. *Proceedings of the 17th European Conference on Management, Leadership and Governance*, Universidade de Malta, Malta, November 8-9, 2021. pp. 191-201. ISBN: 978-1-914587-20-7. **DOI: 10.34190/MLG.21.030**

Jelen, B. & Alexander, M. (2016). *Excel 2016 Pivot Table Data Crunching*. New Jersey, USA: Pearson Education, Limited. **ISBN: 978-078-975-629-9**

Laudon, K. & Laudon, J. (2021). *Management information systems: Managing the digital firm* (17.ª ed.). New York University, USA: Pearson. **ISBN: 978-013-697-154-2**

Machel, H. (2023). *Auditoria de Sistemas de Informação e Tecnologias Aplicadas: uma análise ao Sistema de Informação da Segurança Social de Moçambique (SISSMO)*. Dissertação de Mestrado, Instituto Superior Contabilidade e Auditoria de Moçambique (ISCAM), Maputo, Moçambique. Disponível em https://www.iscam.ac.mz

Martins, P. (2018). *Introdução à blockchain*. Lisboa: FCA Editora. **ISBN: 978-972-722-887-4**

Merkow, M., Breithaupt, J. (2005). *Computer Security Assurance – Using the Common Criteria*. New Jersey, USA: Thomson/Delmar Learning. **ISBN: 978-140-186-265-7**

Moreira, C. (2023). *Os Impactos do Blockchain na Auditoria*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/handle/10400.21/16100

Moreira, C., & Rodrigues, F. (2022). *Blockchain Impacts on Auditing*. In: Blockchain and Cryptocurrency Congress (B2C' 2022). *Proceedings in open access at:* https://b2c-conference.com/b2c_2022_proceedings.html. Barcelona, Spain, November 9-11, 2022. pp. 134-139. ISBN: **978-84-09-45763-2.**

Nigrini, M. (2012). *Benford's Law – Applications for Forensic Accounting Auditing and Fraud Detection*. New Jersey, USA: John Wiley & Sons. **ISBN: 978-111-815-285-0**

Nogueira, N. (2018). *Power BI para gestão e finanças*. Lisboa: FCA Editora. **ISBN: 978-972-722-895-9**

Pereira, J. (2022). *A nova tecnologia 5G e a cibersegurança – perceção dos impactos nas organizações e os desafios para os auditores*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/handle/10400.21/15439

Ramos, I., Sousa, R., & Quaresma, R. (2022). *Sistemas de informação: Diagnóstico e prospetivas*. Lisboa: Edições Sílabo. **ISBN: 978-989-561-212-3**

Rodrigues, F., Benedict, T., Kirchmer, M., & Scarsig, M. (2021). *BPM CBOK Version 4.0: Association of Business Process Management Professionals International* – ABPMP USA. **ISBN: 979-870-606-154-8**

Rodrigues, J. (2024). *Sistema de normalização contabilística: SNC explicado (9.ª Ed.)*. Porto: Porto Editora. **ISBN: 978-972-000-542-7**

Romney, M., *et al*. (2020). *Accounting Information Systems 15th Edition*. Brigham Young University & Arizona State University, USA: Pearson Education, Limited. **ISBN: 978-013-557-283-2**

Santos, V. (2018). *Criatividade em sistemas de informação*. Lisboa: FCA Editora. **ISBN: 978-972-722-891-1**

Silva, M. (2021). *A Auditoria e a Proteção de Dados dos Consumidores de Alojamento Local*. Dissertação de Mestrado, Instituto Superior Contabilidade e Administração de Lisboa. Lisboa: ISCAL. Disponível em https://repositorio.ipl.pt/handle/10400.21/13916

Taborda. D. (2021). *Auditoria – Revisão legal das contas e outras funções do revisor oficial de contas (3.ª Ed.)*. Lisboa: Edições Sílabo. **ISBN: 978-989-561-164-5**

Parte III

Glossário

Glossário

D

G

I

O

P

Sistemas de Informação e Auditoria

As organizações não existem sem dados e informação. Estes elementos combinados devidamente geram conhecimento, mas não sobrevivem sem Sistemas de Informação (SI) integrados e extensivos que permitam uma gestão adequada dos processos de negócio, subprocessos, atividades e tarefas.

Partindo do conhecimento gerado, a orientação ao Cliente é um imperativo do modelo de negócio, de modo a fornecer os produtos e serviços que estão disponíveis, pretensão essa que passa por um preço justo e enquadrado nas expectativas de cada um. A outra componente de sucesso são as pessoas que fazem parte da organização e a capacidade de envolvimento de todos na execução dos objetivos (estratégicos), designadamente, procurando assegurar as necessidades do Cliente.

A relação existente entre SI e os auditores traduz-se de uma forma idêntica a outras funções críticas e atividades interrelacionadas entre si em qualquer organização, pelo que os auditores devem avaliar os riscos associados aos SI e a correlação chave existente entre indicadores, atividades e iniciativas que devem estar ligadas com a estratégia (*core business*) da organização.

Que papel deve desempenhar o auditor no âmbito das auditorias a realizar aos SI? Que passos devem ser seguidos para formular recomendações de melhoria, em obediência ao princípio fundamental:

Que processos de "***Governance***" se aplicam aos SI?

A expressão *Corporate Governance* (boa governação) é uma expressão que as Equipas de Gestão já assumem há largos anos e têm a noção clara da importância da auditoria, tanto ao nível da estrutura de controlo interno, como ao nível do envolvimento em ações de maior risco negativo, com o propósito de potenciar a melhoria do desempenho da organização. Neste contexto, os princípios de boa governação sustentam em síntese, três aspetos essenciais para o sucesso da auditoria de SI:

a) A auditoria reporta ao mais alto nível (estratégico) da organização como bom exemplo de gestão;
b) A estrutura, o mandato e as funções da auditoria são claramente definidas em documento (digital) com divulgação a toda a organização, através dos seus canais tradicionais (internos e externos);
c) A auditoria obtém da Equipa de Gestão, a informação adequada para a realização das suas ações em concreto, a informação suficiente para a realização dos trabalhos a executar, a política de controlo interno implementada, a estratégia aprovada para proteção da informação, sistemas e tecnologias, bem como, quem tem acesso ao Plano Estratégico.

Existem ainda dois princípios fundamentais que as sociedades evoluídas e na vanguarda da maturidade orientadas a uma Gestão por Processos de Negócio procuram salvaguardar, centrando especial atenção aos seus Clientes, enquadradas nos SI e auditorias a realizar: o princípio ético e o princípio **democrático**.

O glossário seguinte de termos e expressões normalmente utilizados no controlo e avaliação de toda e qualquer organização é uma base de conhecimento (não exaustiva) de como o auditor deve interpretar o desafio de observar, analisar e julgar, emitindo um parecer que salvaguarde a realidade e a veracidade dos factos.

A

Abordagem sistémica
Abordagem de auditoria centrada na avaliação integrada das diversas atividades e operações que compõem um determinado sistema, concebidas para a realização harmónica de um mesmo objetivo final (Ver Auditoria de Sistemas).

Ação
Unidade básica de trabalho, destinada a obter evidência sobre situações concretas eleitas para análise, concorrendo para os objetivos do projeto em que se encontra inserida.

Acesso físico
No que diz respeito ao controlo do acesso a informação (automatizada e/ou digitalizada), o acesso físico procura relacionar-se com todos os dados/informações que são produzidas pelo processamento informático como, por exemplo, a apresentação gráfica num terminal/monitor ou uma cópia impressa.

Acesso lógico
Ato de poder aceder a dados informatizados e/ou digitalizados. Estes acessos podem ir desde um acesso de "apenas leitura" até a acessos mais abrangentes, que podem incluir a capacidade para alterar os dados, criar registos novos e apagar os registos existentes.

Acompanhamento
É uma das componentes do sistema de controlo interno. É um processo que permite apreciar a qualidade do funcionamento do sistema de controlo interno no decorrer do tempo. Em concreto, faz-se uma análise sistemática e avaliação, efetuada pelo auditor após determinado período de tempo. Envolve atividades, medidas e tarefas empreendidas pela entidade auditada na sequência das conclusões e recomendações incluídas no relatório de auditoria.

Atividades
Conjunto de tarefas interligadas de caráter sazonal, cíclico ou rotineiro que contribuem para a realização de, pelo menos, um objetivo, bem como, tendo em conta a especificidade do produto, possibilitem a identificação de resultados e dos respetivos meios a utilizar. Ou, mais simplesmente, um processo pelo qual uma organização converte os seus recursos (entradas) em saídas "*outputs*" (resultados/produtos).

Atividades de Controlo
As atividades de controlo interno relacionam-se com as políticas e os procedimentos definidos por uma organização para reduzir o nível de risco nas suas atividades e, consequentemente, alcançar os objetivos organizacionais. Essas atividades são a resposta da organização ao risco, na medida em que são concebidas com a intenção de reduzir o nível de incerteza que envolve sempre os objetivos e os resultados esperados.

Atividades de Financiamento
São as atividades que resultam de qualquer alteração ao nível do orçamento de uma organização, composição dos empréstimos realizados e do capital próprio de uma empresa.

Atividades de Investimento
Atividades que incluem não só a aquisição e alienação de imobilizações corpóreas e incorpóreas como também as aplicações financeiras que não se consideram como sendo equivalentes em caixa.

Atividades Operacionais
Estas atividades são o objeto das atividades da organização. Podem ser também todas as atividades que não sejam consideradas como atividades de investimento ou de financiamento.

Alocação de recursos humanos
Consiste na distribuição e afetação de pessoas a uma determinada tarefa.

Ambiente de aprendizagem
Ambiente interno da organização que se caracteriza pela importância que a aprendizagem assume na organização. A aquisição de competências, partilha de conhecimentos, troca de experiências e o diálogo sobre as melhores práticas são algumas das características deste ambiente.

Ambiente de controlo
É o componente base de todo o sistema de controlo interno, fundamentando todos os restantes componentes. Este ambiente proporciona a disciplina e a estrutura necessárias para a concretização dos objetivos básicos do sistema de controlo interno. O ambiente de controlo consiste na atitude demonstrada, pela Direção e pela Gestão de Topo de uma organização, relativamente às questões do controlo interno e à importância que lhes é atribuída. É constituído pelos seguintes elementos básicos:

- Integridade e valores éticos;
- Filosofia de gestão e estilo operacional;
- Estrutura organizacional;
- Atribuição de autoridade e responsabilidade;
- Políticas e práticas de recursos humanos;
- Competências.

Âmbito da auditoria
É um dos componentes da fase de planeamento e programação de uma auditoria, devendo a sua definição ser realizada após ter sido definido o campo da auditoria. O âmbito da auditoria pretende determinar, de forma clara e precisa, qual a amplitude e exaustão dos processos que serão necessários rever durante a sua realização. Inclui, igualmente, a limitação racional do volume de trabalhos a realizar de forma a reduzir o risco de auditoria para níveis aceitáveis. A finalidade determina o período temporal abrangido, os procedimentos e testes a efetuar face aos objetivos gerais e específicos da auditoria. Em SI releva-se uma modelação/mapeamento/fluxograma.

Amostra
Subconjunto de elementos pertencentes a uma população. É um conjunto de indivíduos (famílias ou outras organizações), acontecimentos ou outros objetos de estudo que o auditor pretende descrever ou para os quais pretende generalizar as suas conclusões ou resultados.

Amostra Representativa
Amostra cujas características são específicas da população (universo) de que provêm e cujos resultados dos testes podem ser extrapolados ao total dessa população.

Amostragem
Seleção de uma amostra em determinada população de acordo com o método apropriado e estudo dos elementos que a compõem com vista a emitir um parecer sobre o total dessa população.

Análise custo-benefício
Estudo da relação entre os custos e os benefícios de um programa, projeto ou ação, expressos numericamente. O seu objetivo é determinar se esses benefícios são superiores aos seus custos.

Análise do risco
É a análise genérica dos riscos que envolvem a atividade e operações de uma organização, a sua magnitude e a melhor forma de os gerir. Esta análise pode ser realizada em qualquer fase de uma atividade ou operação.

Cada análise tem como ponto de partida os resultados obtidos em análises anteriores. Deve ser sempre precedida pela elaboração de um Plano de Análise do Risco. Esta análise deve proporcionar toda a informação necessária à criação/inclusão de registo do risco, conceção de uma estratégia para mitigar os riscos e um plano de resposta a esses riscos. Os resultados desta análise devem ser sempre apresentados sob a forma de um relatório de análise do risco.

Análise multicritérios
Tipo de análise utilizado para facilitar a compreensão e a resolução de questões no processo de tomada de decisão. Permite formular juízos sobre as intervenções com base em critérios múltiplos, os quais podem não ter a mesma escala e possuir uma importância relativa diferente.

Análise swot
Análise dos pontos fortes, pontos fracos (ambiente interno) cruzada com as oportunidades potenciais e ameaças associadas a dificuldades (ambiente externo) de uma organização.

Apetite de risco
É a quantidade de risco aceite por uma organização no decorrer da concretização da sua missão, sem julgar necessário tomar qualquer tipo de medida relativamente à redução desse risco.

Aplicações informáticas
Programa ou conjunto de programas informáticos aplicados a um campo específico. Exemplos práticos: sistemas de remuneração, sistema de processamento dos reembolsos de IVA, sistema integrado de gestão (ERP), entre outros.

Apreciação do risco
É o processo através do qual é possível não só identificar os riscos relevantes para a concretização dos objetivos da organização como analisá-los e determinar qual a resposta adequada para reduzir esses riscos.

Aprendizagem
É o processo de aquisição e compreensão do conhecimento e da informação gerada a partir dos dados que pode levar à melhoria ou à mudança dos processos de negócio. Entre as técnicas, atividades e tarefas de aprendizagem organizacional podemos incluir o benchmarketing, as avaliações externas e internas e/ou as auditorias e estudos de boas práticas. Ao nível das atividades e tarefas de aprendizagem individual podemos incluir a formação e o desenvolvimento de competências.

Área de auditoria
A área de auditoria é definida após a análise conjunta do campo e do âmbito da auditoria. É ela que delimita de forma bastante precisa quais os temas da auditoria em função da organização a auditar e da natureza da auditoria.

Área de verificação
Área determinada pelo campo da auditoria e pelo seu âmbito quando considerados em conjunto. A área de verificação delimita de modo muito preciso os termos da auditoria, em função, por um lado, da entidade a auditar e, por outro, da natureza da auditoria preconizada.

Árvore de objetivos
É uma representação gráfica que permite proceder à classificação dos objetivos de um programa, projeto ou ação, através da sua hierarquização, associando a cada um dos objetivos específicos o respetivo objetivo global. A sua utilização clarifica substancialmente a lógica da intervenção.

É de grande utilidade fazer esta representação através de uma visão de alto nível com recurso a modelação/mapeamento/fluxograma.

Atributo
Conceptualmente, atributo é a propriedade essencial de uma substância. Ao nível da análise de funções, os atributos referem-se aos traços psicológicos ou às características pessoais de um indivíduo, determinados com base nas tarefas da função e que, sendo condição necessária, podem não ser os requisitos suficientes para que esse indivíduo apresente as competências comportamentais que determinam o sucesso.

Auditor
Pessoa competente e independente encarregada de realizar uma auditoria e de elaborar o respetivo relatório escrito (eventualmente) impresso. Em SI a entrega de documentos formais é realizada em formato digital.

Auditor Interno
É o responsável pela apreciação do sistema de controlo interno e que, através das suas avaliações e recomendações, contribui para o aumento da eficácia desse sistema. Apesar disso, ele nunca será responsável pela conceção, implementação, gestão e documentação do sistema de controlo interno da organização,

Auditoria
Processo sistemático que consiste no exame ou verificação objetiva das atividades e operações de uma organização. O objetivo desse exame é analisar a conformidade dessas atividades e operações em relação a determinadas regras e normas e aos objetivos definidos para essa organização. Deve ser realizada por uma pessoa idónea, tecnicamente preparada. A sua realização obedece a um conjunto de princípios, métodos e técnicas geralmente aceites, as quais permitem ao auditor formar uma opinião fundamentada e emitir um parecer acerca da matéria analisada. A auditoria permite identificar quaisquer tipos de desvios que possam vir a requerer uma ação corretiva e as suas conclusões e recomendações devem ser comunicadas a todos os detentores de interesse. No âmbito dos SI trata-se de um exame metodológico de um processo, atividade, tarefa, função, situação, programa ou sistema de uma determinada entidade. A conformidade do tratamento e gestão dos dados e informação gerados deve obedecer a regras, normas e procedimentos, tendo em vista exprimir uma opinião motivada sobre a globalidade do objeto de auditoria em que o resultado final é um relatório técnico especializado.

Auditoria Administrativa
Auditoria cujo objeto de análise são, para além do plano da organização, os procedimentos e os documentos de suporte dos processos para a tomada de decisão, que conduzem à autorização das operações por parte da Direção.

Auditoria Ambiente PED
Técnicas e métodos de auditoria a utilizar num ambiente informatizado que podem consistir no exame da organização de um determinado centro, serviço ou empresa com sistemas informatizados e/ou digitais, no exame do sistema de controlo interno existente nas aplicações informáticas ou na simples utilização de instrumentos informáticos que permitem efetuar trabalhos de auditoria diretamente sobre suportes magnéticos com ajuda de computador.
Auditoria Articulada
Forma de implementação coordenada das auditorias internas e/ou externas, nas situações em que as responsabilidades estejam sobrepostas. Essa coordenação é feita por intermédio da comunicação recíproca da calendarização e dos resultados, assim como da utilização comum de meios, com o objetivo de utilizar eficientemente os recursos que estejam à disposição da auditoria.

Auditoria Contabilística
Auditoria relativa ao plano da organização, aos procedimentos e documentos referentes à salvaguarda dos ativos e à fidedignidade das contas.
Esta auditoria é, consequentemente, concebida com a finalidade de fornecer uma garantia razoável de que:
a) as operações e o acesso aos ativos se efetuem em conformidade com as autorizações;
b) as operações sejam registadas quando necessário;
c) a contabilização dos ativos seja comparada com a existência física a intervalos razoáveis e que sejam tomadas as medidas adequadas relativamente a todas as diferenças não justificadas.

Auditoria Conformidade
Consiste na verificação do cumprimento, por parte organização auditada, das condições, regras e regulamentos de diversas origens, tanto externos como internos. De uma forma geral, os resultados deste tipo de auditoria são comunicados à autoridade que esteve na origem dessas condições, regras e regulamentos.

Auditoria Contas
Ver Auditoria Financeira.

Auditoria Demonstrações Financeiras
Consiste no exame das demonstrações financeiras, através do qual se pretende emitir uma opinião acerca da sua conformidade, ou não, relativamente a critérios pré-estabelecidos, aos princípios contabilísticos geralmente aceites e às normas de contabilidade.
Auditoria Desempenho / Gestão (*Performance Audit*)
É a apreciação e avaliação do desempenho global de uma organização e dos seus gestores. É o controlo de uma determinada entidade, programa, serviço, sistema ou área funcional, que incide na sua gestão, nomeadamente na utilização dos respetivos recursos que lhe foram confiados, segundo princípios, entre outros, de economia, eficiência e eficácia.
Embora conceptualmente próxima da avaliação, com a qual partilha o objetivo de melhoria dos serviços ou programas, está mais fortemente preocupada com questões da boa gestão, enquanto a avaliação vai mais longe e se preocupa sobretudo com os resultados obtidos e os impactos gerados, bem como, com questões como a relevância, pertinência ou sustentabilidade das intervenções públicas. Também conhecida por ser uma auditoria do "valor do dinheiro" ou da "economia, eficiência e eficácia" pela qual se procura analisar a forma como a entidade auditada observa as normas legais e regulamentares, utilizando os seus recursos no desempenho das suas atribuições.

Auditoria Estratégica
Auditoria que consiste em verificar se as decisões tomadas pela organização são consistentes com as políticas estratégicas previamente definidas.

Auditoria Externa

É toda a auditoria que é realizada por um organismo ou organização externa e independente em relação à organização auditada. O seu objetivo é, através da redação dos relatórios correspondentes, emitir um parecer sobre as contas e as declarações financeiras, a regularidade e legalidade das operações e a gestão financeira da organização a auditar. No âmbito dos SI a equipa técnica é altamente especializada em tecnologias de informação, segurança informática, privacidade dos dados, acessos remotos, entre outros.

Auditoria Financeira

Consiste na análise, efetuada por um auditor das contas, situação financeira e da legalidade e regularidade das operações de uma organização. Após concluída essa análise o auditor poderá, ou não, emitir um parecer. Desta forma, neste tipo de auditoria pode incluir-se a:

1) Análise das contas e da situação financeira da entidade fiscalizada, com vista a verificar se:
   a) Todas as operações foram corretamente liquidadas, ordenadas, pagas e registadas;
   b) Foram tomadas todas as medidas apropriadas com vista a registar com exatidão e a proteger todos os ativos, por exemplo: disponibilidades; investimentos; imobilizados; existências.

2) Análise da legalidade e regularidade com vista a verificar se:
   a) Todas as operações registadas estão em conformidade com a legislação geral e específica em vigor;
   b) Todas as despesas e receitas são, respetivamente, efetuadas e arrecadadas com observância dos limites financeiros e dos períodos autorizados;
   c) Todos os direitos e obrigações são apurados e geridos segundo as normas aplicáveis.

Auditoria Financeira relacionada

Visa determinar: se os relatórios financeiros regulares ou especiais e os itens relacionados, tais como, cálculos, declarações de gastos, fundos, dados financeiros relativos à execução de programas ou projetos, estão razoavelmente de acordo com critérios estabelecidos ou declarados; e se a entidade aderiu aos requisitos financeiros específicos determinados.

Auditoria Fiscal
Auditoria realizada por uma pessoa competente às contas, operações financeiras e ao sistema de controlo interno financeiro de uma pessoa coletiva ou singular, tendo em vista verificar o cumprimento das respetivas obrigações contabilísticas e fiscais e de proceder à qualificação jurídico-tributária dos factos e operações fiscalmente relevantes para efeitos da determinação do lucro tributável em determinado(s) exercício(s).

Auditoria Fonte Contratual
Esta auditoria possui um carácter facultativo e tem origem num determinado contrato de prestação de serviços.
Auditoria Fonte Legal
Auditoria que tem origem num normativo legal específico possuindo um cariz obrigatório.

Auditoria Geral
Auditoria à totalidade da organização e as suas operações.

Auditoria Gestão
Auditoria dirigida à avaliação da regularidade, eficácia e eficiência de todos os níveis que compõem o ciclo de gestão (planeamento estratégico, programação, execução, supervisão e avaliação dos resultados).

Auditoria Horizontal
É uma auditoria temática específica que se realiza simultaneamente junto de várias organizações ou serviços como, por exemplo, a auditoria informática.

Auditoria Informação Histórica
Este tipo de auditoria tem como objeto o conjunto de informação histórica, cuja análise é realizada, sempre, *a posteriori*.

Auditoria Informação Previsional ou Prospetiva
O conjunto da informação previsional ou prospetiva da organização é o objeto deste tipo de auditoria, sempre realizada *a priori*. Este tipo de auditoria baseia-se em técnicas de avaliação da validade das previsões.

Auditoria Informática
Auditoria de dados registados em suporte informático, incluindo a avaliação do próprio sistema informático: aplicações, sistema de gestão, programas, aplicativos, entre outros suportes físicos e lógicos.

Auditoria Integrada
É uma auditoria realizada numa perspetiva de conjunto, incluindo simultaneamente a auditoria financeira, a auditoria desempenho e a auditoria operacional ou de resultados. Em SI é um exame que fornece uma visão independente, objetiva e construtiva na forma como os recursos físicos, lógicos e tecnológicos são geridos com vista à sua economia, eficiência e eficácia, se as relações de perfis e responsabilidades definidas estão de acordo com os padrões de segurança informática.

Auditoria Interna
Atividade independente, de avaliação objetiva e de consultoria com o objetivo de acrescentar valor e melhorar as operações de uma organização. Pretende auxiliar a organização na concretização dos seus objetivos, através de uma abordagem sistemática e disciplinada, na avaliação da eficácia da gestão de risco, controlo e dos processos de negócio baseados no modelo de governação/gestão executiva. É uma função contínua, completa e independente, desenvolvida na entidade, por pessoal desta ou não, baseada na avaliação do risco, que verifica a existência, o cumprimento, a eficácia e a otimização dos controlos internos e dos processos existentes, ajudando a entidade no cumprimento dos seus objetivos.
Em termos práticos existe um serviço ou departamento interno incumbido pela Direção de efetuar verificações e avaliar os sistemas e procedimentos da entidade com vista a minimizar as probabilidades de fraudes, erros ou práticas ineficazes. A auditoria interna deve ser independente no seio da organização e reportar diretamente à Direção. Utiliza recursos de acordo com o meio funcional pelo qual os gestores de uma entidade são assegurados, a partir de fontes internas ajudando a criar processos pelos quais eles são responsabilizados, operando numa forma que irá minimizar a probabilidade de ocorrência de fraude, erro ou práticas ineficientes ou não economicamente ajustadas.

Possui muitas das características da auditoria externa, mas pode desempenhar apropriadamente as diretivas do nível de gestão ao qual reporta. Reúne um conjunto de atividades que permitem garantir através de um envolvimento independente e objetivo, acrescentar valor e melhorar as operações de negócio numa organização. Ajuda a alcançar os seus objetivos alinhados com a estratégia definida, através de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia da gestão de risco, através dos processos de controlo e governação.
A auditoria interna é uma atividade de apreciação estabelecida numa entidade, tal como um serviço prestado para a própria entidade. As suas funções incluem, entre outras, examinar e avaliar a adequação e eficácia dos sistemas de contabilidade e de controlo interno e fazer o respetivo acompanhamento. Quer seja realizada num departamento, divisão ou equipa, os consultores ou outros profissionais que prestem serviços de consultoria, fazem-nos de forma independente e objetiva, destinados a acrescentar valor e a garantir o bom desempenho das operações da organização. A atividade de auditoria interna auxilia a organização a cumprir a estratégia suportada pelos seus objetivos, adota uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos seus processos de negócio, avalia a gestão do risco, o controlo e o modelo de governação existente.

Auditoria Ocasional
Como o próprio nome indica, é toda a auditoria que é realizada de forma esporádica e não programada, após ter sido feita uma solicitação pontual para a sua realização.

Auditoria Operacional
Consiste na análise e avaliação sistemática das áreas operacionais de uma organização. O seu objetivo é verificar se as atividades e/ou operações dessa organização respeitam os princípios da economia, eficiência e eficácia. Aplica-se a todas as fases: programação, execução e supervisão. Em termos de SI e num âmbito dos processos de negócio que são representados numa visão de alto nível, através de técnicas que envolvem modelação/mapeamento/fluxograma. Associada regularmente a auditoria de desempenho.

Auditoria Orientada
Este tipo de auditoria caracteriza-se por analisar especificamente um determinado setor, área, atividade ou tipo de procedimento em concreto. Comporta fortes probabilidades de irregularidades ou fraudes.

Auditoria Parcial
Tipo de auditoria que incide apenas num setor de uma organização, podendo analisar uma determinada atividade, operação ou projeto. Em SI obriga a prioritizar o sistema que se audita por razões de segurança.

Auditoria Permanente
Como o próprio nome indica, a auditoria permanente caracteriza-se por ser realizada de forma regular, permitindo um acompanhamento continuado.

Auditoria Planeamento Estratégico
Consiste essencialmente na verificação do grau de concretização dos grandes objetivos organizacionais, especialmente os objetivos de longo prazo e se as políticas e estratégias estão a ser respeitadas ao nível da aquisição, utilização e alienação dos recursos da organização.

Auditoria Práticas de Gestão
Auditoria de todos os sistemas e métodos utilizados pelos gestores para poderem tomar decisões, garantir que estas são aplicadas e para apreciar em que medida os resultados esperados são ou não alcançados.

Auditoria Programas ou Projetos
O objetivo deste tipo de auditoria é proceder à apreciação/análise da execução de programas e projetos específicos. Esta auditoria pode dar origem, por sua vez, a auditorias horizontais.

Auditoria Regularidade/Legalidade
É um exame independente, realizado por uma pessoa competente a uma determinada situação, atividade, função ou sistema, tendo em vista verificar a conformidade do respetivo desempenho com a lei, princípios, regulamentos (bloco legal) e as instruções administrativas aplicáveis.

Auditoria Sistemas
Auditoria que analisa os sistemas, especialmente o sistema de controlo interno da organização auditada e que procura identificar os eventuais pontos fortes e/ou deficiências desse controlo interno. Permite, desta forma, definir o local, a natureza e o âmbito dos trabalhos de auditoria considerados necessários para formular um parecer.

Auditoria Tecnologias de Informação
Este tipo de auditoria incide na análise dos sistemas e ambiente informáticos de uma organização, compreende a segurança das suas informações e políticas, controlos organizacionais inerentes à área das Tecnologias de Informação da organização.

Auditoria Temática
Auditoria realizada junto de uma ou mais entidades/serviços que incide sobre determinadas situações de elevado grau de risco, dado comportarem fortes probabilidades de irregularidades ou fraudes.

Auto Avaliação de Controlo
É um processo que permite verificar e avaliar a eficácia do controlo interno. O seu objetivo é dar uma garantia razoável de que os objetivos da organização estão a ser cumpridos.

Auto Controlo
Ver Auditoria Interna.

Avaliação
Exame objetivo da evidência, cujo objetivo é facilitar a realização de uma avaliação independente dos processos em gestão de risco, do controlo interno e da governação/administração da organização. Podemos incluir neste tipo de exame os trabalhos de auditoria financeira, de desempenho, conformidade, segurança de sistemas e de "due diligence".

Avaliação da Qualidade da Auditoria
Esta avaliação consiste na apreciação independente da auditoria realizada. O seu objetivo fundamental é verificar se está conforme às normas em vigor, se as conclusões são fundamentadas e se os objetivos inicialmente definidos foram atingidos.

Avaliação de Programas
Revisão e avaliação periódica, independente e objetiva de um programa para determinar à luz das circunstâncias presentes, a adequação dos objetivos delineados e os seus resultados, tanto os pretendidos quanto os não pretendidos. As avaliações questionarão a real existência do programa e os seus resultados e impactos.

Avaliação de Políticas
Consiste em medir os efeitos gerados por uma determinada política e em averiguar se os meios jurídicos, administrativos e financeiros utilizados produziram os efeitos esperados.

Avaliação do Risco
Consiste no processo de identificação e análise dos eventos que possam vir a ter uma influência negativa na concretização dos objetivos organizacionais. Pretende-se estimar o impacto que esses riscos podem ter na organização, assim como a probabilidade de virem a ocorrer. Uma vez identificados, os riscos são quantificados e é preparada a resposta mais apropriada para reduzir o seu impacto e a sua probabilidade de ocorrência.

Avaliação do Risco da Informação
Avaliação que identificar e analisar as ameaças potenciais em relação à qualidade/quantidade de informação existente numa organização. Para além disso, pretende, igualmente, identificar as oportunidades que permitem assegurar a existência dos controlos adequados para que se possam minimizar os riscos nesta área.

Averiguações
Procedimento dirigido à obtenção dos elementos necessários à adequada qualificação de eventuais faltas ou irregularidades verificadas no funcionamento dos respetivos serviços.

B

Balanced Scorecard
É uma metodologia de gestão estratégica, disponível no mercado, desenvolvida em 1992 pelos professores da Harvard Business School, Robert Kaplan e David Norton. Os métodos usados na gestão do negócio, dos serviços e das infraestruturas, baseiam-se normalmente em metodologias consagradas que podem utilizar as TI e os softwares de ERP (*Enterprise Resource Planning* – Sistema Integrado de Gestão) como soluções de apoio, relacionando-a à gestão de serviços e garantia de resultados do negócio. Os passos desta metodologia incluem: definição da estratégia organizacional, gestão por processos de negócio, gestão de serviços e gestão da qualidade; os quais são implementados através de indicadores de desempenho. Em regra, a visualização da metodologia passa pela criação de um Mapa Estratégico que permite clarificar a missão, visão valores, vetores estratégicos, objetivos, indicadores e iniciativas, assim como, resumir todos os processos principais.

Esta metodologia baseia-se em quatro perspetivas que refletem a visão e estratégia organizacionais. São elas:

- Financeira;
- Clientes;
- Processos Internos;
- Aprendizagem e Crescimento.

Balanço
Relativo a serviços públicos de caixa, é um procedimento de auditoria financeira que visa o apuramento da responsabilidade financeira dos agentes responsáveis pelos serviços de tesouraria sujeitos à prestação de contas, fornecida por um exame independente expresso através de uma opinião sobre a contabilidade, existências, movimentos de entrada e saída de fundos e de valores ou outras informações financeiras da entidade auditada, realizado por um auditor/inspetor e de acordo com obrigações decorrentes de atribuições legais de controlo financeiro.

Benchmarking
Processo de comparação do desempenho entre várias organizações que permite a aprendizagem organizacional a partir das boas práticas constatadas e das lições aprendidas por outras organizações.

Boa Gestão Financeira
Avaliação que integra um dos objetivos da auditoria financeira (ou das finanças públicas) e que assenta nos exames a efetuar aos desempenhos da gestão financeira, em função da economicidade, eficiência e eficácia.

C

CAAT
Técnicas de auditoria assistida por computador.

Cadeia de valor
Cadeia constituída pelo conjunto de todas as atividades interrelacionadas, que são desenvolvidas por uma unidade económica, com o objetivo de alcançar os seus objetivos e resultados esperados. Estas atividades incluem todas as que se desenvolvem, desde as relações com os fornecedores até à apresentação do produto final. Cada elo dessa cadeia deve estar relacionado com o elo seguinte.

Caixa
Por caixa, entende-se o conjunto de numerário e de depósitos bancários que podem ser imediatamente mobilizados.

Campo da auditoria
O campo da auditoria define o objeto e o período de tempo que é necessário auditar. Além disso, define também a natureza da auditoria (por exemplo, se é uma auditoria de conformidade de determinadas operações realizadas no ano x). O objeto da auditoria pode incluir a organização no seu todo (um organismo público, uma empresa ou um projeto, entre outros) ou apenas um setor ou atividade nessa organização.

Carta de auditoria
Mais conhecida como a base de funcionamento da auditoria interna, definida e aprovada pelo seu Conselho de Administração. Complementarmente, o relatório de auditoria é a comunicação escrita dos factos comprovados que o auditor envia à entidade auditada, sem comprometer a instituição de auditoria como tal e que trata:

- dos resultados das verificações enquanto temos potenciais para conclusões posteriores; e/ou
- das deficiências de rotina evidenciadas por ocasião da auditoria, bem como, das recomendações no sentido de as corrigir.

Certificação das contas
Parecer profissional, elaborado por um auditor devidamente habilitado, sobre a forma, verdadeira e apropriada, como a situação financeira e os resultados das operações da organização auditada são apresentados em relação à data e ao período a que essas contas se reportam.

Ciclo de apreciação de risco
É um processo corrente e sistemático de identificação e análise das alterações verificadas nas condições, oportunidades e riscos de uma organização.

Procura, também, preparar e desencadear as ações necessárias para lidar com os riscos identificados, especialmente as ações que dizem respeito à alteração do sistema de controlo interno, como forma de lidar com o facto de os riscos estarem em constante mutação. Os perfis de risco e os controlos que lhes estão associados devem ser periodicamente revistos e reavaliados. Desta forma, pode haver a garantia de que esses perfis continuam válidos, isto é, que as respostas a esses riscos continuam orientadas de forma adequada e proporcional e que os controlos internos mitigadores estabelecidos continuam eficazes à medida que os riscos mudam com o passar do tempo.

Cidadão/Cliente/Utente
Expressão que pode englobar, simultaneamente, tanto os utilizadores diretos dos serviços públicos como todas as pessoas que, na qualidade de cidadãos e contribuintes, têm interesse nos serviços públicos e nos resultados alcançados por estes. Na área da Saúde designa-se Utente. A expressão Cliente é normal e regularmente usada pelas organizações privadas.

Circularização
Técnica que permite, através da obtenção de prova formal por parte de terceiros, confirmar as informações relativas a atos e factos da organização auditada.

Código de Ética
É um código que norteia a atividade da auditoria interna e foi elaborado e aprovado pelo Instituto de Auditores Internos (IIA). O objetivo principal é promover uma cultura de ética na atividade de auditoria interna a nível geral. Inclui todos os princípios fundamentais para a profissão e para a prática da auditoria interna. Além disso, inclui igualmente as regras de conduta que descrevem o comportamento que os auditores devem ter. O seu âmbito de aplicação inclui não só auditores individuais, mas também todas as entidades que prestam serviços de auditoria interna. Ver URL: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx.

***Common Assessment Framework* (CAF – Estrutura Comum de Avaliação)**
Modelo de autoavaliação do desempenho organizacional, especificamente desenvolvido para ajudar as organizações do sector público dos países europeus a aplicar as técnicas da Gestão pela Qualidade Total, melhorando o seu nível de desempenho e de prestação de serviços.

Competência
É o conhecimento, a capacidade e a experiência que os auditores devem ter e aplicar no desempenho da sua atividade.

Competência para assumir compromissos financeiros
É a responsabilidade atribuída a qualquer indivíduo ou conjunto de indivíduos para poder, isoladamente ou em conjunto, assumir compromissos financeiros em nome da sua Organização e perante terceiros.

Componentes do controlo interno
O controlo interno baseia-se em cinco grandes componentes que permitem que a organização possua não só um sistema de controlo interno eficaz, mas também, que possa ter a garantia de que os objetivos definidos podem ser alcançados.

Cada objetivo está interrelacionado com essas componentes, que são: ambiente de controlo, avaliação do risco, atividades de controlo, informação, comunicação e supervisão/acompanhamento. Estas componentes devem funcionar em profunda articulação, de forma a potenciar sinergias e possuir um carácter dinâmico que permita responder a qualquer tipo de alteração no contexto envolvente.

Comprovação de auditoria
Factos importantes evidenciados e relatados por escrito pelo auditor durante a sua auditoria, com vista a deles tirar conclusões.

Comprovação fundamental
A comprovação fundamental relaciona-se com todo e qualquer tipo de facto que tenha sido detetado relativamente às contas e situação financeira de uma organização e que põe em dúvida o seu valor. Pode significar que o auditor se encontra impossibilitado de chegar a conclusões satisfatórias e, no limite, que a certificação de contas pode ser recusada.

Comunicação
Consiste, essencialmente, na divulgação das conclusões da auditoria, realizada através de um relatório escrito com um determinado grau de confiança ou em modo de apresentação.

Conclusões de auditoria
As conclusões de auditoria exprimem, de forma sintética, a opinião do auditor relativamente ao objeto da auditoria realizada. Devem incluir o grau de autenticidade e fiabilidade de todos os elementos examinados. Todas as conclusões devem ser fundamentadas nas comprovações realizadas pelo auditor. Além disso, o auditor deve avaliar, também, o provável impacto que as deficiências detetadas podem ter, assim como os seus riscos e efeitos.

Conferir uma conta
Ato de verificar a exatidão de todas as operações de cariz contabilístico e financeiro lançadas numa determinada conta.

Confidencialidade
Os auditores devem respeitar o valor e a propriedade da informação recebida e não divulgar essa informação sem a devida autorização, a não ser que sejam obrigados legal ou profissionalmente a fazê-lo.

Conflito de interesses
Por conflito de interesses entende-se todas as situações em que exista um relacionamento que represente, ou aparente representar, algo contrário ao interesse público. A existência deste tipo de conflitos prejudica diretamente a capacidade de um indivíduo desempenhar os seus deveres e cumprir com as suas responsabilidades de forma isenta e objetiva.

Conformidade
A conformidade diz respeito à capacidade existente numa determinada Organização em assegurar, com um grau de garantia satisfatório que as suas atividades e operações respeitam e cumprem não só todas as leis, regulamentos e contratos que envolvem a atividade dessa organização, mas também, as políticas, planos e procedimentos organizacionais por ela definidos.

Conluio
Entendimento e união de esforços de cooperação entre dois ou mais indivíduos com a intenção de prejudicar, em proveito próprio, a organização de que fazem parte. Essa situação pode verificar-se ao nível de fraudes financeiras, de inventário ou outros bens.

Conselho/Comité de Auditoria
A função de um Conselho/Comité de Auditoria é auxiliar o dirigente máximo da organização a desempenhar as suas responsabilidades, nomeadamente no que diz respeito às políticas contabilísticas, ao controlo interno e à emissão de relatórios financeiros.

Constatação de auditoria
Uma constatação de auditoria é aquilo que o auditor verificou durante a auditoria e que irá servir de fundamento para as suas conclusões e recomendações.

Contabilidade Pública
Obrigação de todos os indivíduos ou organismos públicos, incluindo as empresas públicas às quais foram confiados dinheiros públicos, de responder de forma estruturada e normalizada pelas responsabilidades fiscais, gestionárias e de programas que lhes foram atribuídas e reportar àqueles que lhes atribuíram essas responsabilidades.

Controlo
O processo pelo qual se verifica se as atividades de uma organização estão de acordo com um plano de ação desejado e o plano está conforme com as atividades dessa mesma organização. É um processo que habilita o gestor a dirigir e monitorizar as suas atividades, abrangendo a estrutura de controlo, a qual inclui a sua componente ambiental: os sistemas financeiro-operacionais, as políticas, objetivos, planos e procedimentos; a delegação de autoridade para execução; o acompanhamento e avaliação contínuos a fim de identificar desvios do quadro traçado; e a ação corretiva para restaurar as operações de acordo com o previsto, quando necessário.

Controlo acessos
Conceito utilizado no domínio das TI que designa os controlos concebidos para proteger os recursos informáticos de uma organização relativamente a qualquer tipo de alteração não autorizada, perda ou revelação não pretendida.

Controlo adequado
Um controlo adequado implica necessariamente a existência dos planos e dos controlos necessários, preparados pela Direção, que garantam, de forma razoável, a existência de uma gestão eficaz dos riscos da organização e que os seus objetivos serão atingidos de forma económica, eficaz e eficiente.

Controlo compensatório
São os controlos que, de certa forma, compensam uma deficiência do sistema de controlo.
Por exemplo, quando o sistema de pagamento não possui os procedimentos de segurança necessários e suficientes para garantir que o vencimento é pago a todos os funcionários, os próprios funcionários funcionam como controlo compensatório, dado que podem reclamar o pagamento do seu vencimento sempre que isso ocorra, colmatando assim a deficiência original do sistema de pagamento.

Controlo cruzado
Controlo que abrange as operações, registos, documentos, entre outros, realizadas por mais do que uma entidade pública ou privada.

Controlo deteção
Controlo concebido para detetar a ocorrência de qualquer acontecimento ou resultado não pretendidos (contrasta com o controlo preventivo).

Controlo externo
Fiscalização realizada por um organismo externo, independente da entidade fiscalizada.

Controlo geral
Conjunto de políticas e procedimentos que incluem a totalidade ou apenas um setor considerável do SI de uma organização. Asseguram a operação contínua e adequada desses sistemas, proporcionando um ambiente adequado para a operação dos sistemas aplicacionais e de controlo. Nesses controlos, podem incluir-se os controlos sobre a gestão das TI, a sua infraestrutura, a gestão da segurança e a aquisição, desenvolvimento e manutenção do software. Estes controlos devem suportar o funcionamento de todos os controlos aplicacionais programados. Podem ser também designados como controlos informáticos gerais ou controlos de tecnologia de informação.

Controlo gestão
Processo que permite aos gestores da organização assegurar que os recursos são não só obtidos como também utilizados e que a organização implementa a sua estratégia, de forma eficaz e eficiente, na concretização dos seus objetivos.

Um controlo de gestão inclui:
(i) Lista dos objetivos da organização;
(ii) Plano organizacional para alcançar os objetivos;
(iii) Existência de pessoal em qualidade e quantidade proporcional às suas responsabilidades e com adequada segregação de funções;
(iv) Estabelecimento de um sistema de políticas;
(v) Sistema de revisão eficiente em todos os níveis de atividade, para certificar que o referido sistema de políticas e práticas está a ser implementado.

Controlo interno
Existem duas definições comummente aceites quando se fala em controlo interno:

"Qualquer ação empreendida pela gestão, pelo conselho de administração e outros membros da entidade, para aperfeiçoar a gestão do risco e melhorar a possibilidade do alcance dos objetivos e metas da organização. A gestão planeia, organiza e dirige o desempenho de ações suficientes para assegurar com razoabilidade que os objetivos e metas serão alcançados." (IIA)

"Processo levado a cabo pelo Conselho de Administração, Direção e outros membros da entidade com o objetivo de proporcionar um grau de confiança razoável na concretização dos seguintes objetivos: eficácia e eficiência dos recursos, fiabilidade da informação financeira; cumprimento das leis e normas estabelecidas." (COSO)

De uma forma geral, o controlo interno é um processo integrado, dotado de um plano e de um conjunto de sistemas coordenados entre si, que se destina a prevenir a ocorrência do risco, erros e irregularidades e a minimizar os seus impactos. Procura igualmente garantir, de forma razoável, que os objetivos da organização estão a ser alcançados, que as operações estão a ser realizadas de forma ética, económica e eficaz, que as obrigações contabilísticas estão a ser cumpridas, que existe conformidade com as leis e regulamentos e que existe a salvaguarda dos recursos. O controlo interno é instituído e gerido pela Direção da organização. Inclui o controlo interno contabilístico e o controlo administrativo.

Controlo manual
São os controlos que, não sendo executados por um computador, são executados manualmente pelo próprio utilizador.

Controlo primeiro nível
Ver Auditoria Interna.

Controlo segundo nível
Controlo administrativo interno que incumbe realizar a um organismo independente da organização a auditar, muito embora ambos dependam de um mesmo ou diferente membro do Governo.

Controlo preventivo
É o controlo que previne a ocorrência de qualquer tipo de acontecimento ou resultado inesperado (contrasta com o controlo de deteção).

Controlo qualidade
Controlo sistemático da capacidade que a organização possui para criar qualidade nos processos e atividades que desenvolve.
É um controlo sistemático porque os seus resultados surgem na sequência de um esforço planeado e intencional. Algumas organizações escolhem os seus sistemas de controlo de qualidade através de manuais da qualidade e/ou mapeamento de processos. Esses sistemas consistem num conjunto de linhas de orientação para implementar, na prática, os controlos de qualidade e a forma como medir e melhorar essa qualidade.

Controlo responsabilidade financeira (***Accountability Control***)
Visa assegurar que o dinheiro afeto a um propósito particular não seja gasto para outro fim ou em duplicado e que, de uma forma geral, a arrecadação e a realização de todas as receitas e despesas públicas sejam efetuadas de forma legal, regular, económica, eficiente e eficaz.

Controlo sistema operacional
Conjunto de ações consideradas integrantes do sistema de controlo interno e que se relacionam com a estrutura organizacional, bem como, todos os métodos e procedimentos adotados pela gestão da organização. O seu objetivo é conduzir e implementar o negócio, os processos, programas, projetos, atividades e funções da organização de forma regular, produtiva e económica. Além disso, deve também gerar informação de gestão com base nos resultados alcançados.

CSR – *Corporate Social Responsibility Directive*
Os cidadãos da União Europeia (UE) esperam que as empresas compreendam os seus impactos positivos e negativos na sociedade e no ambiente. E que, por conseguinte, previnam, gerem e atenuem qualquer impacto negativo que possam causar, incluindo na sua cadeia de fornecimento global. O cumprimento deste dever é comummente conhecido como CSR ou traduzido para português "Responsabilidade Social das Empresas (RSE)" ou ainda "*Responsible Business Conduct* (RBC)", traduzido para português "Conduta Empresarial Responsável".

A Comissão Europeia definiu a RSE como a responsabilidade das empresas pelo seu impacto na sociedade, sendo a sua condução no terreno um dever das próprias empresas. As empresas podem e devem tornar-se socialmente responsáveis por; integrar preocupações sociais, ambientais, éticas, de consumo e de direitos humanos na sua estratégia empresarial e nas suas atividades; cumprir a lei. A RSE e o RBC são importantes para as empresas, uma vez que proporcionam benefícios em termos de gestão do risco, poupança de custos, acesso ao capital, relações com os clientes, gestão dos recursos humanos, sustentabilidade das operações, capacidade de inovação e por fim, lucro. Para a economia da UE, a RSE e o RBC tornam as empresas mais sustentáveis e inovadoras, o que contribui para uma economia mais sustentável.

Para a sociedade, a RSE e o RBC oferecem um conjunto de valores sobre os quais podemos construir uma sociedade mais coesa e sobre os quais podemos basear a transição para um sistema económico sustentável.

Correspondência
Medida qualitativa e/ou quantitativa da conformidade das informações, situações ou procedimentos relativamente a critérios pré-estabelecidos.

Corrupção
Existe sempre que os poderes atribuídos são utilizados de forma ilegal ou pouco ética, com a intenção de obter ganhos, benefícios ou vantagens pessoais.

COSO (*Committee of Sponsoring Organizations of the Treadway Commission*)
Organização privada, criada nos EUA em 1985, para prevenir e evitar fraudes nas demonstrações contabilísticas das empresas. Reúne atualmente várias organizações contabilísticas. Publicou, em 1992, um estudo sobre o controlo interno (*Internal Control – Integrated Framework*). É um dos estudos de referência sobre esta matéria, conhecido como o Relatório COSO.

Critérios pré-estabelecidos
Conjunto de leis, normas, regras, regulamentos (tanto internos como externos), contratos e princípios corporativos que conformam qualquer tipo de atividade ou operação de uma organização.

Cultura organizacional
A cultura organizacional é o conjunto de valores, crenças, convicções, conhecimentos e perceções que conferem à organização uma identidade própria e uma capacidade para atuar com maior ou menor coerência e eficácia e que inspiram e condicionam os comportamentos dos seus colaboradores.

Custos
Medida dos recursos consumidos durante um período de tempo, sem considerar quando foram ordenados, autorizados ou pagos.

D

Delimitação da auditoria
Ver Âmbito da Auditoria.

Deficiência
Uma deficiência é uma limitação assumida do controlo interno, tanto potencial como efetiva. Pode ser também entendida como uma oportunidade para fortalecer o controlo interno de forma a garantir razoavelmente que os objetivos organizacionais serão alcançados.
Desempenho
Medida de realização alcançada por um indivíduo, equipa, processo ou organização.

Detentores de interesse/Interessados
São todos aqueles que têm interesse/necessidade de receber informação do auditor, tanto ao nível interno como externo. Podem ser os órgãos dos diferentes níveis hierárquicos da organização, colaboradores, acionistas ou sócios, investidores, Estado e cidadãos em geral, entre outros.

Devida atenção/diligência devida (*due care*)
O elemento apropriado de cautela/atenção e habilidade que um auditor deve aplicar, considerando a complexidade das tarefas de auditoria, incluindo a atenção cuidadosa ao planeamento, recolha e avaliação de evidências, a formação de opiniões, conclusões e formulação de recomendações.

Diagnóstico
Identificação de causas de deficiências ou da não qualidade.

Diagrama/desenho do processo
Representação gráfica, modelação/mapeamento/fluxograma do conjunto de ações que ocorrem num processo.

Diretor executivo de auditoria
Lugar na organização que tem como responsabilidade todas as atividades de auditoria interna. Corresponde, de uma forma geral, ao lugar de Diretor de Auditoria Interna. No caso de as atividades de auditoria interna serem realizadas por prestadores de serviço externos, o Diretor Executivo de Auditoria é responsável pela supervisão e acompanhamento do contrato de prestação de serviços e por garantir a qualidade geral dessas atividades. Está subordinado à Direção e ao Conselho de Auditoria relativamente às atividades de auditoria interna e ao acompanhamento dos resultados dos trabalhos de auditoria.

Documentação controlo interno
Esta documentação, relacionada com a estrutura do sistema de controlo interno, é constituída pela evidência material e escrita de todas as componentes desse sistema. Inclui a identificação da estrutura e da política organizacional e suas categorias operacionais, os objetivos e as atividades de controlo. Estas evidências devem constar de documentos como, por exemplo, as diretivas de gestão, as políticas administrativas, manuais de procedimentos e de contabilidade.

Documentos justificativos
Documentos que permitem confirmar que as operações foram, de facto, efetuadas e/ou registadas.

Documentos trabalho
O documento de trabalho é o suporte e fundamento de todo o trabalho realizado pelo auditor interno. Deve incluir o registo de todas as informações utilizadas, as verificações realizadas e as conclusões alcançadas no decorrer do trabalho de auditoria.

Dossier permanente
Dossier que contém todos os documentos e informações gerais de caráter permanente, úteis à auditoria, incluindo os resultados de auditorias anteriores. Este dossier deve ser atualizado em função da evolução da situação da entidade auditada e dos resultados das auditorias que, entretanto, forem realizadas.

DPO – *Data Protection Officer*
O principal papel do responsável pela proteção de dados, em Portugal utiliza-se o termo Encarregado Proteção de Dados (EPD), é assegurar que na sua Organização os dados pessoais do seu pessoal, clientes, fornecedores ou quaisquer outros indivíduos (também designados por titulares dos dados) são tratados em conformidade com as regras de proteção de dados aplicáveis. Nas instituições e organismos da UE, o regulamento relativo à proteção de dados aplicável (Regulamento UE 2018/1725) obriga cada um deles a nomear um EPD. O Regulamento UE 2016/679, que obriga algumas Organizações nos países da UE a nomear um EPD, é aplicável a todos os Estados Membros, desde o dia 25 de maio de 2018.

Due diligence
Due diligence consiste na verificação das áreas de atividade interna de uma organização, com a intenção de identificar prováveis situações de risco ou situações que se relacionem com contingência, obrigações fiscais, legais e contabilísticas, como, por exemplo, valores a receber, existências, entre outros.

E

Economia
Minimização dos custos inerentes a qualquer tipo de atividade, através da aquisição dos recursos financeiros, humanos e materiais apropriados, tanto ao nível da sua qualidade como da sua quantidade, ao menor custo e no momento oportuno.

Económico
Ausência de desperdícios, obtendo ao mais baixo custo, com a qualidade devida e na altura adequada, os recursos necessários.

Efeitos (*outcomes*)
São os eventos que mudaram ou que devem ser vistos como tendo sido modificados, em resultado dos "outputs" de um processo, programa, projeto ou atividade. Esse conjunto de eventos inclui tanto as consequências pretendidas como as não pretendidas do processo, programa, projeto ou atividade.

Eficácia
É a relação entre o impacto esperado de uma atividade e o seu impacto real. Uma atividade é eficaz sempre que os resultados alcançados correspondem ou superam os objetivos pretendidos.

Eficácia da gestão
Trata-se de atingir os resultados ao mais baixo custo e com qualidade. Pode ser avaliada por intermédio de um conjunto variado de métricas: liderança, delegação, motivação, retorno sobre o/do investimento, retorno sobre/dos ativos e retorno sobre o/do património líquido.

Eficaz
Grau de concretização dos objetivos ou medida em que os resultados de uma atividade correspondem aos objetivos esperados.

Eficiência
Relação entre os recursos financeiros, humanos e materiais utilizados numa determinada atividade e os resultados produzidos por essa atividade. Implica que com um montante mínimo de recursos disponíveis se maximizem os resultados, sem descurar a sua qualidade.

Encarregado Proteção de Dados (EPD)
Ver *DPO – Data Protection Officer*

Enterprise Risk Management (ERM)
ERM é um processo contínuo que estabelece objetivos para a gestão do risco e define qual o nível de tolerância e os limites para todos os riscos organizacionais relevantes. Também pode ser descrita como uma abordagem baseada no risco para gerir uma organização, integrando conceitos de planeamento estratégico, gestão operacional e controlo interno.

Entidade auditada
A Organização, serviço, processo, programa, projeto, atividade ou função sujeitas à auditoria.

Equivalentes em caixa
São os depósitos bancários e os investimentos de curto prazo que se podem converter em numerário, sem que isso implique riscos significativos de alteração de valor no prazo máximo de três meses a partir da sua constituição ou aquisição. Os chamados descobertos bancários (*overdraft*) podem ser considerados como os componentes negativos dos equivalentes em caixa.
Erro
Um erro é uma falta profissional motivada pela negligência ou desconhecimento de determinados princípios, normas ou regras estabelecidas e que pode prejudicar a regularidade dos atos e dos factos.

Estratégia
Plano de longo prazo das ações ou medidas a tomar, hierarquizadas, para alcançar os objetivos globais ou cumprir a missão de uma organização.

Estrutura organizacional
É o esqueleto que constitui a base de uma organização. É a forma como as unidades orgânicas se organizam, com o objetivo de promover a concretização dos objetivos da organização e de melhorar a sua própria capacidade. Inclui, por exemplo, a divisão por áreas de trabalho ou funções, as vias de comunicação entre gestores e colaboradores e a divisão de responsabilidades e atividades na organização.

Estudo dos sistemas
Este tipo de estudo inclui a análise do conjunto das informações de natureza regulamentar, organizacional e de controlo interno da organização. Engloba, igualmente, a descrição dos sistemas e dos controlos internos existentes com a intenção de, posteriormente, proceder à verificação dessa mesma descrição e, no final, fazer uma avaliação de conjunto.

Estudo preliminar
É um documento que dá uma visão global preliminar das características fundamentais da divisão de responsabilidades numa organização. O objetivo do estudo preliminar é recolher as informações relacionadas com a organização a auditar.

Ética
Por ética no serviço público entende-se o conjunto de valores e normas comuns que devem reger a atividade do funcionário público no desempenho das suas funções.

A natureza moral desses valores/normas, que podem ser declaradas ou implícitas, referem-se ao que é considerado ser correto, errado, bom ou mau comportamento. Enquanto os valores definem os princípios morais, as normas estabelecem, também, o que é legalmente correto numa determinada situação.

Evidências (de auditoria)
As evidências de auditoria são todas as provas documentais que fundamentam o trabalho e as observações realizadas pelo auditor. São as informações que comprovam uma declaração ou um facto e são fundamentais para a formulação de conclusões e recomendações objetivas e corretas. Podem ser obtidas através da pesquisa documental, da observação ou do consenso.

Exame fiscal
Ver Auditoria Fiscal.

Exequibilidade
Tipo de procedimento que permite definir de forma plausível, até que ponto o nível de conhecimento disponível e as condições técnicas e institucionais existentes numa organização permitem antecipar respostas fiáveis e credíveis às questões de auditoria.

F

Fases da auditoria
Uma auditoria inclui normalmente as seguintes fases sucessivas:

1. estudo preliminar;
2. plano da auditoria;
3. programa de trabalho;
4. execução da auditoria in loco;
5. elaboração do relatório;
6. procedimento de contraditório;
7. decisão final;
8. acompanhamento de resultados.

Ver Programa de Auditoria.

Ferramenta
Utensílio, dispositivo, mecanismo físico ou intelectual utilizado por trabalhadores das mais diversas áreas para realizar qualquer tipo de tarefa. Também pode ser definida como um dispositivo que forneça uma vantagem mecânica e/ou mental para facilitar a realização de tarefas diversas.

Fiabilidade
Coerência e consistência dos dados e conclusões de uma auditoria, tomando como referência as técnicas, procedimentos e análises empregues na recolha e interpretação da informação durante o processo de auditoria. A auditoria será fiável sempre que as observações repetidas, utilizando metodologias similares, nas mesmas condições, dão origem a resultados semelhantes.

Fiscalização "a posteriori"
Atividade que consiste em verificar, posteriormente à sua realização, se a atividade das entidades sujeitas a fiscalização se desenvolveu de acordo com as leis em vigor e os objetivos fixados, podendo-se traduzir em julgamento de contas, auditorias, entre outros.

Fiscalização concomitante
Verificação, no decorrer da realização das atividades e operações de uma organização, da sua conformidade não só com a legislação e com as normas em vigor, mas também, com os objetivos inicialmente fixados.

Fiscalização externa
Ver Controlo Externo.

Fiscalização orçamental
Verificação, por parte da organização, da forma como o seu orçamento foi executado, tendo em consideração a conformidade com as previsões efetuadas, com as autorizações concedidas e com os regulamentos enquadradores.

Fiscalização prévia
Atividade que consiste em verificar, antes da respetiva produção de efeitos financeiros, se determinados atos e contratos a ela submetidos por força da lei, estão em conformidade com as normas em vigor e se os respetivos encargos têm cabimento em verba orçamental própria.

Fiscalização sucessiva
Verificação, após conclusão das atividades e operações de uma organização, da sua conformidade não só com a legislação e com as normas em vigor, mas também, com os objetivos que tinham sido fixados inicialmente. Pode assumir a forma de um julgamento das contas, auditorias, entre outras.

Fluxograma
Representação gráfica dos fluxos de procedimentos, documentos e informação que existem numa organização, através de um diagrama que os apresenta de forma sequencial. É uma ferramenta muito útil visto que descreve sinteticamente circuitos ou procedimentos complexos.

Fluxos de caixa
São as entradas em caixa (recebimentos) e saídas (pagamentos) e seus equivalentes.

Fraude
Manipulação, falsificação ou omissão intencional de registos e/ou documentos por um indivíduo ou organização, com a intenção de obter vantagens pessoais, injustas e desonestas. Pode traduzir-se tanto na obtenção imprópria de dinheiro, propriedades ou serviços, como na tentativa de evitar despesas ou perder serviços. Envolve necessariamente atos de engano, traição, ocultação ou quebra de confiança, sem recurso a ameaças ou força física.

Função
Conjunto de atividades que caracterizam um determinado posto de trabalho no contexto organizacional.

Fundação Europeia para a Gestão da Qualidade (EFQM)
A EFQM é uma fundação sem fins lucrativos, fundada em 1988 pelos presidentes de 14 grandes empresas europeias, com o apoio da Comissão Europeia. Resultou da necessidade de desenvolver uma estrutura europeia para a melhoria da qualidade. Desenvolveu um modelo de gestão organizacional, chamado Modelo de Excelência EFQM, introduzido em 1991. O seu objetivo é facilitar a autoavaliação da qualidade organizacional e constituir a base de apreciação das candidaturas ao *European Quality Award* (EQA) – Prémio Europeu da Qualidade.

Fundamental
Um assunto torna-se fundamental ("suficiente material") mais do que "material" quando o seu impacto nas demonstrações financeiras ou outra informação financeira que esteja sendo auditada, seja tão vasto que as põe em causa como um todo.

G

Garantia razoável
A garantia razoável significa que existe um nível de confiança satisfatório de que os objetivos pretendidos da organização serão alcançados, de acordo com os custos, benefícios e riscos identificados. Significa que o controlo interno apenas pode dar essa garantia razoável, não podendo garantir a concretização dos objetivos organizacionais.

Generalized Audit Information Network (GAIN)
Rede de informação criada pelo IIA que permite que as organizações que a integram possam comparar a dimensão, experiência, especialização e outras medições das suas unidades de auditoria com a média geral de outras organizações de características e dimensões semelhantes, do mesmo sector de atividade.

Gestão de recursos humanos
Abordagem de gestão que se relaciona com a gestão, desenvolvimento e utilização dos conhecimentos, competências e potencialidades totais dos colaboradores da organização. O seu objetivo é apoiar as políticas e o planeamento das atividades, bem como, o funcionamento eficaz dos processos.

Gestão de risco
Processo de identificação, avaliação, gestão e controlo de potenciais acontecimentos ou situações que possam afetar a concretização dos objetivos da organização, procurando proporcionar uma garantia razoável de que esses objetivos serão atingidos.

Gestão do conhecimento
Gestão explícita e sistemática do conhecimento vital, que está associada aos processos de criação, organização, difusão, utilização e exploração do conhecimento. Este tipo de gestão utiliza várias práticas e processos, desde a criação, partilha e aprendizagem (comunidade de práticas), organização e gestão.

Gestão orientada para os resultados
Estratégia de gestão que se centra no desempenho e na obtenção de resultados, efeitos e impactos.

Gestão pela qualidade total
Abordagem de gestão orientada para a valorização da qualidade superior de todos os processos organizacionais, cujo objetivo é envolver todos os níveis da organização. Centrada no cliente, esta abordagem procura melhorar constantemente os processos através da utilização de ferramentas analíticas e do trabalho de equipa envolvendo

todos os colaboradores da organização. A CAF (*Common Assessment Framework* – Estrutura Comum de Avaliação) é um dos exemplos de modelos deste tipo de gestão.

Governação
Por governação entende-se o conjunto de processos e estruturas que são implementados para dirigir uma organização. É a forma como essa organização toma e implementa as suas decisões, informa, dirige, gere e acompanha as suas atividades e operações para alcançar os seus objetivos. Implica que quem define esses objetivos os comunica a todos os detentores de interesse e toma medidas que garantam que as atividades da organização estão orientadas para a sua concretização.

Governação Corporativa
Conjunto de processos, hábitos, políticas, leis e instituições que afetam a forma como se dirige, administra e controla uma organização.

I

Idoneidade
Atributo da informação que é quantitativamente suficiente e apropriada para alcançar os resultados da auditoria; e é qualitativamente imparcial a fim de inspirar confiança e segurança.

Impacto
O efeito final dos resultados não apenas na obtenção direta dos objetivos, mas também, no efeito mais amplo noutras metas ou nos objetivos de outrem. O impacto refere-se também ao conjunto de resultados não pretendidos do processo, programa, projeto ou atividade.

Incerteza
Impossibilidade de conhecer antecipadamente que eventos poderão vir a afetar a atividade da organização, qual o seu impacto e probabilidade de ocorrência.

Independência
Inexistência total de qualquer tipo de condição/situação que possa representar uma ameaça real ou potencial à objetividade do auditor. Essas ameaças devem ser geridas a vários níveis, desde o nível individual de cada auditor até ao nível organizacional.

Indicador
Medida de um objetivo que se pretende alcançar ou atingir, de um recurso mobilizado, de um efeito obtido, de um elemento de qualidade, de uma variável de contexto. Os indicadores são, acima de tudo, instrumentos de informação com vista a apoiar os gestores a comunicar, negociar e decidir. Representam uma determinada grandeza, um número, uma cifra, um cálculo (n.º, % ou taxa) que permite objetivar um acontecimento ou uma situação e interpretá-los.

Indícios
Os indícios são sinais ou vestígios que determinam a orientação do trabalho de investigação do auditor, no sentido de comprovar a existência, ou não, de uma determinada condição ou situação.

Informações probatórias
São as provas documentais e outras informações pertinentes que fundamentam as conclusões e o relatório final de auditoria.

Inputs
São os recursos humanos, financeiros, físicos, lógicos, tecnológicos, entre outros, que uma organização utiliza ou consome. Em SI uma orientação a processos é muito relevante.

Inovação
Processo que permite transformar ou converter novas ideias em novos serviços, processos, ferramentas, sistemas e relações humanas. Para uma organização ser considerada inovadora tem que realizar uma atividade preexistente de forma diferente; oferecer aos seus clientes um serviço novo ou prestar o mesmo serviço, mas de forma diferente (por exemplo, através da internet).

Inquérito por questionário
Técnica de obtenção de dados que consiste na recolha sistemática de informação a partir de uma população definida. Essa informação é, normalmente, obtida através da realização de entrevistas ou questionários numa amostra da referida população. Os inquéritos são utilizados para recolher informação detalhada e específica de um grupo de pessoas ou organizações. São especialmente úteis quando se pretende quantificar informação oriunda de um elevado número de indivíduos sobre uma determinada questão ou assunto.

Inspeção
A inspeção pode ser definida de duas formas diferentes:

1. Procedimento utilizado para suprir qualquer omissão ou lacuna ao nível da informação, esclarecer dúvidas ou qualquer denúncia respeitante à legalidade ou legitimidade de factos/atos administrativos praticados por qualquer responsável que esteja sujeito a esse tipo de procedimento.
2. Verificação física de determinados bens do ativo (existências, imobilizado corpóreo, etc.) e dos documentos de suporte de diversas operações (vendas, compras, recebimentos, pagamentos, entre outros).

Inspetor
Auditor pertencente a organismos públicos de inspeção. Ver Auditor.

Instituição de fiscalização
Entidade pública que, independentemente da forma como é designada, constituída ou organizada, desempenha, em conformidade com a lei, as funções de fiscalização.

Intensidade da auditoria
Maior ou menor exaustão dos procedimentos de auditoria aplicados. A intensidade determina o tamanho das amostras ou a cobertura em percentagem dos elementos a verificar.

Intervalo de confiança
Ver Nível de Significância.

Institute of Internal Auditors (IIA)
O IIA é uma organização internacional que define os padrões éticos e práticos da atividade de auditoria interna, proporciona formação profissional e fomenta o profissionalismo de todos os seus membros. Em Portugal é representado pelo IPAI – Instituto Português de Auditoria Interna.

Integridade
Qualidade ou estado de possuir princípios morais sólidos. Implica retidão, honestidade e lealdade, desejo ou vontade de fazer aquilo que está certo, professar e viver de acordo com um conjunto de valores e expectativas.

Interessados/Detentores de interesse
São todos aqueles que têm interesse/necessidade de receber informação do auditor, tanto ao nível interno como externo. Podem ser os órgãos dos diferentes níveis hierárquicos da organização, colaboradores, acionistas ou sócios, investidores, Estado e cidadãos em geral, entre outros. Ver *Stakeholders*.

Intervenção da gestão
Qualquer tipo de ação tomada pela gestão, que se sobrepõe a qualquer política ou procedimento prescrito com a intenção de legitimação. Essa intervenção é, geralmente, necessária para lidar com transações ou eventos pontuais, que não sejam nem correntes nem padronizados e que poderiam, se não houvesse essa intervenção, ser tratados de forma desadequada pelo sistema.

ISO (International Organization for Standardization)
ISO ou Organização Internacional para a Normalização é uma rede global que identifica as normas internacionais exigidas às empresas, governos e sociedade, as desenvolve com os contributos nacionais em parceria com os setores que as adotam mediante procedimentos transparentes e as divulga para serem implementadas em todo o mundo.

J

Julgamento de contas
Exercício do poder jurisdicional, atribuído a certas instituições de controlo, visando apreciar e decidir sobre a legalidade e regularidade das contas, prestadas por pessoas responsáveis pela gestão de recursos públicos.

L

Líder
A expressão líder é tradicionalmente associada às pessoas responsáveis por uma organização. São pessoas com características pessoais que lhes permite potenciar a motivação nos seus colaboradores.

Liderança
Forma como os líderes desenvolvem e prosseguem a missão e a visão da organização. Está relacionada com a forma como os líderes desenvolvem os valores necessários para o sucesso a longo prazo e os implementam por meio de ações e comportamentos adequados. Indica a forma como os líderes estão pessoalmente empenhados em garantir que o sistema de gestão está desenvolvido, implementado e revisto e que a organização aposta permanentemente na inovação e na mudança.

Limitações inerentes
Todos os sistemas de controlo interno possuem limitações que lhes são inerentes. Estas limitações estão relacionadas com vários fatores: limitações da capacidade de julgamento humano; constrangimentos ao nível dos recursos e da necessidade de considerar o custo desses controlos em comparação com os benefícios pretendidos; a probabilidade real de que esses sistemas podem falhar e a possibilidade de serem ultrapassados e de haver um conluio ao nível da gestão.

M

Manual auditoria
O manual de auditoria é um documento que deve conter a descrição dos princípios, métodos e técnicas de auditoria, assim como as normas de auditoria que devem ser respeitadas pelos auditores. Constitui um instrumento indispensável para uma abordagem coordenada e harmonizada dos auditores integrados numa mesma instituição de auditoria.

Manual qualidade
Manual que define a política, o sistema e as práticas de qualidade de uma organização. Apesar de ser utilizado na relação da organização com o exterior (por exemplo, clientes, fornecedores e entidades oficiais), deve servir fundamentalmente como um guia para os funcionários da organização. O manual pode abranger apenas um sector de atividade da organização e podem coexistir manuais a diversos níveis.

Mapa de processos
Representação gráfica da sequência de ações que ocorrem entre processos.

Materialidade
Ver Relevância.

Maturidade do risco
A maturidade do risco é a forma como a gestão adotou e aplicou, em toda a organização, uma gestão de risco robusta, de acordo com o planeado, para identificar, apreciar e decidir respostas e identificar as oportunidades e ameaças que possam afetar a concretização dos objetivos da organização.

Meta
Projeção futura de realização em tempo determinado numa área de reconhecida responsabilidade. Uma meta envolve a conversão de objetivos em tarefas que sejam faseadas no tempo, possíveis, quantificáveis e alcançáveis.

Métodos de auditoria
Processos racionais, orientados de acordo com normas específicas, que permitem conduzir o auditor em direção ao resultado esperado.

Métodos de seleção
Métodos, estatísticos ou não estatísticos, utilizados para se proceder à seleção da amostra.

Missão
Conceito de gestão estratégica muito utilizado em Gestão orientada para os resultados.

A missão resume o que uma organização deve definir para a sua estratégia, nomeadamente, qual é a sua finalidade para existir no mercado, razão de ser, a imagem que pretende transmitir aos seus clientes, os processos de negócio e as atividades principais que se propõe prosseguir.

Monitorização contínua
A monitorização contínua é o processo sistemático e permanente que permite obter, analisar e comunicar qualquer informação relacionada com o negócio da organização, de forma a poder identificar e responder aos riscos operacionais desse negócio.

N

NIS2 – *Network and Information Security Directive*
Introduzida em 2020 entrou em vigor a 16 de janeiro de 2023. A Diretiva NIS2 é uma continuação e expansão da anterior diretiva da UE relativa à cibersegurança, a NIS. Foi proposta pela Comissão Europeia para desenvolver e retificar as deficiências da diretiva NIS original. Esta Diretiva tem por objetivo reforçar a segurança das redes e dos sistemas de informação na UE, exigindo que os operadores de infraestruturas críticas e de serviços essenciais apliquem medidas de segurança adequadas e comuniquem quaisquer incidentes às autoridades competentes.

Nível de confiança
O nível de confiança é o nível máximo de inexatidões, ilegalidades e/ou irregularidades detetadas na população analisada, considerado tolerável pelo auditor. Esse nível deve ser fixado a priori pelo próprio auditor uma vez que a dimensão da amostra é por ele influenciada. Neste sentido, quanto menor for o nível de confiança mais extensa e abrangente será a auditoria a realizar.

Nível de significância
Máximo de inexatidões, ilegalidades ou irregularidades que o auditor pode tolerar numa população a analisar. Fixado "a priori" pelo auditor, influencia o tamanho da amostra sobre a qual se realizam as auditorias. Quanto menor for o nível, maior será a extensão da auditoria a realizar. Ver Risco de Auditoria.

Normas de auditoria interna
As normas são o conjunto de regras e procedimentos a serem respeitadas pelo auditor em todas as fases de uma auditoria, desde o seu planeamento, passando pela execução até à elaboração do relatório final. São pronunciamentos profissionais emitidos pelo Conselho de Normas de Auditoria Interna, que estipulam não só como se processam as atividades de auditoria como a forma de se avaliar o seu desempenho. São os critérios que vão permitir avaliar os resultados alcançados pela auditoria.

Normas para elaboração de relatórios de auditoria
Estas normas gerais têm como função orientar o auditor na elaboração dos relatórios de auditoria que contenham os respetivos resultados. Essas normas incluem orientações não só sobre a forma do relatório, mas também sobre o seu conteúdo.

O

Objetividade
A objetividade é um elemento fundamental em qualquer tipo de trabalho de auditoria. É uma disposição mental que se caracteriza pela isenção. Garante que as atividades de auditoria sejam realizadas pelos auditores de tal forma que sejam aceites por todos como sendo honestas e isentas, sem comprometer a sua qualidade. O auditor deve ser independente na apreciação e julgamento da informação disponível, ou seja, não ser permeável a interferências de terceiras partes. As suas conclusões devem ser fundamentadas em procedimentos pré-estabelecidos.

Objetivos do trabalho de auditoria
Estes objetivos são as declarações mais abrangentes propostas pelos auditores internos e definem o que se pretende com o trabalho de auditoria em causa.

Objetivos específicos
Concretização dos objetivos gerais de auditoria num conjunto de aspetos e questões específicas a verificar no decorrer da auditoria.

Objetivos gerais
Declaração exata daquilo que se pretende que a auditoria realize e/ou da questão que é necessário esclarecer.

Objeto da auditoria
O objeto da auditoria é aquilo que vai ser fiscalizado/verificado pela auditoria. Pode ser uma organização, programa, atividade, função, projeto, operação ou sistema.

Obrigação de prestar contas
Obrigação imposta a uma pessoa ou a uma entidade sujeita a fiscalização, para demonstrar que a gestão ou fiscalização dos recursos que lhe foram confiados foi feita em conformidade com as condições estabelecidas aquando da atribuição desses recursos.

Orçamento
Expressão quantitativa e financeira de um programa de ação cuja realização é preconizada para determinado período futuro, permitindo o acompanhamento da sua execução e o controlo "a posteriori" dos resultados obtidos.

Operações
As operações são o conjunto de funções, processos e atividades que permitem alcançar os objetivos de uma organização. São implementadas com "objetivos" e "controlos" definidos e, devido ao seu papel no alcançar dos objetivos de uma organização, estão relacionadas com a eficácia e a eficiência das atividades organizacionais, incluindo os objetivos de desempenho, de rentabilidade e de salvaguarda de bens.

Otimização de recursos
A otimização de recursos consiste na obtenção da melhor relação qualidade-preço.

Orçamento
Expressão quantitativa e financeira de um programa de ação, cuja realização é prevista ocorrer num determinado período no futuro. É possível realizar o acompanhamento da sua execução e proceder ao controlo *a posteriori* dos resultados alcançados.

Organização aprendente
Uma organização onde as pessoas aumentam continuamente as suas capacidades para alcançar os resultados pretendidos, onde são estimulados novos e elevados padrões de pensamento, onde as aspirações coletivas emergem e onde as pessoas se encontram em aprendizagem contínua no contexto da própria organização.

Organização Internacional das Instituições Superiores de Auditoria (INTOSAI)
Organização internacional que reúne as instituições superiores nacionais de auditoria de diversos países. O grande objetivo do INTOSAI é promover o intercâmbio de ideias e experiências entre essas instituições no que diz respeito às finanças públicas e ao controlo do desempenho. O Tribunal de Contas português é membro desta organização.

Outputs
Numa orientação a processos, trata-se do produto/atividade em termos de bens, serviços ou outros resultados.

P

Padrões de ação/execução
Quadro de referência para o auditor sistematicamente cumprir o objetivo de uma auditoria, incluindo o seu planeamento e supervisão, a obtenção de evidência qualifica, relevante e razoável, bem como, o adequado estudo e avaliação dos controlos internos.

Padrões auditoria
Critérios ou medidas de comparação relativamente aos quais a qualidade dos resultados da auditoria são avaliados.

Padrões usuais do auditor
Qualificações, competências, objetividade e independência necessárias e o exercício da devida atenção que deverão ser exigidas do auditor para desempenhar de forma competente, eficiente e eficaz as tarefas relacionadas com a sua área e com os padrões de relatório.

Papéis de trabalho
Ver Documentos Trabalho.

Papel de consultor
Posição em que o auditor desempenha uma função de orientar, a qual é estritamente consultiva.

Parecer
Um parecer é a opinião formulada pelo auditor sobre o objeto da auditoria. Normalmente, refere-se à exatidão, legalidade e regularidade das operações e dos elementos que foram examinados.

Pasta de arquivo corrente
O arquivo corrente é constituído por toda a documentação e informação obtida e/ou recolhida pelo auditor no decorrer da auditoria e que irá servir para elaborar o relatório final de auditoria. Esta pasta permite conservar a prova do trabalho efetuado, facilitando, por isso, a supervisão do trabalho. A sua estrutura é, normalmente, a seguinte: Índice, Plano Global de Auditoria, Programas de Auditoria, documentos justificativos do trabalho realizado; comprovativos; relatórios dirigidos às entidades fiscalizadas; conclusões e recomendações da auditoria.

Pasta de arquivo permanente
O arquivo permanente é constituído por toda a documentação e informação geral, que possua carácter de utilidade permanente para a auditoria, incluindo os resultados de auditorias realizadas anteriormente. Deve ser atualizado permanentemente de forma a acompanhar a evolução da situação da entidade fiscalizada e dos trabalhos de auditoria que estejam/venham a ser realizados.

PED
Processamento Eletrónico de Dados. Em inglês, *Electronic Data Processing* (abrev. EDP). Utilização de computadores para o tratamento de dados, através da execução de instruções simples e/ou repetitivas para processar grandes volumes de informação.

Perfil de exigências
Conjunto de condições base para o desempenho de determinada função – como, por exemplo, formação e experiência profissional, aptidões, traços de personalidade, entre outros.

Estas condições são suscetíveis de serem avaliadas e medidas instrumentalmente e que são condição necessária, mas não suficiente, para o desempenho efetivo dessa função. Este perfil obtém-se através da análise do posto de trabalho, a qual é realizada com uma tónica especial nos atributos de cada função.

Perfil de risco
O perfil de risco é constituído por um resumo, ou matriz básica, de todos os principais riscos que podem afetar a atividade de uma organização ou unidade orgânica. Esse perfil deve incluir o nível de impacto desse risco (isto é, se é alto, médio ou baixo) e a probabilidade de vir a ocorrer.

Pista de auditoria
Vestígio que pode influenciar a orientação da auditoria.

Planeamento de auditoria
Processo de definição dos principais objetivos da auditoria, do âmbito, prazo e métodos a utilizar durante a sua realização. É fundamental para identificar os instrumentos considerados necessários à gestão das tarefas de auditoria (como, por exemplo, o plano global de auditoria, programas de auditoria, orçamentação de recursos).

Planeamento dos recursos humanos
Processo constituído pelo conjunto de sistemas e procedimentos que vão permitir a uma organização dispor, no momento e local oportunos, do número adequado de pessoas competentes para concretizar os seus objetivos.

Plano dos recursos humanos
Este plano indica quais as diferentes fases do trabalho a realizar e a quantidade de tempo a ser despendida por cada um dos membros da equipa de auditoria com cada uma dessas fases.

Plano global de auditoria
O plano global de auditoria é o documento básico de auditoria. Os seus objetivos gerais são:

1. Apresentação dos objetivos gerais da auditoria;
2. Definição da estratégia global da auditoria e do campo de auditoria;
3. Correta documentação das opções importantes que foram tomadas para que a auditoria fosse realizada.

Em termos específicos, um plano de auditoria é suportado por um documento que integra um programa de auditoria e tem os seguintes objetivos:

a) expor os objetivos gerais da auditoria;
b) definir o risco da auditoria;
c) definir a metodologia e o âmbito da auditoria;
d) definir os pontos críticos a verificar e os principais procedimentos a adotar;
e) definir as amostras;
f) propor a equipa e o cronograma da auditoria.

Política
Uma política é a forma como a gestão de uma organização determina o que deve ser feito para exercer o controlo. Ela serve de fundamento aos procedimentos necessários para a sua implementação.

Pontos-chave de controlo
Os pontos-chave têm como função evitar e/ou detetar erros que possam ocorrer em fases decisivas dos procedimentos e operações da organização. Por isso, assumem um papel fundamental num sistema de controlo interno.

População de referência (universo)
A população de referência é um conjunto finito de dados, delimitado no tempo e no espaço. No caso da verificação efetuada ser exaustiva, a constatação referir-se-á a essa população de referência. Caso a verificação seja parcial, os resultados obtidos serão alargados a ela.

Postulados
Hipóteses básicas, premissas consistentes, princípios lógicos e demais requisitos que representam o quadro geral para o desenvolvimento dos padrões de auditoria.

Prejuízos à independência
A objetividade do auditor e a independência organizacional da auditoria interna podem ser prejudicadas por várias razões: existência de conflito de interesses, âmbito de auditoria limitado, restrições ao acesso a registos, pessoas e instalações, assim como limitações ao nível orçamental.

Premissas básicas de auditoria
Estas premissas são: Integridade, Objetividade, Confidencialidade e Competência.

Prestação de contas (*accountability*)
Dever, decorrente de dispositivos legais, que as organizações ou seus colaboradores têm de demonstrar que a gestão e controlo dos recursos públicos que lhes foram confiados respeitou os termos estabelecidos aquando da sua atribuição. É efetuada através da apresentação de documentos que expressam e comprovam a situação financeira da organização e o resultado das operações realizadas sob responsabilidade dessa organização. É uma forma de responsabilização das organizações públicas, e dos colaboradores, pelas suas decisões e ações, desde as relacionadas com a administração dos fundos públicos até ao seu desempenho.

Prestador externo de serviços
Pessoa ou entidade externa à organização e que possui o conhecimento, a capacidade e a experiência específica numa determinada área ou disciplina.

Princípios contabilísticos geralmente aceites
Princípios gerais aceites pelas associações ou organismos profissionais que se ocupam da harmonização das normas contabilísticas e nos quais se baseia a contabilidade.

Princípios gerais de auditoria
São as premissas básicas que orientam a elaboração das normas de auditoria. Todo o trabalho de auditoria deve respeitar de forma rigorosa estes princípios, especialmente nas situações em que não existam normas de auditoria específicas.

Procedimento de contraditório
Procedimento que consiste em submeter, formal ou informalmente, o projeto de relatório de auditoria à análise da entidade auditada para que esta manifeste a sua posição sobre as respetivas asserções, conclusões e recomendações, dentro de um determinado prazo.
Procedimentos
Ação ou conjunto de ações que implementam uma determinada política.

Procedimentos de auditoria
Conjunto de procedimentos que são descritos no programa de auditoria e devem ser aplicados sistematicamente e de forma adequada. As verificações, instruções e detalhes são alguns exemplos destes procedimentos.

Processo
Conjunto de procedimentos que transformam as entradas em resultados ou impactos e, deste modo, acrescentam valor.

Processo disciplinar
Procedimento que tem em vista efetivar a responsabilidade disciplinar.

Processo de gestão
Conjunto de ações executadas pela gestão, com o objetivo de gerir a organização. O controlo interno faz parte e está integrado no processo de gestão organizacional.

Processo organizacional
Processo de definição e delegação de tarefas, objetivos e responsabilidades. No âmbito de um processo organizacional define-se, igualmente, a autoridade de cada pessoa, estabelecendo-se, assim, uma hierarquia.

Processos de controlo
Os processos de controlo são o conjunto de políticas, procedimentos e atividades que constituem a estrutura de controlo. O seu objetivo é assegurar que os riscos identificados pela organização são contidos dentro dos limites de tolerância ao risco estabelecidos no decorrer do processo de gestão do risco.

Produtividade
O "ratio" entre a quantidade de bens e serviços produzidos e a quantidade ou o custo, dos recursos envolvidos e consumidos, em toda a cadeia de valor e de produção da organização.
Produto
É o resultado de um processamento para satisfazer necessidades expressas ou implícitas dos clientes. Numa orientação a uma gestão por processos de negócio, o resultado final é independente da tecnologia ou processo produtivo.

Profundidade da auditoria
Por profundidade da auditoria entende-se a maior ou menor aplicação exaustiva dos procedimentos de auditoria. A intensidade desses procedimentos determina a dimensão da amostra e/ou a percentagem dos elementos que é necessário verificar.

Programa de auditoria

Documento básico da auditoria elaborado na fase de planeamento de qualquer auditoria. O seu objetivo é definir a forma mais económica, eficiente e oportuna para alcançar os objetivos da auditoria. Deve descrever, numa ordem lógica, a natureza e o âmbito do trabalho a efetuar, a definição, para a fase de execução da auditoria, das

atribuições de cada membro da equipa de auditoria, assim como os respetivos prazos, que devem ser compatíveis não só com a complexidade, mas também com a importância de cada tarefa. Devido às suas características, o programa de auditoria:

1. Serve de base ao trabalho que conduz às conclusões de auditoria
2. Facilita a auditoria e a supervisão da execução do trabalho
3. Organiza o trabalho dos auditores de forma mais eficaz.

O programa deve conter uma descrição detalhada dos seguintes elementos:

1. Objetivo(s) da auditoria;
2. Âmbito da auditoria;
3. Técnicas e procedimentos a utilizar;
4. Critérios;
5. Etapas a cumprir e respetivos cronogramas de ação;
6. Recursos humanos necessários, especificando a qualificação exigida;
7. Matriz de planeamento.

Projeto

Um projeto é um conjunto de atividades coordenadas, com início e fim bem definidos e que é implementado por uma organização pública ou privada. O seu objetivo é alcançar objetivos específicos, possuindo uma parametrização rigorosa do tempo, custos e rendimento.

Proteção de Denunciantes

A lei de proteção dos denunciantes, Lei n.º 93/2021, de 20 de dezembro, garante que qualquer um pode denunciar infrações em empresas, mas não só. Estabelece o regime geral de proteção de denunciantes de infrações, transpondo a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União. Esta lei criou o Regime Geral de Proteção de Denunciantes de Infrações (RGPDI).

Ao abrigo desta lei, o denunciante é uma pessoa singular que denuncia ou divulga publicamente uma infração com fundamento em informações obtidas (i) no âmbito da sua atividade profissional, independentemente da natureza desta atividade e do setor em que é exercida, (ii) numa relação profissional entretanto cessada, (iii) durante o processo de recrutamento ou (iv) durante outra fase de negociação pré-contratual de uma relação profissional constituída ou não constituída. É considerado denunciante a pessoa singular que denuncie uma infração com fundamento em informações obtidas no âmbito da sua atividade profissional, independentemente da sua natureza e do setor em que a mesma é exercida.

Provas de auditoria

As provas de auditoria são todas as informações que fundamentam as opiniões, conclusões e recomendações apresentadas pelo auditor no relatório final. Elas devem ser:

– **Adequadas**: devem ser suficientes tanto ao nível quantitativo (ou seja, suficientes para alcançar os resultados da auditoria) como qualitativo (devem possuir a imparcialidade necessária para incutir um sentimento de confiança na sua fiabilidade);

– **Pertinentes**: devem ser relevantes para os objetivos definidos para a auditoria;
– **Razoáveis**: devem ser económicas, ou seja, o custo tido durante a sua obtenção deve ser proporcional ao resultado pretendido pelo auditor.

Q

Quadro de Gestão de Risco
A totalidade das estruturas, metodologia, procedimentos e definições que uma organização escolheu utilizar para implementar os seus processos de gestão do risco.

Qualidade Total
Conceito de gestão que se baseia na cultura de melhoria contínua, na melhoria do relacionamento com clientes e fornecedores, na excelência dos processos, no envolvimento dos trabalhadores a todos os níveis e numa orientação clara para o mercado.

R

Razoabilidade
Atributo da informação que é "económica", ou seja, o custo com a sua obtenção é proporcional ao resultado que o auditor procura atingir.

Recomendações de auditoria
Todas as medidas corretivas identificadas pelo auditor, que se destinam a corrigir qualquer tipo de deficiência detetado durante a auditoria.

Recursos de auditoria contratados
Refere-se à contratação de pessoas especializadas em auditoria, para executar projetos específicos de auditoria interna, geralmente sob a figura de prestador de serviços. Nesta situação, estas pessoas não fazem parte do mapa de pessoal da organização nem dependem hierarquicamente dela, visto não serem seus funcionários.

Reengenharia
Processo que consiste na redefinição radical dos processos utilizados tendo em vista a obtenção de melhorias significativas ao nível do seu funcionamento. Deve possuir também um impacto nos custos desses processos, nos seus tempos de execução e nos serviços por eles prestados.

Registo do risco

O registo de risco é uma lista que identifica os riscos e que possui os detalhes descritivos completos das referências cruzadas relativamente a esses riscos. É elaborado após terem sido identificados os riscos organizacionais.

Regulamento ou estatuto de auditoria

O regulamento ou estatuto de auditoria interna é um documento formal que orienta a atividade de auditoria interna, através da definição do seu objetivo, autoridade e responsabilidade. Além destes aspetos, o documento deve:

1. Definir o posicionamento da função auditoria interna no âmbito da organização;
2. Autorizar e garantir que a auditoria interna tem acesso a todos os registos pessoais e propriedades físicas relevantes para a concretização dos objetivos da auditoria;
3. Definir o âmbito das atividades de auditoria interna.

Relatório de auditoria

Documento que descreve formalmente a forma como se desenvolveu o trabalho de auditoria e onde é emitida, de forma clara, concisa e exata, uma opinião de auditoria acerca dos resultados alcançados pelo auditor. Este relatório deve integrar, sempre que for caso disso, a resposta e as observações dos responsáveis, assim como as conclusões e recomendações elaboradas pelo auditor.

Relevância / Materialidade

A relevância ou materialidade em auditoria é a capacidade que uma determinada informação possui para influenciar as decisões daqueles a quem se destina, auxiliando-os a avaliar os acontecimentos passados, presentes e futuros ou a confirmar e/ou corrigir essas avaliações. Ela é normalmente definida em função do seu valor monetário, mas a natureza e/ou as características próprias de um determinado elemento ou de um determinado grupo de elementos podem tornar um assunto relevante.

Responsabilidade financeira
É a obrigação de prestar contas decorrente de uma responsabilidade que tenha sido conferida. Pressupõe a existência de pelo menos duas partes: uma que confere a responsabilidade e outra que a aceita, com o compromisso de relatar a forma pela qual tenha sido executada.

Responsabilidade Social das Empresas (RSE)
Ver *CSR – Corporate Social Responsability Directive*

Responsável financeiro ou Diretor Financeiro
O responsável financeiro é aquele que efetivamente administra os bens e os recursos públicos colocados à disposição de uma Organização. Em organizações maiores e mais estruturadas designa-se por Diretor Financeiro. Por este motivo, deve assumir sempre a responsabilidade de prestar contas relativamente a essa gestão.

RBC – *Responsible Business Conduct*
Ver *CSR – Corporate Social Responsability Directive*

Resposta ao risco
Forma como a organização opta por gerir os riscos organizacionais. Existem vários tipos de resposta ao risco como, por exemplo, tolerar o risco, tratá-lo, procurando reduzir o seu impacto ou probabilidade, transferir o risco ou terminar a atividade que o origina. Os controlos internos são uma das formas de tratar o risco.

Resultado
Produtos, efeitos ou impactos (esperados ou não, positivos e/ou negativos) de uma intervenção.

Risco
Numa organização, o risco relaciona-se com a probabilidade que um acontecimento tem de ocorrer e com o impacto negativo que poderá ter ao nível do alcançar dos objetivos organizacionais. Por este motivo, o risco é medido a dois níveis: o do seu impacto nas atividades e o da sua probabilidade de vir ou não a ocorrer.

Risco de auditoria
O risco de auditoria é o risco relacionado com a hipótese de o auditor poder não detetar um erro ou fraude durante a realização do seu trabalho de auditoria e que ele assume como sendo aceitável, visto não colocar em causa a validade das suas conclusões.

Risco de deteção
Risco de o auditor não detetar um erro, irregularidade ou fraude.

Risco do sistema de controlo interno
Grau de risco que um determinado sistema de controlo interno representa face ao estudo que o auditor lhe fez.

Risco inerente
O risco inerente é o risco que pode surgir sempre que uma organização não implementa as medidas necessárias para limitar o impacto e reduzir a probabilidade dos riscos identificados. Assim, ele é inerente a todas as organizações que não tomam medidas para o combater.

Risco residual
O risco residual, contrariamente ao risco inerente, é todo o risco que persiste mesmo depois de terem sido tomadas as medidas e ações necessárias para combater o impacto e a probabilidade dos riscos identificados. É o risco que permanece após a gestão tomar todas as medidas necessárias para lhe responder, isto porque nunca é possível eliminar completamente o risco.

S

Segregação de funções
Princípio básico de qualquer sistema de controlo interno que se relaciona diretamente com a sua eficácia. Consiste na separação de funções entre pessoas diferentes, especialmente as funções que se relacionam com a autorização, execução, controlo e contabilização das operações ou atividades. Desta forma, é possível reduzir o risco de erros ou de esses erros não virem a ser detetados, uma vez que ninguém, nem individualmente nem inserido numa equipa, controla a totalidade das principais fases do processo (autorização, implementação, registo e revisão) das operações organizacionais.

Seguimento (Follow-up)
Análise e avaliação sistemática das medidas implementadas pela organização auditada em resposta às conclusões e recomendações apresentadas no relatório de auditoria. O seguimento é realizado após um determinado período de tempo e permite verificar que medidas foram tomadas efetivamente pela organização.

Sindicância
Procedimento destinado a uma averiguação geral acerca do funcionamento de um serviço ou organismo.

Sinergia
Sinergia significa que, por vezes, é mais eficaz realizar duas atividades em conjunto do que em separado, visto que as duas atividades se potenciam uma à outra, aproveitando-se, assim, as complementaridades existentes entre ambas. Normalmente, a soma de duas atividades em conjunto é maior do que a soma dessas atividades em separado.

Síntese das observações (conclusões)
É o resumo das observações e conclusões apresentadas no relatório de auditoria que permite que todos os interessados tenham acesso aos factos essenciais apurados no decorrer do processo de realização da auditoria.

Sistema
O conjunto de procedimentos, processos, métodos, rotinas, elementos e técnicas que se inter-relacionam com o objetivo de alcançar um determinado resultado. Inclui não só as informações recebidas, mas também, as operações realizadas, os recursos empregues para executar essas operações, os resultados alcançados e os seus impactos no exterior. Por outro lado, inclui a organização que orienta todos estes elementos para garantir o alcançar dos resultados esperados.

Sistema de controlo administrativo
Sistema de controlo relacionado com a definição de estratégias, políticas e objetivos da organização por parte dos seus responsáveis. Inclui o controlo hierárquico e o controlo de procedimentos e os registos relacionados com o processo de tomada de decisão.

Sistema de controlo contabilístico
Sistema constituído pelo conjunto de ações que integram o sistema geral de controlo interno e que se relaciona com todos os procedimentos de natureza contabilística.

O seu objetivo é garantir a conformidade com as regras e políticas adotadas neste setor de atividade. Além disso, pretende garantir a boa gestão dos recursos da organização e a fiabilidade dos seus registos contabilísticos e relatórios financeiros.

Sistema de controlo interno (Processo)
Sinónimo do Controlo Interno que é planeado e implementado numa Empresa/Organização. É o sistema completo de controlos de gestão, financeiro e administrativo. Inclui a estrutura organizacional e todos os métodos e procedimentos coordenados, estabelecidos pela lei e pela direção da organização para salvaguardar os seus ativos e recursos humanos, financeiros e físicos; assegurar a veracidade, fiabilidade, integridade e oportunidade dos registos contabilísticos e da respetiva informação financeira; prevenir e detetar fraudes e erros, atitudes de desperdício, abusos ou práticas antieconómicas ou corruptas e outros atos ilegais; produzir informação financeira fiável e rápida: cumprir as leis e regulamentos; assegurar o cumprimento das políticas de gestão adotadas e dos planos e procedimentos da organização; conduzir e executar as suas atribuições/objeto social, programas, projetos, atividades e funções de forma regular, produtiva, económica, eficiente e eficaz e produzir informação de gestão relativa aos resultados e efeitos alcançados.

Sistema de informação
Sistema automatizado, ou mesmo manual, que abrange pessoas, máquinas e/ou métodos organizados para recolher, processar, transmitir e divulgar dados que representam informação para o utilizador e/ou cliente.

Sistema de informação de gestão
É o sistema constituído pelos circuitos e meios que possibilitam a circulação e o controlo da informação estratégica, operacional ou de apoio, de suporte às atividades.

Sistema de qualidade
O sistema de qualidade é constituído não só pela estrutura organizacional, mas também pelas responsabilidades, procedimentos, processos e recursos necessários para promover e implementar na prática uma gestão pela qualidade.

Sistema Integrado Gestão Empresarial (*Enterprise Resource Planning* – ERP)

Sistema informático que integra todos os dados e processos de uma Organização num único sistema. A integração pode ser realizada numa perspetiva funcional (sistemas de: finanças, contabilidade, recursos humanos, fabrico, marketing, vendas, compras, entre outros) e/ou numa perspetiva sistémica (sistema de processamento de transações, sistemas de informações de gestão, sistemas de apoio à decisão, entre outros).

Em termos gerais, é uma plataforma de software desenvolvida para integrar os diversos departamentos de uma organização/empresa, possibilitando a informatização e o armazenamento de todas as informações do negócio.

Sistemas de gestão e de controlo interno

Estes sistemas abrangem a totalidade da organização interna, desde os sistemas de controlo administrativo e contabilístico até aos procedimentos e/ou práticas que permitem a concretização dos objetivos da organização. Incluem:

- Sistema de planeamento, que permite preparar as decisões políticas e administrativas;
- Sistema de execução, que permite que as ordens sejam transmitidas desde os órgãos de gestão superior até aos níveis inferiores da organização, com a indicação relativamente à divisão de responsabilidade;
- Sistema de controlo interno, que permite verificar, através de um conjunto de procedimentos e práticas coerentes, se a organização implementa as suas atividades e/ou operações em conformidade com os princípios do controlo interno.

Sistemas em tempo real

São os sistemas cujo processamento é imediato.

Sistemas financeiros

São os procedimentos para preparar, registar e reportar informações fiáveis relativas às transações financeiras.

Sobreposição da gestão
Existe sobreposição da gestão quando esta, com fins ilegítimos, se sobrepõe às políticas e procedimentos aprovados. Essas situações incluem a obtenção de benefícios pessoais ou a apresentação da situação financeira e/ou do estatuto de conformidade da organização, de forma melhorada em relação à sua situação real.

Stakeholders
Em português o termo é utilizado de forma traduzida como partes interessadas ou intervenientes. Aplica-se em diversas áreas como a gestão de projetos, na comunicação social (Relações Públicas) e áreas funcionais diversas. Em geral refere-se às partes interessadas que devem estar de acordo com as práticas de governação corporativa executadas pela empresa. Um *Stakeholder* é um membro dos grupos que apoia a Empresa/Organização. As partes interessadas são elementos essenciais no planeamento estratégico de uma Gestão por Processos de Negócio.

Supervisão da auditoria
A supervisão da auditoria é um requisito essencial de auditoria. Subentende não só uma liderança adequada, mas também, uma direção e um controlo a todos os níveis, de forma a adequar eficazmente as atividades e procedimentos, verificações e exames a executar com os objetivos que é necessário alcançar.

Suporte lógico de auditoria
Conjunto de software informático que se aplica à atividade de auditoria e que possibilita ao auditor a análise, de forma informática, dos dados armazenados informaticamente como, por exemplo, a totalização, classificação, estratificação, amostragem aleatória ou estatística, substituição, comparação entre conteúdos de vários arquivos e amostragem baseada em critérios. Este conjunto de software também pode ser referido como técnica de auditoria assistida informaticamente.

T

Tarefa de auditoria
A tarefa de auditoria é a análise de um tema selecionado, de forma clara, do programa de auditoria. A sua realização tem como fim alcançar determinados objetivos de auditoria.

Técnicas de auditoria
São os meios ou ferramentas utilizadas pelo auditor e que permitem que este possa vir a formar uma opinião fundamentada.

Teste analítico
Um teste analítico é a analise e ponderação de um conjunto variado de dados e informações de natureza económico-financeira. Inclui rácios, tendências e variações em relação aos anos e aos orçamentos anteriores.

A realização de um teste analítico tem como objetivo identificar questões ou saldos anormais, que necessitam de uma atenção ou investigação especial, quando comparados com os saldos ou variações que se apresentem de forma razoável ou justificável.

Teste de auditoria
Análise de um elemento previamente selecionado, com a intenção de determinar se os objetivos específicos da auditoria vão, ou não, ser alcançados.

Teste de conformidade (aderência)
É um tipo de teste que se destina a confirmar se os procedimentos e medidas de controlo interno são adequados e se o seu funcionamento, durante o período de exercício, é regular. Destina-se a verificar se os controlos chave funcionam de forma correta. Caso revelem algum tipo de deficiência, o auditor poderá ter de recorrer a verificações suplementares, como, por exemplo, a realização de testes substantivos, de forma a avaliar de forma mais precisa qual a dimensão e o alcance das deficiências detetadas.

Teste de procedimento
É um tipo de teste que tem como objetivo verificar e confirmar se a descrição dos sistemas, baseada em notas descritivas e/ou fluxogramas, feita pelo auditor, está correta. Neste sentido, é selecionada uma operação de cada tipo e o seu percurso é acompanhado em todo o sistema de processamento e controlo.

Teste substantivo
Conjunto de procedimentos de verificação utilizados para confirmar se o processamento contabilístico é o adequado, se os registos contabilísticos estão completos, são razoáveis e válidos e se a expressão financeira e o suporte documental dos saldos das diversas operações realizadas estão corretos. Podem ser realizados como complemento aos testes de conformidade.

Tipo de auditoria
Designação de uma auditoria tendo em conta o seu objeto e objetivos.

Tolerância ao risco
Nível de risco que a organização está disposta a aceitar antes de considerar implementar medidas ou ações para lidar com ele.

Trabalho de campo
O trabalho de campo é a execução prática do programa de auditoria, fase em que se aplicam os procedimentos e as técnicas constantes desse programa.

Transparência
Critério que permite verificar a medida em que os processos de decisão, relato e avaliação são abertos e/ou se encontram disponíveis para livre consulta pelo público em geral.

Trilho de auditoria ("*Audit Trail*")
Também conhecido por pista de auditoria, o trilho de auditoria é o conjunto de registos que comprovam o funcionamento do sistema. Permite reconstruir, rever e examinar as transações, desde o momento da entrada de dados até à produção dos resultados finais. Além disso, permite igualmente avaliar a utilização desse sistema e detetar e identificar utilizadores não autorizados do sistema.

U

Unidade de auditoria interna
Departamento, divisão ou equipa inserida numa organização que possui a responsabilidade de gerir a atividade de auditoria interna, através da realização de verificações e exames dos sistemas e procedimentos organizacionais, de forma a minimizar os riscos que possam ameaçar os objetivos da organização. Desta forma, essa unidade pode ajudar a organização a alcançar os seus objetivos, através de uma abordagem sistemática e disciplinada que permite potenciar a eficácia da gestão de risco e dos processos de controlo e de governação. A unidade de auditoria interna deve ser independente ao nível orgânico e hierárquico e reportar diretamente ao responsável máximo da organização. É possível, assim, garantir a sua objetividade e rigor.

V

Valor acrescentado
Os serviços de avaliação e de consultoria prestados pela auditoria acrescentam valor através da melhoria das oportunidades de concretização dos objetivos organizacionais, da identificação das melhorias operacionais e/ou da limitação dos efeitos resultantes da exposição ao risco. Visa determinar em que medida a organização alcançou o máximo benefício ao nível dos resultados alcançados, considerando os recursos disponíveis.

Valores éticos
Valores morais que possibilitam que um responsável determine a forma de comportamento apropriada. Os valores éticos devem basear-se naquilo que está "certo", o que pode significar ir para além daquilo que é exigido legalmente.

Verificação formal
A verificação formal é o exame que incide nos aspetos formais de um determinado procedimento ou documento como, por exemplo, a existência e a conformidade de uma assinatura, de um carimbo ou de uma data.

Verificação indiciária
Este procedimento de auditoria tem como objetivo identificar anomalias que indiquem a necessidade de proceder a verificações suplementares, como testes substantivos, através da análise e comparação das relações e variações das contas no tempo.

Verificações
São as evidências específicas obtidas pelo auditor a fim de satisfazer os objetivos da auditoria.

W

Whistleblower
Trata-se de uma pessoa denunciante que informa e revela informações sobre atividades de uma outra pessoa ou Empresa/Organização, que são consideradas ilegais, imorais, ilícitas, inseguras ou fraudulentas.


POLITÉCNICO
DE LISBOA
POLYTECHNIC
UNIVERSITY
OF LISBON

Fernando Rodrigues

Fernando Rodrigues é doutorado em Informática e Gestão de Empresas com especialização em Gestão por Processos de Negócio. Mestre em Modelos de Avaliação de Desempenho. Licenciado em Informática de Gestão pela UAL. É docente de carreira do ISCAL estando integrado na Área Departamental de Ciências da Informação e Comunicação (CIC), onde leciona unidades curriculares de licenciatura e mestrado.
Com um percurso militar iniciado em 1983, no posto de Tenente foi integrado em ações de Defesa Nacional na Força Aérea Portuguesa. Iniciou em 1989 a sua experiência profissional em empresas privadas nacionais e multinacionais, sempre na área dos Sistemas/Tecnologias de Informação. Foi formador no INA na Formação de Dirigentes e acompanhou dezenas de projetos aplicados por todo o país, fazendo parte de júris de avaliação no final dos cursos CAGEP, CADAP e FORGEP.
Tem a certificação CBPP® (*Certified Business Process Professional*) atribuída pela ABPMP. Para além deste livro é também coautor do BPM CBOK Version 4.0: *Association of Business Process Management Professionals International* (*Portuguese Edition*).

A decisão de fazer um Mestrado em Auditoria é sempre um desafio pessoal e profissional de enorme responsabilidade, tanto mais porque a maioria dos estudantes e profissionais que frequentam as aulas sentem que determinadas matérias têm uma elevada potencialidade de aprendizagem, torna o seu dia-a-dia mais fácil e sobretudo, acrescentam valor no mercado de trabalho.
Este é um livro de consulta e estudo obrigatório para compreensão do que significa ASITA aplicada a uma solução de auditoria que o ISCAL protocolou para ser possível assegurar as aulas práticas. Em rigor, a aposta em aprender praticando é o desejo de todos os que pretendem obter o grau de Mestre.
A definição dos trabalhos em auditoria implica adquirir conhecimentos iniciais e básicos de uma Gestão por Processos de Negócio. Compreendendo o que significam os conceitos ao nível da notação BPMN 2.0 é possível apresentar, definir, discutir, propor e acrescentar valor junto dos Clientes que anseiam e exigem explicações sucintas junto das equipas de auditoria sobre os trabalhos realizados no terreno.
A visão e comunicação interna e externa com que as empresas hoje se debatem passa por contratar profissionais certificados para efetuar transformações digitais e liderar com processos e pessoas, não com tecnologia. Este desígnio é sempre referido a todo o momento, até porque os conteúdos técnicos mais significativos e que são ministrados durante o curso noutras unidades curriculares, reforçam a importância dos sistemas de informação, embora a área financeira seja a mais densa em termos de compreensão.
Neste contexto, o livro está orientado ao que se desenvolve na UC ASITA do ISCAL e serve de apoio à matéria que decorre das aulas práticas. O leitor poderá abordar as matérias e os exercícios práticos propostos de duas formas: ordenada e sequencialmente, partindo do início, ou pesquisando diretamente e de livre vontade o que considera ser mais apropriado, aprofundando o conhecimento dos conteúdos com recurso a práticas de *Design Thinking*.
O pensar "fora da caixa" poderá melhor reproduzir o(s) problema(s) que pretende resolver e começar a sua imersão de conceitos, propondo a si próprios casos práticos que podem até vir a ser testados. Procura-se deste modo estimular a vivência em ambiente de "laboratório" tendo em vista a aplicação prática da matéria lecionada e validada perante desafios do mundo real.

Exemplos e perguntas de revisão para:
- Gerir melhor os dados e informação crítica para tomar decisões
- Aumentar o conhecimento de conceitos utilizados no mercado
- Potenciar uma aprendizagem digital a novos modelos de negócio
- Planear uma aposta profissional que garante resultados a curto prazo
- Explorar se a atividade estimula a importância das certificações

9 789893 515839

POLITÉCNICO DE LISBOA | POLYTECHNIC UNIVERSITY OF LISBON