Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

RELATÓRIO DE ESTÁGIO

ANÁLISE AOS RISCOS DE TI NO ÂMBITO DE UMA AUDITORIA FINANCEIRA

PEDRO RAFAEL VIOLANTE DE ALMEIDA

OUTUBRO - 2022

Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
RELATÓRIO DE ESTÁGIO

ANÁLISE AOS RISCOS DE TI NO ÂMBITO DE UMA AUDITORIA FINANCEIRA

PEDRO RAFAEL VIOLANTE DE ALMEIDA

ORIENTAÇÃO:

ENGª. CAROLINA CASTANHEIRA PEREIRA FERNANDES

PROF. DOUTOR JESUALDO CERQUEIRA FERNANDES

OUTUBRO – 2022

“The difficulty lies not so much in developing new ideas as in escaping from old ones.”

John Maynard Keynes

LISTA DE ABREVIATURAS

ACL - *Audit Command Language*

DS - Direção de Segurança

DSI - Direção de Sistemas de Informação

IAASB - *International Auditing and Assurance Standards Board*

ISA – *International Standard on Auditing*

ITGC – *IT General Control*

RAS – *Risk Assurance Services*

SI – Sistemas de Informação

TFM – Trabalho Final de Mestrado

TI – Tecnologias de Informação

RESUMO

Numa altura em que as empresas fazem investimentos cada vez maiores nos seus sistemas de informação, vemos um aumento da preocupação por parte das empresas de auditoria em garantir que as informações presentes nos relatórios financeiros estão corretas. Para tal, as auditorias financeiras necessitam de recorrer a especialistas de Tecnologias de Informação para obter o conforto necessário relativamente à completude e integridade das informações financeiras alvo de análise no momento da emissão da certificação legal de contas.

Dada a relevância da utilização destes especialistas para que exista uma auditoria financeira de qualidade, foi desenvolvido o presente relatório de estágio, com o objetivo de perceber a metodologia utilizada nos trabalhos de análise aos sistemas de informação de um cliente do ramo de Banca e Seguros.

Com a elaboração deste trabalho foi possível entender que existem riscos associados à utilização de sistemas de informação que tentam ser colmatados com a introdução de controlos informáticos. Estes controlos são analisados pelos especialistas de TI para que a equipa de auditoria financeira obtenha o conforto necessário para a emissão da certificação legal de contas. Foi também possível verificar que a colaboração entre as equipas de auditoria financeira e os especialistas de TI permite um aumento da qualidade dos trabalhos de auditoria.

PALAVRAS-CHAVE: Auditoria, Sistemas de Informação, risco, controlo.

ABSTRACT

At a time when companies make increasing investments in their information systems, we see an increase in the concern on the part of auditing companies to ensure that the information present in financial reports is correct. To this end, financial audits need the support of an Information Technologies specialist to obtain the necessary comfort regarding the completeness and integrity of the financial information being analyzed at the time of issuance of the legal certification of accounts.

Given the importance of using these specialists for a quality financial audit, this internship report was developed, with the aim of understanding the methodology used in the analysis of the information systems of a client in the Banking and Insurance branch.

With the elaboration of this work, it was possible to understand that there are risks associated with the use of information systems that can be overcome with the introduction of computer controls. These controls are analyzed by the IT specialists so that the financial audit team obtains the necessary comfort for the issuance of the legal certification of accounts. It was also possible to verify that the collaboration between the financial audit teams and the IT specialists allows an increase in the quality of the audit work.

ÍNDICE

AGRADECIMENTOS

Em primeiro lugar, quero agradecer ao Professor Doutor Jesualdo Fernandes pelo tempo e apoio que me disponibilizou ao longo da elaboração deste Trabalho Final de Mestrado.

Quero também fazer um agradecimento especial à minha orientadora de estágio Engenheira Carolina Fernandes por todo o apoio que me deu e por tudo o que me ensinou ao longo do estágio, e à minha *manager* Ana Matias Correia que me incentivou a realizar este relatório e contribuiu com ideias, assim como a todos os meus colegas do RAS que tão bem me acolheram na equipa.

Por último, agradecer também à minha família e amigos que estiveram sempre comigo nos momentos mais difíceis.

ANÁLISE AOS RISCOS DE TI NO ÂMBITO DE UMA AUDITORIA FINANCEIRA

Por Pedro Almeida

1. INTRODUÇÃO

Numa altura em que os avanços nas Tecnologias de Informação (TI) têm mudado completamente o ambiente de negócios de muitas empresas nas últimas duas décadas, também a profissão de auditoria tem sofrido alterações, visto que o processo de auditoria tradicional passou a necessitar muito mais de ter em consideração as novas tecnologias (Tarek et al., 2017). Apesar de todos os benefícios que a utilização de TI traz para as empresas, existem também riscos que têm de ser tidos em conta, como ataques de vírus, *hackers*, fraude, manipulação ou o acesso não autorizado a dados e informações relevantes para a empresa. Assim, é necessário que os auditores estejam cientes desses riscos na altura de planear os trabalhos, recolher evidências e emitir os relatórios de auditoria, levando à necessidade de adquirir habilidades e técnicas relacionadas às TI e incorporar esses conhecimentos nos trabalhos de auditoria (Tarek et al., 2017).

É então necessário recorrer a especialistas de TI para efetuar uma auditoria financeira de qualidade, tendo em consideração que os processos de negócio estão concentrados em componentes de TI, como sistemas ERP, aplicações internas e bases de dados, onde é necessário garantir um correto armazenamento dos dados, de forma a que estes não possam ser modificados ou acedidos de forma indevida (Barta, 2018).

O presente relatório apresenta-se como Trabalho Final de Mestrado (TFM), no âmbito do Mestrado em Gestão de Sistemas de Informação do Instituto Superior de Economia e Gestão (ISEG) da Universidade de Lisboa, para a obtenção do grau de Mestre, tendo como finalidade descrever o estágio profissional realizado na empresa PwC, no período de 1 de Outubro de 2021 a 31 de Março de 2022, inserido na equipa de *Digital Assurance* do departamento de *Risk Assurance Services* (RAS), com o objetivo de aplicar os conhecimentos obtidos durante a frequência deste mestrado, assim como compreender todo o processo a realizar para analisar os sistemas de informação (SI) relevantes para uma auditoria financeira, de modo a que a equipa de auditoria financeira

consiga obter conforto sobre os sistemas utilizados pelo cliente nas rubricas do relato financeiro relevantes para a emissão da certificação legal de contas.

Neste sentido, este trabalho encontra-se dividido em cinco capítulos. No segundo capítulo encontra-se a revisão de literatura, onde são apresentados temas sobre informação e sistemas de informação, definição de auditoria e quais as etapas de auditoria que devem ser realizadas, assim como a definição de sistemas de informação e os seus componentes. No capítulo 3 é apresentada a empresa e o departamento onde foi elaborado o estágio, assim como uma descrição geral do trabalho desempenhado. No capítulo 4 é efetuada uma explicação detalhada das funções desempenhadas ao longo do período do estágio. Por fim, no capítulo 5 são apresentadas as conclusões e limitações do trabalho efetuado.

2. REVISÃO DE LITERATURA

2.1. Informação e Sistemas de Informação

Nos últimos tempos temos verificado um grande aumento da importância dada à informação, sendo já considerada como um dos ativos mais importantes e estratégicos para qualquer empresa (Lateef & Omotayo, 2019; Leming, 2015). Segundo Lateef & Omotayo (2019) pode considerar-se como um ativo de informação um conjunto de dados estruturados, semiestruturados ou não estruturados que a empresa tem à disposição para utilizar na tentativa de alcançar os seus objetivos. Estes ativos podem ser armazenados tanto fisicamente, em registos de papel, fotografias, desenhos, entre outros, como em sistemas computadorizados.

A informação está presente em quase tudo o que fazemos, sendo utilizada na tomada de decisões, para permitir a entrega de programas, produtos e serviços relevantes para a empresa, tal como registar o desempenho financeiro e os objetivos da empresa (Leming, 2015).

Como a informação é tão importante, há riscos que devem ser tidos em conta, e que estão presentes em vários momentos, como na receção, criação, armazenamento, utilização, consulta, transmissão e partilha da informação. Estes riscos podem levar a que exista partilha de informação confidencial, falhas nos servidores ou problemas técnicos que impeçam a sua consulta ou que destruam informação relevante (Lateef & Omotayo, 2019). Risco pode ser definido como uma condição onde existe exposição a adversidades ou a possibilidade de ocorrer um desvio face ao resultado esperado ou desejado (Gallati, 2003).

Aliada à cada vez maior importância dada à informação está o investimento bastante elevado que é realizado pelas empresas na melhoria ou aquisição de novas aplicações de negócio, de forma que consigam diferenciar-se das restantes empresas do mercado e conseguindo melhorar a sua *performance* ao utilizar as capacidades computacionais disponíveis (Bellino et al., 2007).

Segundo Coates et al. (2013) a utilização de aplicações de negócio é muito importante no processo de negócio das empresas, e como tal, não podem ser separadas dos restantes processos que suportam. Normalmente, são classificadas em dois tipos:

aplicações transacionais, e aplicações de suporte. As aplicações transacionais têm como principal função o registo e processamento de transações comerciais, como é o caso de aplicações de processamento de pedidos de vendas e de registo de transações de débitos e créditos (Coates et al., 2013). Já as aplicações de suporte, tal como o nome indica, dão suporte às atividades desenvolvidas pelas empresas, de forma a facilitar as mesmas, sendo que normalmente não efetuam o processamento das transações. Alguns exemplos destas aplicações incluem programas de e-mail e *software* de processamento de imagem de documentos (Bellino et al., 2007; Coates et al., 2013).

Segundo Tarek et al. (2017) as empresas utilizam cada vez mais as TI para fazer a gestão das suas atividades de dia-a-dia, fazendo uso da *internet*, de sistemas contabilísticos de tempo real, comércio eletrónico e sites onde é efetuada a divulgação de informação financeira, acrescentando ainda que atualmente todos os processos contabilísticos são efetuados com recurso a computadores e a *softwares* de contabilidade.

Naturalmente que aliada à utilização destas tecnologias surge a ameaça à segurança da informação da organização (Dai & Vasarhelyi, 2016), dado que a informação gerada está presente em diversas camadas, onde estão presentes os dados, *hardware*, *software*, instalações e segurança física, utilizadores, acessos, autenticação e comunicações *web*. Estas camadas vão condicionar a segurança e a fiabilidade dos dados, podendo assim afetar de forma séria a continuidade do negócio ou mesmo a sobrevivência da empresa nos casos em que existe uma forte dependência da utilização de sistemas de informação. Nestes casos a empresa pode mesmo chegar à falência se os *stakeholders*[1] não tiverem confiança nos sistemas utilizados (Pedro, n.d.).

Portanto, a utilização deste tipo de sistemas pode trazer riscos para a empresa, que podem ter um impacto negativo nas informações financeiras da empresa ao não garantir a integridade, completude e disponibilidade da informação financeira do negócio (Bellino et al., 2007).

[1] Grupo de indivíduos que de alguma forma se relacionam com uma empresa, fornecendo recursos/contribuições para a empresa e esperando em troca ver os seus interesses satisfeitos (Hill & Jones, 1992).

2.2. Auditoria

Todos os riscos mencionados no ponto anterior, podem levar a que exista adulteração da informação presente nos relatórios financeiros das empresas, pelo que é importante que se realizem auditorias que possam fornecer confiança aos intervenientes do mercado de capitais, de modo que o mercado funcione de forma eficiente. É bastante reconhecido que a auditoria tem uma grande importância para que exista uma operação eficiente dos mercados de capitais. Se não existir uma auditoria de alta qualidade, o mercado de capitais funcionaria de forma ineficiente e com um custo de capital muito mais elevado (Kilgore et al., 2011).

O processo de auditoria pode ser definido como uma inspeção formal a uma organização, onde se verifica se um conjunto de diretrizes são aplicadas e cumpridas, os seus registos precisos e se as metas de eficiência e eficácia propostas são alcançadas (ISACA, 2015). Portanto, o objetivo principal da realização de uma auditoria é verificar se as demonstrações financeiras estão livres de distorção, que pode surgir devido a fraude ou a erros, e se são preparadas de acordo com uma estrutura de relatório adequada (IAASB, 2009a).

Para fazer um correto trabalho de auditoria existem várias etapas que devem ser cumpridas, assim como *International Standard on Auditing* (ISA) que devem ser tidas em consideração (IAASB, 2009a). ISAs são padrões profissionais utilizados na realização de auditorias financeiras, emitidos pelo *International Auditing and Assurance Standards Board* (IAASB), com o objetivo de melhorar e uniformizar os trabalhos de auditoria, de forma a fortalecer a confiança do público em geral nos trabalhos desenvolvidos pelas empresas de auditoria (Haapamäki & Sihvonen, 2019).

A primeira etapa é a fase de planeamento, onde é necessário estabelecer a estratégia que vai ser tomada no processo de auditoria, definindo qual o âmbito, o período temporal e os objetivos da auditoria, bem como considerar resultados de trabalhos de auditoria anteriores que possam ser relevantes ter em consideração na preparação dos trabalhos (IAASB, 2009c). A fase de planeamento é um processo interativo e contínuo que começa muitas vezes logo a seguir à conclusão dos trabalhos de auditoria anteriores e se desenrola até ao final do presente trabalho de auditoria. No entanto existem certas atividades que têm obrigatoriamente de ser realizadas no início dos trabalhos, como é o caso da avaliação

de risco, compreensão de questões legais, determinação da materialidade e o envolvimento de especialistas (IAASB, 2009c). A materialidade depende do julgamento profissional do auditor, devendo ter em consideração o tamanho e a natureza da omissão ou distorção encontrada nas demonstrações financeiras. Essas distorções ou omissões serão consideradas relevantes se influenciarem as decisões tomadas com base nas demonstrações financeiras (IAASB, 2009d; Barta, 2018).

Os principais benefícios desta fase dos trabalhos de auditoria é a ajuda que dá ao auditor em dedicar o seu foco às áreas mais importantes, organizar de forma adequada o trabalho a realizar de forma que este seja executado eficaz e eficientemente, auxiliando na seleção dos membros de equipa mais apropriados, assim como na determinação da necessidade de recurso a especialistas (IAASB, 2009c).

Tanto esta etapa como todas as outras devem seguir certos requisitos exigidos ao auditor, entre os quais requisitos éticos, que garantam integridade, objetividade, competência profissional, confidencialidade e comportamento profissional. É também necessário garantir que o auditor planeia e executa os trabalhos de auditoria com ceticismo profissional e exercendo sempre o seu julgamento profissional, assim como obter as evidências apropriadas e suficientes que permitam ao auditor tirar conclusões razoáveis de forma a emitir uma opinião (IAASB, 2009a).

Na obtenção de tais evidências é necessário ter em atenção se as mesmas são relevantes e confiáveis para o propósito da auditoria, tendo em atenção se cumprem os critérios de exatidão e integridade e confirmando se são suficientemente precisas para serem utilizadas nos trabalhos (IAASB, 2009e). É também necessário fazer a seleção dos itens que devem ser testados, existindo três meios disponíveis para selecionar a quantidade de itens a testar. Se se tratar de uma população pequena ou existir um risco elevado que não possa ser mitigado com outras evidências talvez faça sentido analisar a totalidade da população (IAASB, 2009e). Segundo a ISA 530 população define-se como o conjunto de dados a considerar na altura de selecionar uma amostra que permita ao auditor tirar conclusões (IAASB, 2009f).

No entanto, esta forma de teste pode não ser a mais eficaz, estando, portanto, disponível a possibilidade de testar apenas itens específicos ou testar uma amostra da população (IAASB, 2009e). Para qualquer das formas de teste escolhidas, deve-se avaliar

qual ou quais os procedimentos a efetuar para fazer a análise das evidências, que incluem inspeção, observação, confirmação, *reperformance*, recálculo e realização de procedimentos analíticos. Outro procedimento é o questionário (*inquiry*) que não deve ser utilizado de forma isolada, mas sim como forma de complemento aos outros procedimentos (IAASB, 2009f).

Após obtenção das evidências, determinação dos itens a testar e do procedimento de teste a realizar, é necessário fazer a correta documentação dos trabalhos de auditoria efetuados, de forma a que esta seja suficiente para permitir a um auditor que não tenha tido contacto com os trabalhos de auditoria realizados entender a natureza, período em âmbito e extensão dos trabalhos realizados, as evidências e resultados obtidos e questões que tenham surgido durante o decorrer dos trabalhos, bem como os julgamentos profissionais efetuados para chegar às conclusões do trabalho e as respetivas conclusões (IAASB, 2009b).

É também importante deixar documentado quais as características dos itens ou assuntos que foram testados, quem executou os trabalhos e a data em que os mesmos foram concluídos, assim como quem efetuou a revisão dos trabalhos e a data em que a revisão ocorreu. Devem também ser documentadas as discussões tidas com a administração ou outros responsáveis da entidade auditada sobre os pontos significativos que foram encontrados no decorrer dos trabalhos (IAASB, 2009b).

Por vezes pode ser necessária a utilização de auditores especialistas em campos que não estejam ligados a contabilidade ou auditoria financeira. Segundo a ISA 620, um auditor especialista é um indivíduo ou organização que detém experiência em áreas que não sejam contabilidade ou auditoria cujo trabalho por ele desenvolvido é utilizado para obter evidências apropriadas e suficientes dessa área. Este pode ser um funcionário interno da firma de auditoria ou um especialista externo (IAASB, 2009g).

Um exemplo de especialistas que podem ser necessários nos trabalhos de auditoria são os especialistas de TI, devendo então ser constituídas equipas de auditoria compostas por auditores financeiros e especialistas de TI que trabalhem em conjunto para alcançar os objetivos identificados e obter conclusões apropriadas (Estep, 2021).

Na era de digitalização em que estamos a viver, não é possível realizar uma auditoria financeira sem recorrer a especialistas de TI, tendo em conta o aumento da

utilização de SI por parte das empresas. Esta utilização de SI permite a redução de erros humanos, assim como a melhoria dos processos de negócio, mas introduz nas empresas riscos que devem ser colmatados com a implementação de controlos que permitam a proteção das informações relevantes para o relato financeiro. Desta forma, é cada vez mais necessário que os especialistas de TI efetuem testes aos ambientes tecnológicos das empresas, de forma a garantir que os dados financeiros estão protegidos e que as vulnerabilidades presentes nos sistemas não podem ser exploradas para a prática de fraudes (Barta, 2018).

A utilização destes especialistas de TI numa auditoria financeira passa também pelo conhecimento por eles obtido quer em trabalhos de auditoria, quer em trabalhos de consultoria. É bastante benéfico para as empresas de auditoria ter foco também nos serviços de consultoria, uma vez que os especialistas levam para os trabalhos de auditoria o conhecimento que vão adquirindo ao desempenhar trabalhos de consultoria, melhorando assim a qualidade do trabalho efetuado (Estep, 2021).

Portanto, uma identidade de equipa forte entre os auditores e os especialistas de TI traz benefícios para os trabalhos de auditoria, pois assim existe uma maior cooperação e partilha de informação que aumentam a qualidade da auditoria que está a ser realizada (Estep, 2021), de forma a ser possível garantir a disponibilidade, confidencialidade e integridade da informação (Sayana, 2002).

2.3. Envolvimento de especialista de TI na Auditoria Financeira

Para uma correta auditoria aos sistemas de informação relevantes na ótica da auditoria financeira é importante começar por obter um entendimento do ambiente de TI da empresa, percebendo quais as aplicações, infraestrutura de TI (rede, sistemas operativos e bases de dados), processos de TI e funcionários envolvidos nesses processos que a organização tem ao dispor para dar suporte à operação de negócio (IAASB, 2019). Para além disto é também necessário identificar quais os principais controlos que a organização tem implementados (IAASB, 2019).

É importante obter este entendimento uma vez que existem riscos associados à utilização das tecnologias de informação e que podem levar a que o processamento dos dados ocorra de forma imprecisa por existirem acessos indevidos, que podem resultar na

adulteração ou destruição de dados, obtenção de privilégios desadequados, alterações indevidas dos dados mestre, ocorrência de falhas nas alterações ou atualizações das aplicações ou a perda de dados ou indisponibilidade de acesso aos mesmos conforme seja necessário (IAASB, 2019).

Assim, para conseguirem mitigar esses riscos e proteger os seus ativos, clientes e parceiros e preservar a sua reputação e confiança, as empresas introduzem controlos de TI nos seus processos. Estes permitem a existência de automação dos controlos de negócio de forma a suportar a sua gestão e fornecer controlos gerais sobre as principais infraestruturas de TI utilizadas (Richards et al., 2005).

Quando falamos de controlos, estes podem assumir a forma de políticas, procedimentos, práticas ou estruturas organizacionais que são pensadas e desenvolvidas de forma a permitir que exista uma garantia razoável de que os objetivos da organização serão alcançados e que acontecimentos indesejáveis serão evitados ou detetados e corrigidos de forma atempada, tentando assim reduzir ou mitigar ao máximo esses riscos (ISACA, 2015).

A introdução dos controlos de TI é efetuada sempre com base nos riscos que são identificados e que a gestão tem como objetivo mitigar. Conforme esses riscos forem sendo identificados, a empresa pode tomar a decisão de aceitar o risco e, como tal, não efetuar nenhuma ação, ou decidir que é necessário desenvolver e implementar um conjunto de controlos específicos, de forma a dar a resposta mais adequada que ajude a mitigar esses riscos (Richards et al., 2005)

Portanto, é necessário verificar a eficácia dos controlos implementados, sejam eles controlos aplicacionais ou controlos gerais informáticos (*IT General Controls* (ITGC)) (Bellino et al., 2007).

Os controlos aplicacionais podem ser implementados pelas empresas aos processos de negócio de forma individual, de forma a obter um controlo sobre a edição de dados, segregação de funções, *logs* de transações e relatórios de erros. Os principais objetivos destes controlos é garantir que os dados são introduzidos nas aplicações e bases de dados de forma precisa, completa e por utilizadores autorizados, o seu processamento é realizado conforme o pretendido, as exportações de informação e dados são igualmente

precisas e completas, e que se mantém um registo do processo efetuado pelos dados desde a sua entrada, armazenamento e exportação (Bellino et al., 2007; Richards et al., 2005).

De entre os controlos aplicacionais que existem, Bellino et al. (2007) e Richards et al. (2005) destacam os seguintes:

- *Input Control*: Usados essencialmente para verificar de que forma foram inseridos os dados na aplicação, ou seja, se foi de forma automática, via *interface*, ou por algum elemento da equipa ou parceiro de negócio, de modo a garantir que os dados são introduzidos cumprindo os parâmetros definidos e confirmando a integridade dos dados;
- *Processing Control*: Controlos que visam garantir que o processamento dos dados se realiza de forma completa, precisa e devidamente autorizada;
- *Output Controls*: Controlos que verificam o que é feito com os dados, comparando o *output* final com o resultado esperado;
- *Integrity Controls*: Monitorizam os dados que foram armazenados e são processados, de modo a garantir que continuam corretos e consistentes com o introduzido;
- *Management Trail*: Estes controlos guardam um histórico do processamento efetuado aos dados, que normalmente são chamados de "trilha de auditoria", permitindo à gestão identificar e rastrear as transações e eventos efetuados desde a sua origem até ao *output*.

Os controlos aplicacionais podem também ser classificados como detetivos ou preventivos. Os controlos preventivos são utilizados pelas organizações para evitar que ocorram erros dentro das aplicações, como por exemplo, fazendo uma validação dos dados no momento em que são introduzidos de forma a verificar se os dados são consistentes e válidos. Já os controlos detetivos são utilizados para detetar erros que possam ter ocorrido, através de uma lógica de programa predefinida, como por exemplo, detetar a existência de diferenças entre o preço registado da fatura de um fornecedor e o preço real do pedido de compra (Bellino et al., 2007).

É também importante ter em consideração e analisar os ITGCs implementados pela organização. Podemos definir ITGCs como sendo controlos que são aplicados de forma geral aos processos de TI das organizações, de forma a garantir que serviços, aplicações, bases de dados, sistemas operativos e infraestrutura de TI dão um suporte adequado às aplicações e processos utilizados pelo negócio, garantindo uma operação contínua e adequada do ambiente de TI (Chan & Lao, 2009; IAASB, 2019). Segundo Chan & Lao (2009), estes podem ser divididos em quatro domínios:

1. *Program Development*: Neste domínio é feita a identificação de soluções automatizadas que podem vir a ser implementadas pela organização, bem como a elaboração dos requisitos, testes, aprovações, supervisão e avaliação dos riscos que um projeto de aquisição ou implementação de novas aplicações pode trazer.
2. *Program Changes*: Para uma correta gestão das aplicações é necessário gerir as constantes mudanças que são necessárias de realizar, assim como a implementação de novas versões do sistema.
3. *Access to Programs and Data*: Os controlos que estão associados ao acesso a programas e dados ganham maior importância quando a conectividade interna e externa da organização aumenta, levando a riscos como ataques informáticos, *software* malicioso ou outras tentativas de acessos indevidos por parte de colaboradores ou ex-colaboradores, que podem pôr em causa a integridade dos dados e dos programas.
4. *Computer Operations*: O objetivo por detrás dos controlos deste domínio é garantir que as operações diárias e a entrega diária de serviços de informação acontecem, definindo as operações que devem ser tomadas como a aquisição, instalação, configuração, integração e manutenção da infraestrutura de TI.

Portanto, os principais objetivos da utilização de ITGCs é garantir que se realiza um correto desenvolvimento e implementação das aplicações e que são cumpridos os requisitos de integridade dos arquivos, dos dados e das operações realizadas com auxílio de um computador (ISACA, 2001).

Para melhor compreender a utilidade dos ITGCs, a IAASB (2019) na sua ISA 315 descreve alguns exemplos de ITGCs que podem ser implementados pelas empresas, sendo alguns deles:

- Autenticação: Controlos que verificam as credenciais de *login* do utilizador para garantir que acede apenas a aplicações ou outros sistemas de TI utilizando as suas próprias credenciais válidas;
- Autorização: Controlos que permitem a existência de segregação de funções ao permitir que os utilizadores acedam apenas a informações necessárias para realizar as suas funções;
- Acessos privilegiados: Controlos que permitem monitorizar os acessos efetuados por utilizadores administrativos ou com poderes privilegiados;
- Acessos físicos: Controlos que validam/monitorizam os acessos físicos ao *Data Center* e ao *hardware*;
- Processo de gestão de alterações: Controlos que estão presentes no processo de gestão de alterações para projetar, programar, testar e migrar as alterações efetuadas para o ambiente de produção;
- *Backup and recovery*: Controlos que garantem que são efetuados *backups* dos dados de *reports* financeiros de acordo com o planeado e que esses dados podem ser recuperados quando necessário.

É então importante que se garanta um elevado grau de confiança nestes controlos, que está dependente diretamente da forma como os mesmos são desenhados e da sua eficácia. Se os ITGCs não forem corretamente implementados ou não estiverem a operar de forma eficaz, a organização não pode ter confiança nos controlos realizados para fazer a gestão dos riscos que estão inerentes à sua operação (Bellino et al., 2007).

Após a análise aos controlos da organização, assim como ao ambiente de TI é necessário reportar as principais conclusões do trabalho de auditoria, assim como validar os problemas encontrados com o cliente e desenvolver planos de ação para a sua correção (Davis et al., 2020).

No que diz respeito ao contributo que a auditoria pode trazer para a organização auditada, segundo Davis et al. (2020), só existe um verdadeiro contributo da auditoria quando é efetuada a resolução dos problemas que são encontrados ao longo dos trabalhos, para que desta forma as organizações consigam melhorar o estado dos seus controlos de SI. Através dos relatórios efetuados pela auditoria, os responsáveis das organizações ficam mais conscientes dos problemas que possam existir, e dessa forma passar para a sua resolução. O ideal é que exista uma atitude de colaboração e de cooperação entre as organizações e as equipas de auditoria de SI para que, de forma aberta e positiva, se possa analisar os problemas encontrados e traçar possíveis ações de melhoria. Outro contributo identificado por estes autores é que através da apresentação dos relatórios de auditoria aos responsáveis das organizações é possível conquistar a atenção dos mesmos, o que facilita a obtenção de recursos que são necessários para a resolução desses problemas (Davis et al., 2020).

3. APRESENTAÇÃO DA EMPRESA

O estágio ao qual o presente relatório se refere foi efetuado na empresa PricewaterhouseCoopers & Associados - Sociedade de Revisores Oficiais de Contas, Lda, também designada de PwC-SROC. A PwC-SROC, pertence a uma rede de empresas constituída por firmas independentes entre si, que estão presentes em 156 países contando com mais de 295.000 colaboradores que prestam serviços nas áreas de auditoria, consultoria e fiscalidade (PwC, 2021). A PwC faz parte de um grupo de quatro empresas (PwC, Deloitte, EY e KPMG) denominadas *Big 4*, que são consideradas as quatro maiores empresas de consultoria e auditoria do mundo (Francis & Yu, 2009). A PwC apresentou, a nível mundial, no exercício de 2021 cerca de 45 mil milhões de dólares de receita bruta (PwC, 2021).

A PwC em Portugal, Angola e Cabo Verde conta atualmente com 48 *partners*, dos quais 31 se encontram no escritório de Lisboa, 11 no Porto e 6 em Luanda, e mais de 1.800 colaboradores permanentes distribuídos pelos escritórios de Lisboa, Porto, Luanda e Praia.

O estágio foi desenvolvido no departamento de *Risk Assurance Services* (RAS), na equipa de *Digital Assurance*. Para além de dar apoio à equipa de auditoria financeira, o RAS disponibiliza mais serviços, contando ao todo com 8 serviços, entre os quais Auditoria Interna, *Cybersecurity*, Privacidade e Proteção de Dados, *Data Assurance*, *Risk Management & Compliance*, *Third Party Assurance*, *Enterprise Systems Risk and Controls* e *Process Assurance*, estando alguns destes serviços interligados.

Um dos principais objetivos do departamento é prestar auxílio à equipa de auditoria financeira da PwC fornecendo conforto sobre o ambiente de TI e o estado dos controlos de TI existentes na organização auditada, de forma que a equipa de auditoria financeira consiga perceber se tem conforto nos documentos de relato financeiro que são gerados pelos sistemas informáticos do cliente, trabalhando assim em sintonia com as equipas de auditoria financeira ao longo de todo o processo de auditoria.

O estágio teve por base o acompanhamento da realização dos trabalhos de auditoria a 5 empresas do ramo de banca e seguros, tendo o aluno acompanhado todos os processos de auditoria, desde o seu início até à sua conclusão. No entanto, neste relatório apenas

será abordado o trabalho de auditoria a uma empresa no setor da banca, por se ter revelado o projeto mais complexo e ambicioso.

O objetivo do trabalho realizado consistiu na realização de procedimentos de teste e análise aos controlos gerais informáticos e a utilização de outros procedimentos de auditoria de TI para suporte da Equipa de Auditoria Financeira na avaliação do risco de distorção material das contas no âmbito do processo de relato financeiro da entidade.

Para a realização deste trabalho de auditoria, duas equipas da PwC trabalham em conjunto, nomeadamente a Equipa de Auditoria Financeira e a Equipa de especialistas em Sistemas de Informação (equipa do RAS), para que seja possível alcançar os objetivos traçados para o projeto.

Para desenvolver os trabalhos de auditoria deste cliente, a auditoria aos SI foi efetuada seguindo as seguintes etapas:

- A avaliação dos riscos da distorção material das contas dos subprocessos relevantes;
- O levantamento das dependências de TI relevantes e, com base nas dependências identificadas, definição do âmbito aplicacional e da estratégia de testes por forma a testar as dependências de TI;
- A execução de testes de desenho e operacionalidade dos controlos planeados;
- A avaliação e execução de procedimentos adicionais de auditoria, por forma a validar se o risco inerente aos controlos identificados se encontrava mitigado; e
- Reporte e conclusão do trabalho.

Para a elaboração deste trabalho foi constituída uma equipa com quatro elementos pertencentes ao RAS, entre os quais um *Assistant Associate*, uma *Senior Associate*, uma *Senior Manager* e um *Partner*. Durante o estágio o aluno teve a designação de *Assistant Associate*, tendo trabalhado mais diretamente com a *Senior Associate* do trabalho, que desempenhou também a função de orientadora de estágio.

4. DETALHE DOS TRABALHOS REALIZADOS

4.1. Formação

O estágio teve início com a frequência por parte do aluno de sessões de formação obrigatórias, que estiveram divididas em três fases:

- A primeira fase teve por base temas relacionados com boas práticas comportamentais, éticas e morais, onde foram abordados temas como ceticismo profissional, independência, confidencialidade e ética.
- Numa segunda fase foram realizadas formações *online*, também denominadas de *e-learnings*, complementadas por explicações efetuadas pelos formadores sobre temas mais relacionados com auditoria, onde foi explicado a metodologia e as ferramentas utilizadas pela empresa.
- Por fim, numa terceira fase, a formação foi mais direcionada para o departamento do RAS, onde foi explicada a metodologia a utilizar nos projetos de auditoria em que os elementos do RAS são envolvidos como especialistas de TI, assim como alguns tópicos fundamentais para a realização do projeto.

Adicionalmente a esta formação inicial, a PwC fornece uma plataforma de *e-learnings* onde é possível realizar formações mais específicas sempre que surgem dúvidas ao longo do projeto, ou é necessário aprofundar determinados conhecimentos. Existe também uma plataforma que funciona como guia de auditoria, onde é possível consultar várias informações relacionadas com a metodologia utilizada pela empresa nos seus trabalhos de auditoria.

4.2. Início dos trabalhos

Após a formação inicial, deu-se início ao projeto de auditoria com uma "passagem de pasta" sobre o cliente, de forma a ser possível a nova equipa ficar a conhecer os trabalhos efetuados nos anos anteriores pela equipa anterior. Nesta "passagem de pasta" foram disponibilizados à nova equipa os entendimentos obtidos nos anos anteriores, bem como os trabalhos realizados, de forma a compreender o trabalho previamente realizado.

Para tal, a anterior equipa preparou apresentações e vídeos explicativos, que simplificaram e facilitaram bastante o processo de conhecer o cliente e em especial o ambiente de TI do cliente.

Uma vez adquirido o conhecimento existente sobre o cliente, deu-se início à primeira fase dos trabalhos de auditoria, com o planeamento das atividades a serem desenvolvidas. Durante a fase de planeamento foram realizadas reuniões internas entre os elementos da equipa do RAS, mas também com os elementos da equipa de Auditoria Financeira, de forma a delinear os planos de ação para os trabalhos de auditoria, onde ficou definido quais as aplicações em âmbito, os domínios de ITGC a serem testados e quais as Dependências de TI em que era necessário realizar testes aos controlos.

Posteriormente, foram realizadas reuniões de *kick-off* com a Direção de Sistemas de Informação (DSI) e a Direção de Segurança (DS) do cliente, de forma a alinhar o âmbito dos trabalhos, nomeadamente os prazos e o parque aplicacional em âmbito de auditoria. Após as reuniões era responsabilidade do aluno realizar as minutas da reunião para que nenhuma informação relevante fosse perdida.

Feito o alinhamento dos trabalhos e discutidas as datas relevantes a ter em consideração, seguiu-se a fase de preparação e envio dos pedidos de informação e evidências necessárias. Para tal foi efetuado um levantamento das informações necessárias para se obter um bom entendimento do ambiente de TI do cliente, assim como das evidências necessárias para dar resposta às análises de controlos a serem efetuadas nos vários domínios em âmbito do trabalho. Com base nesse levantamento, foi criada uma lista de pedidos que podem ser divididos nas seguintes categorias:

- Pedidos gerais, como listagens de colaboradores, organigrama da organização e contratos celebrados com fornecedores;
- Gestão de operações, de forma a obter informação relativa às operações efetuadas aos sistemas, como evidências da realização e monitorização de *backups* e de *jobs* de sistema, assim como procedimentos e políticas de gestão de incidentes e continuidade de negócio;
- Gestão de alterações, de forma a obter informação relativa às alterações efetuadas às aplicações, bases de dados e sistemas operativos em âmbito;

- Gestão de acessos, de forma a obter informação relativa à concessão, remoção e revisão de acessos, assim como questões de segurança como configurações de *passwords* e acessos privilegiados.

Adicionalmente a esta lista de pedidos, foram também realizadas reuniões com o CISO do cliente, de forma a obter um melhor entendimento relativamente a temas de cibersegurança.

Esta lista de pedidos foi colocada na plataforma *Connect* e partilhada com os interlocutores do cliente.

A plataforma *Connect* é uma plataforma desenvolvida pela PwC, utilizada para efetuar pedidos de informação e de documentos ao cliente de forma rápida, eficiente e segura ao longo dos trabalhos de auditoria. Esta plataforma permite também às equipas e aos clientes visualizar o estado dos pedidos de informação, assim como a informação e documentos partilhados, permitindo que seja guardado um histórico das comunicações efetuadas com os clientes (PwC-SROC, 2022).

No intervalo de tempo entre o envio dos pedidos de informação e recolha de evidências por parte do cliente, foi competência do aluno preparar a base de dados *Aura* para documentar os trabalhos.

O *Aura* é uma plataforma desenvolvida pela PwC com o objetivo de ser o sistema global de documentação dos trabalhos de auditoria efetuados pela PwC. Nesta plataforma é possível desenvolver e executar o plano de auditoria, documentando os trabalhos realizados, observando de forma fácil e clara a ligação existente entre os riscos, procedimentos obrigatórios, controlos e o trabalho que deve ser realizado para colmatar esses riscos, seguindo a metodologia de trabalho da PwC. Nesta plataforma é possível guardar todos os papéis de trabalho realizados para efetuar as análises aos controlos, assim como os resultados obtidos, e também serve de repositório de evidências, visto ser aqui que são guardadas todas as evidências partilhadas pelo cliente. O *Aura* inclui também *dashboards* que permitem às equipas verificar de forma rápida e simples o progresso dos trabalhos de auditoria, verificando se todo o trabalho foi devidamente concluído e revisto pelos elementos com as competências adequadas para o efeito (PwC-SROC, 2022).

4.3. Execução dos testes aos controlos

Após a receção das evidências e informações solicitadas foi necessário selecionar os itens a serem testados, decidindo para cada teste a necessidade de analisar a totalidade da população ou apenas uma amostra. No caso de ser necessário selecionar uma amostra, a seleção foi feita de uma de duas formas:

- Seleção estatística, onde a amostra foi selecionada de forma aleatória, com uma distribuição de probabilidades que deve ser uniforme; ou
- Seleção não estatística, onde a amostra foi selecionada recorrendo ao julgamento profissional da equipa, com o objetivo de obter uma amostra representativa das principais características relevantes na população. Apesar de esta forma de amostragem permitir uma maior escolha da amostra, deve ser o mais aleatória possível, de forma a não existir enviesamentos na amostra devido a julgamentos tendenciosos.

Seguidamente foi documentado no *Aura* o entendimento obtido sobre o ambiente de TI da empresa, onde foram abordados temas como a organização de TI do cliente, procedimentos de gestão de TI, gestão de fornecedores, funções de controlo interno do cliente, principais características dos sistemas em âmbito, gestão de acessos, gestão de alterações e continuidade de negócio.

Posteriormente foram realizados os testes aos controlos anteriormente definidos.

Os testes aos controlos foram efetuados para os domínios de ITGC de *Program Changes, Access to Programs and Data* e *Computer Operations*.

4.3.1. Program Changes

Neste domínio foram realizados os seguintes testes:

- Testar se as alterações efetuadas foram corretamente testadas e aprovadas antes de passarem para o ambiente de produção;

- Testar o controlo existente sobre o acompanhamento e monitorização das alterações ocorridas durante o ano de 2021; e
- Testar se existe uma correta segregação de ambientes (desenvolvimento, testes e produção).

Através destes testes foi possível verificar se o processo de gestão de alterações e os controlos associados se encontram operacionais, de forma a mitigar o risco de alterações indevidas nas aplicações em âmbito.

Para a realização destes testes foram pedidos os documentos relativos ao processo de gestão de alterações, de forma a analisar o desenho do controlo. De seguida foi selecionada uma amostra de alterações efetuadas aos sistemas em âmbito, de forma a testar se o processo estava a ser seguido, verificando a existência de uma aprovação formal para o desenvolvimento da alteração, realização e certificação de testes em ambientes de testes e a existência de aprovação para efetuar a passagem a produção.

Nos casos em que não se verificou o cumprimento do processo instituído pela empresa foram efetuadas reuniões de entendimento com a DSI do cliente e formalmente documentadas as exceções encontradas.

4.3.2. Access to Programs and Data

Neste domínio foram realizados os seguintes testes:

- Testar os controlos existentes nos processos de concessão, remoção e revisão de acessos às camadas aplicacional, base de dados e sistema operativo;
- Testar os controlos existentes sobre a monitorização das atividades desenvolvidas por utilizadores com acessos privilegiados aos sistemas em âmbito; e
- Testar se as configurações de *passwords* dos sistemas em âmbito se encontram alinhadas com a política de *passwords* definida pelo cliente, assim como com as boas práticas.

Através destes testes foi possível verificar se os controlos implementados nestas áreas estavam a funcionar de forma correta, ou se existia o risco de acessos indevidos aos sistemas em âmbito que pudesse resultar numa incorreta, incompleta ou inválida introdução ou processamento da informação, que poderia levar a distorção das contas da empresa. Foi também possível verificar a existência de acessos privilegiados, e se os mesmos eram mantidos apenas para o necessário desempenho das funções atribuídas, de forma a existir uma correta segregação de funções, assim como verificar se a gestão das contas genéricas estava a ser efetuada corretamente, confirmando a existência de um inventário de genéricos onde fosse possível identificar a função do acesso e o responsável atribuído a cada conta.

Para a realização destes testes foi analisada a Política de Segurança de Informação da empresa, bem como outras políticas e procedimentos acerca da nomenclatura de contas, processo de concessão, remoção e revisão de acessos e política de *passwords*. Após a análise destes documentos foi emitida uma opinião relativamente ao desenho dos controlos e efetuado os testes através da análise de evidências como lista de utilizadores dos sistemas em âmbito, onde foi verificado a data de concessão e de remoção dos acessos desses utilizadores, bem como quais os perfis associados de forma a analisar se os mesmo estavam corretamente atribuídos, verificando a existência de segregação de funções e de acessos privilegiados corretamente atribuídos. Adicionalmente foi efetuada uma análise à lista de saída de colaboradores para o ano de 2021 de forma a analisar se algum ex-colaborador mantinha acessos ativos.

Para além disso, foram também analisadas as configurações de *passwords* dos diferentes sistemas, de forma a validar se os parâmetros configurados correspondiam aos parâmetros definidos na política de *passwords* e às boas práticas.

4.3.3. Computer Operations

Neste domínio foram realizados os seguintes testes:

- Testar se os dados estão devidamente copiados (*backed up*) e se é possível a sua reposição;
- Testar se existe a devida monitorização à realização dos *backups*; e

- Verificar se estão asseguradas as condições de segurança física nos locais de armazenamento dos *backups*.

Através destes testes foi possível compreender e verificar se a atuação da empresa em caso de incidentes ou desastres que pudessem pôr em causa a continuidade das operações opera de forma correta, seguindo os normativos implementados pela empresa e as práticas instituídas em normas internacionais, e testar a capacidade da empresa de recuperar os dados conforme necessário.

Para a realização destes testes foi solicitada à direção de sistemas de informação os procedimentos onde se encontram definidos os processos de calendarizar, executar, monitorizar e de garantir a continuidade dos sistemas utilizados pela empresa. Após análise destes procedimentos foi emitida uma opinião sobre o desenho destes processos e efetuados os testes através da análise do calendário de *backups* definido, verificando se os mesmos foram realizados sem erros nas datas previstas e corretamente armazenados. Adicionalmente, foram pedidas evidências da monitorização dos *backups* e da deteção e correção dos erros de *backups* ocorridos.

No que diz respeito ao armazenamento físico dos *backups*, a visita ao *datacenter* do cliente foi efetuada pela PwC Espanha, dado que o *datacenter* se encontra em Barcelona, tendo sido responsabilidade do aluno analisar e documentar o trabalho efetuado pelos colegas da PwC Espanha.

Sempre que nas análises efetuadas se verificou a ocorrência de desalinhamentos entre o que estava a ser praticado e o que devia ser a prática correta, foram elaborados procedimentos mitigatórios de forma a verificar se o risco se encontrava mitigado. Para isso foram pedidas justificações ao cliente, assim como consultadas outras listas, ou feitas análises adicionais que permitissem compreender melhor o risco existente para as rubricas do relato financeiro. Sempre que eram encontradas deficiências que a equipa do RAS não conseguia mitigar, a equipa de auditoria financeira era informada para proceder a análises adicionais às contas da empresa.

Ao longo de todo o trabalho de auditoria foram efetuadas várias reuniões com o cliente, de forma a melhorar o entendimento acerca do ambiente de TI da empresa, ou para esclarecimento de dúvidas ou deficiências encontradas pela equipa no desenrolar dos

testes. Nestas reuniões, sempre que possível o aluno esteve presente, com intervenções ocasionais sempre que necessário e elaborando minutas e efetuando os testes necessários decorrentes da reunião.

Mais perto da conclusão dos trabalhos de auditoria foi dada ao aluno formação específica relativa à análise das *Journal Entries*, explicando o seu conceito e como deveria ser feita a análise. *Journal Entries,* são registos de transações efetuadas em *journal items*, consistindo assim num conjunto de registos, cada um correspondendo a um crédito ou um débito. Foi também explicado que o objetivo desta análise no âmbito de uma auditoria financeira é identificar os movimentos contabilísticos que não são usuais ou expectáveis de ocorrer.

Para a realização desta análise são utilizadas duas ferramentas, o *Microsoft Excel* e a ferramenta *Audit Command Language* (ACL). A ferramenta ACL é um *software* de auditoria bastante utilizado, que auxilia os auditores na realização dos trabalhos de auditoria (Puspaningrum, 2014). Esta ferramenta permite a análise de dados de diversas fontes, superando algumas das limitações existentes na utilização do *Microsoft Excel*, que apenas permite cerca de 1 milhão de linhas, enquanto que o ACL não tem limite. Para além disso, o ACL permite guardar o registo das ações efetuadas de forma que fique registado todos os passos efetuados para a realização da análise.

Portanto a análise às *Journal Entries* é efetuada em 4 etapas.

Após o fecho das contas por parte do cliente, foi da responsabilidade da equipa do RAS acompanhar, via videochamada, a extração das *journal entries* do sistema contabilístico do cliente, de forma a garantir a completude dos movimentos.

De seguida, foi realizada a reconciliação das contas do balancete de forma a verificar se existiam variações entre o saldo dos movimentos a débito e a crédito declarados no balancete, com o saldo dos movimentos extraídos do sistema. Nos casos em que essas variações foram detetadas, foi feito um *follow-up* com a equipa de auditoria financeira, de forma a entender as mesmas.

Feita a reconciliação e o *follow-up* das variações detetadas foi efetuada a importação dos movimentos contabilísticos para a ferramenta ACL. Aí foram criados novos campos para facilitar a análise dos dados, assim como a remoção de determinados movimentos considerados irrelevantes por parte da equipa de auditoria financeira.

Por fim, são analisados os critérios definidos pela equipa de auditoria financeira para a identificação de movimentos não usuais. Alguns exemplos desses critérios são a análise dos movimentos que não foram realizados por colaboradores do departamento de contabilidade, movimentos em duplicado ou movimentos realizados ao fim de semana. Após realizada a análise destes critérios o resultado é colocado num ficheiro *Excel* e enviado para a equipa de auditoria financeira analisar de forma a concluir se o trabalho pode ser terminado ou é necessário elaborar algum procedimento adicional ou questionar o cliente.

4.4. Conclusão dos trabalhos

Uma vez concluídos todos os testes de desenho e da eficácia operacional dos controlos implementados pelo cliente e guardados todos os papéis de trabalho e evidências analisadas, foram realizadas reuniões entre os elementos da equipa do RAS para discutir os resultados e as conclusões obtidas. Essas conclusões foram posteriormente comunicadas à equipa de auditoria financeira, para que estes pudessem verificar a necessidade de efetuar procedimentos adicionais.

De seguida, foi elaborado um primeiro memorando com as deficiências encontradas para ser partilhado tanto com a equipa de auditoria financeira como com o cliente.

Após a partilha deste memorando com o cliente, foram efetuadas reuniões de esclarecimento de dúvidas acerca das deficiências, para que as mesmas ficassem claras para o cliente, de forma a puderem elaborar as medidas corretivas para dar resposta às deficiências encontradas.

Por fim, foram efetuadas algumas alterações no memorando decorrentes da discussão e das medidas corretivas elaboradas pelo cliente, de forma a emitir o memorando final.

5. CONCLUSÃO

Este relatório é o resultado do estágio desenvolvido no departamento do RAS na empresa PwC, onde foi permitido ao aluno pôr em prática conhecimentos adquiridos ao longo da sua formação, assim como aprender bastante sobre a forma de trabalho de uma grande empresa de auditoria.

Através da elaboração deste estágio, foi possível ao aluno perceber a importância dada por parte da equipa de auditoria financeira aos riscos existentes nas empresas da utilização das tecnologias de informação. Não há dúvida que a crescente dependência das empresas nos SI traz riscos para a empresa que podem pôr em causa a disponibilidade, integridade, precisão e completude da informação financeira (Al-Dmour, 2018). Portanto, as empresas de auditoria apostam cada vez mais no recurso a especialistas de TI para melhorar a qualidade das auditorias desenvolvidas, visto que estes especialistas permitem à equipa de auditoria financeira obter um maior conforto relativo às rubricas financeiras analisadas para a emissão da certificação legal de contas (Krieger et al., 2021).

Desde o início do estágio que existiu um permanente contacto com as práticas e metodologias a utilizar, de forma a tornar o trabalho do estagiário o mais autónomo possível. No desenrolar dos trabalhos efetuados no estágio, foi possível verificar que é dada uma grande importância ao estipulado nas ISAs, de forma a garantir um trabalho de auditoria de alta qualidade.

No que diz respeito à utilização dos especialistas de TI na auditoria financeira, verificou-se uma grande atenção dada aos diferentes domínios de ITGC, de forma a confirmar que os controlos estavam a funcionar de forma correta. Um dos domínios onde o foco é maior é o domínio de *Access to Programs and Data,* o que é compreensível, tendo em consideração que a correta gestão dos acessos à informação é fundamental para garantir que não existem distorções nas rubricas financeiras, pois, tal como mencionado por Chan & Lao (2009), é neste domínio que o risco de acessos indevidos pode pôr em causa a integridade dos dados e dos programas, seja por via de ataques informáticos, *software* malicioso ou outras formas de acesso não autorizado.

O desenvolvimento deste estágio permitiu também ao aluno compreender que de facto existe um benefício muito elevado na partilha de colaboradores para projetos de auditoria e de consultoria, tal como referido por Estep (2021). No desenrolar o estágio o

aluno teve a oportunidade de estar envolvido num projeto de consultoria, onde pode pôr em prática conhecimentos adquiridos no projeto de auditoria, e obter novos conhecimentos que levou de volta ao projeto de auditoria.

É então possível afirmar que os objetivos do estágio foram atingidos, tendo em conta que o mesmo permitiu pôr em prática conhecimentos já adquiridos, assim como adquirir novos conhecimentos, e dado que o estágio permitiu ao aluno a passagem aos quadros da empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

Al-Dmour, A. (2019). The impact of the reliability of the accounting information system upon the business performance via the mediating role of the quality of financial reporting. *The International Journal of Accounting and Business Society, 26*(1), 56-88.

Barta, G. (2018). The increasing role of IT auditors in financial audit: risks and intelligent answers. *Business, Management and Economics Engineering, 16*, 81-93.

Bellino, C., Wells, J., Hunt, S., & Horwath LLP, C. (2007). *Global Technology Audit Guide (GTAG) 8: Auditing Application Controls*. *The Institute of Internal Auditors*.

Chan, W. H. B., & Lao, S. K. (2009). A study of the business value of IT general controls in China. *Journal of Information Technology Management*, *20*(4), 22–36.

Coates, S., Haege, M., Rune, J., Lourens, J., & Martinez, C. L. (2013). Global Technology Audit Guide (GTAG®) 4: Management of IT Auditing. *The Institute of Internal Auditors*.

Dai, J., & Vasarhelyi, M. A. (2016). Imagineering audit 4.0. *Journal of Emerging Technologies in Accounting*. 13(1), 1-15.

Davis, C., Kegerreis, M., & Schiller, M. (2020). *IT Auditing: Using Controls to Protect Information Assets*. 3ª Ed. New York: McGraw-Hill Education.

Estep, C. (2021). Auditor integration of IT specialist input on internal control issues: How a weaker team identity can be beneficial. *The Accounting Review*, *96*(5), 263–289.

Francis, J. R., & Yu, M. D. (2009). Big 4 office size and audit quality. *Accounting Review*, *84*(5), 1521–1552.

Gallati, R. R. (2003). *Risk management and capital adequacy*. McGraw-Hill.

Haapamäki, E., & Sihvonen, J. (2019). Research on International Standards on Auditing: Literature synthesis and opportunities for future research. *Journal of International Accounting, Auditing and Taxation*, *35*, 37–56.

Hill, C. W. L., & Jones, T. M. (1992). Stakeholder-Agency Theory. *Journal of Management Studies*, *29*(2), 131–154.

IAASB. (2009a). *ISA 200: Overall Objectives of The Independent Auditor and The Conduct of An Audit In Accordance With International Standards On Auditing*.

IAASB. (2009b). *ISA 230: Audit Documentation*.

IAASB. (2009c). *ISA 300: Planning an Audit of Financial Statements*.

IAASB. (2009d). *ISA 320: Materiality in Planning and Performingan Audit*.

IAASB. (2009e). *ISA 500: Audit Evidence*.

IAASB. (2009f). *ISA 530: Audit Sampling*.

IAASB. (2009g). *ISA 620: Using the Work of An Auditor's Expert*.

IAASB. (2019). *International Standard on Auditing 315 (Revised 2019)*.

ISACA. (2001). *Is Auditing Guideline Application Systems Review*.

ISACA. (2015). *ISACA ® Glossary of Terms English-Brazilian Portuguese Expert Translation Reviewers*.

Kilgore, A., Radich, R., & Harrison, G. (2011). The Relative Importance of Audit Quality Attributes. *Australian Accounting Review*, *21*(3), 253–265.

Krieger, F., Drews, P., & Velte, P. (2021). Explaining the (non-) adoption of advanced data analytics in auditing: A process theory. *International journal of accounting information systems, 41*.

Lateef, A., & Omotayo, F. O. (2019). Information audit as an important tool in organizational management: A review of literature. *Business Information Review*, *36*(1), 15–22.

Leming, R. (2015). Why is information the elephant asset? An answer to this question and a strategy for information asset management. *Business Information Review*, *32*(4), 212–219.

Pedro, J. M. (n.d.). *Segurança informática em auditoria*. [Em linha]. Disponível em: https://www.igf.gov.pt/inftecnica/75_anos_IGF/pedro/pedro_tema.htm [Acesso em: 2022/03/13].

Puspaningrum, M. T. (2014). The students' perception towards the audit using Audit Command Language (ACL) software. *The Indonesian Accounting Review*, *4*(1), 89–96.

PwC. (2021). *PwC Global Annual Review 2021. The New Equation - Building trust - delivering sustained outcomes*. [Em linha]. Disponível em https://www.pwc.com/annualreview [Acesso em: 2022/07/20].

PwC-SROC. (2022). *Relatório de transparência - Exercício 2021*. [Em linha]. Disponível em https://www.pwc.pt/pt/quem-somos/pwc-relatorio-transparencia-2021.pdf [Acesso em: 2022/07/20].

Richards, D. A., Oliphant, A. S., & le Grande, C. H. (2005). *Information Technology Controls*, *1*, 8-16.

Sayana, S. A. (2002). The IS Audit Process. *Information Systems Control Journal*, *1*, 20-22.

Tarek, M., Mohamed, E. K., Hussain, M. M., & Basuony, M. A. K. (2017). The implication of information technology on the audit profession in developing country: Extent of use and perceived importance. *International Journal of Accounting and Information Management*, *25*(2), 237–255.