Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO

GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

RELATÓRIO DE ESTÁGIO

A UTILIZAÇÃO DE METODOLOGIAS PARA AVALIAÇÃO DOS RISCOS EM SISTEMAS DE INFORMAÇÃO

MICKAËL PESTANA RODRIGUES

OUTUBRO 2022

Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
RELATÓRIO DE ESTÁGIO

A UTILIZAÇÃO DE METODOLOGIAS PARA AVALIAÇÃO DOS RISCOS EM SISTEMAS DE INFORMAÇÃO

MICKAËL PESTANA RODRIGUES

ORIENTAÇÃO:

RUI TRIGO PEREIRA (ISEG)
ANDRÉ GOMES ARAÚJO (PWC)

OUTUBRO 2022

“Try not to become a man of success, but ratter try to become a man of value.” (Albert Einstein)

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

ACL - *Audit Command Language*

AICPA - *American Institute of Certified Public Accountants*

CAAT - *Computer Assisted Audit Technique*

COBIT - *Control Objectives for Information and Related Technologies*

COSO - *Committee of Sponsoring Organizations of the Treadway Commission*

ISA - *International Standards on Auditing*

ITGC – *IT General Controls*

RAS - *Risk Assurance Services*

RGPD – Regulamento Geral de Proteção de Dados

SOC - *Service Organization Control*

SI – Sistemas de Informação

TI – Tecnologias de Informação

TSC - *Trust Services Criteria*

RESUMO

Nos últimos anos, a auditoria financeira tem sido objeto de grandes desenvolvimentos. Estes têm-se revelado nos conceitos aplicados e objetivos definidos, nas técnicas e métodos utilizados durante os trabalhos de auditoria. Em particular, a auditoria a sistemas de informação possui uma relevância maior e um papel mais crítico no contexto atual e procura ser mais do que um prolongamento da auditoria tradicional.

O âmbito do estágio realizado na PwC, nomeadamente no departamento de *Risk Assurance Services*, compreendeu a área de auditoria a sistemas de informação e avaliação dos riscos envolvidos. O presente relatório de estágio procura descrever e refletir de forma pormenorizada as atividades desenvolvidas. O estágio teve por base o acompanhamento de um conjunto de clientes relevantes do ramo de Indústria & Serviços e de *Financial Services*, nomeadamente a auditoria e revisão de Controlos Gerais Informáticos (ITGC). A principal finalidade dos ITGC é prestar auxílio à equipa de auditoria financeira na emissão de relatórios financeiros, concedendo conforto sobre os sistemas aplicacionais que podem influenciar diretamente as demonstrações financeiras.

Simultaneamente, o estágio é composto por uma componente importante onde é feito um enquadramento teórico e análise dos métodos e processos para a emissão de relatórios de certificação, *Service Organization Control* (SOC), executados de acordo com as melhores práticas atualmente instituídas, nomeadamente o COSO. O propósito da emissão deste tipo de relatório é fornecer conforto necessário aos clientes, fornecedores, reguladores ou outros *stakeholders*, sobre os controlos internos implementados numa organização.

O trabalho realizado no estágio permitiu consolidar competências no desenvolvimento das várias etapas do processo de auditoria de sistemas de informação, desde a fase de avaliação, execução e conclusão de análise a controlos implementados pelas organizações.

Em conclusão, a aprendizagem teórica e o trabalho prático realizado consolidaram conhecimentos e permitiu o recurso estruturado a metodologias para melhor avaliação dos riscos associados aos sistemas de informação de acordo com as normas internacionais aplicáveis.

PALAVRAS-CHAVE: Risco; Normas Internacionais; Controlo Interno; Sistemas de Informação; *Service Organization Control*; *Trust Services Criteria*.

ABSTRACT

In recent years, financial auditing has been the subject of major developments. These have been revealed in the applied concepts and defined objectives, in the techniques and methods used during the audit work. In particular, the audit of information systems has a greater relevance and a more critical role in the current context and seeks to be more than an extension of the traditional audit.

The scope of the internship at PwC, namely in the Risk Assurance Services department, included the area of auditing information systems and assessing the risks involved. This internship report seeks to describe and reflect in detail the activities developed. The internship was based on the monitoring of several relevant customers in the Industry & Services and Financial Services sectors, namely the audit and review of General Computer Controls (ITGC). The main purpose of the ITGC is to assist the financial audit team in issuing financial reports, providing comfort on the application systems that can directly influence the financial statements.

Simultaneously, the internship is composed of an important component where a theoretical framework and analysis of the methods and processes for issuing certification reports, Service Organization Control (SOC), executed in accordance with the best practices currently established, namely COSO. The purpose of issuing this type of report is to provide necessary comfort to customers, suppliers, regulators, or other stakeholders, about the internal controls implemented in an organization. The work carried out in the internship allowed the consolidation of skills in the development of the various stages of the information systems audit process, from the evaluation, execution, and conclusion of analysis to controls implemented by organizations.

In conclusion, the theoretical learning and the practical work carried out consolidated knowledge and allowed the structured use of methodologies to better assess the risks associated with information systems in accordance with applicable international standards.

KEYWORDS: Risk; International Standards; Internal Control; Information System; Service Organization Control; Trust Services Criteria.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

AGRADECIMENTOS

A realização deste trabalho representa o fim de uma jornada académica, com altos e baixos, muitos desafios e imensa aprendizagem. A todos os que se cruzaram no meu caminho e em especial ao longo do mestrado, o meu obrigado!

Ao Professor Rui, pelo apoio, suporte, compreensão, conhecimento, total disponibilidade e conselhos ao longo desta caminhada! Obrigado por tudo, foi incansável!!

Quero agradecer ao *Senior Manager* André Araújo pela disponibilidade e simpatia, pelo constante desafio, por acreditar, pelas oportunidades e experiência que me tem proporcionado!

À minha família. Obrigado, por todos os esforços realizados, pelas palavras, por sempre acreditarem em mim! Vocês são a base de tudo, sem vocês não estaria aqui, obrigado por tudo!

À Bea, que esteve sempre presente, motivando e dando sempre força para terminar esta etapa!

Por último, a todos os meus amigos, à b.logic, e todas as reuniões intermináveis ao longo do mestrado. Um obrigado!

A todos, um grande obrigado!!

1. INTRODUÇÃO

A informação é um recurso fundamental e crítico para as empresas. As informações são criadas, utilizadas, retidas, armazenadas e destruídas. A tecnologia desempenha um papel fundamental nessas ações. No entanto, a adoção da tecnologia traz novos riscos em diversas áreas, como a privacidade e segurança de informação, que é necessário acautelar e manter.

As normas técnicas internacionais determinam regras, diretrizes e características mínimas para atividades ou resultados. Estas são aprovadas por um organismo reconhecido e as empresas que cumprem as suas exigências podem obter uma certificação após o processo de auditoria. Assim, é frequente o recurso a auditores de sistemas de informação para realizar este tipo de trabalho de revisão com vista à certificação do ambiente interno de uma organização.

O presente relatório realizado no âmbito do estágio realizado na PwC, nomeadamente no departamento de *Risk Assurance Services* (RAS), procura descrever e refletir, de forma pormenorizada, as atividades desenvolvidas no âmbito de auditoria a sistemas de informação, ITGC (*IT General Controls*).

Adicionalmente, este prevê descrever o processo de auditoria a uma organização que presta serviços de consultoria de TI e de negócio sobre o ambiente interno, para emissão do relatório de certificação SOC 2 *Type* I. Para além da descrição das atividades, o Trabalho Final de Mestrado é composto por uma componente onde é feito um enquadramento teórico e análise dos métodos e processos existentes para a elaboração de auditorias aos sistemas de informação, em particular metodologias e relatórios de certificação, *Service Organization Control* (SOC).

O presente relatório está estruturado em 5 capítulos: (2) a revisão de literatura, que contextualiza a auditoria de sistemas de informação e os diferentes tipos de *Service Organization Control*; (3) as principais metodologias utilizadas; (4) a descrição do estágio, no qual é apresentada a organização e departamento onde foi desenvolvido o presente estágio, os objetivos gerais que o desencadearam, o cronograma e a formação desenvolvida; (5) a descrição das atividades desenvolvidas durante o estágio; e, por último, (6) a conclusão, bem como as suas limitações e perspetivas futuras.

2. REVISÃO DE LITERATURA

2.1. Auditoria de Sistemas de Informação

As auditorias desempenham um papel relevante nas considerações dos investidores e partes interessadas, pois fornecem uma opinião sobre a confiabilidade das demonstrações financeiras sobre as organizações alvo de auditorias.

Neste sentido, o papel de uma auditoria é melhorar a confiança dos utilizadores sobre as demonstrações financeiras. O auditor independente emite uma opinião sobre se as demonstrações financeiras estão materialmente corretas.

Esta opinião é alcançada pelos auditores reunindo evidência de auditoria adequada e suficiente para emitir uma opinião sobre a adequabilidade e completude das demonstrações financeiras. Isto é, se estas são preparadas, em todos os aspetos relevantes, de acordo com a estrutura aplicável e estabelecida do relatório financeiro (IAASB, 2009a). Portanto, ao fortalecer a confiança do público, as auditorias acabam contribuindo para o bom funcionamento dos mercados (European Comission, 2010).

Com a avanço tecnológico todo o processo de auditoria tem vindo a sofrer alterações consideráveis, o acesso aos dados é de certa forma mais rápido e ao mesmo tempo mais complexo, fazendo com que o processo de registo da informação sofresse grandes modificações. Logo, a auditoria a sistemas de informação não pode agora ser vista como uma prolongação da auditoria financeira.

A atualidade empresarial está muito dependente da componente de TI, sendo através desta que toda a informação financeira é processada e os dados armazenados capazes de proporcionar uma correta avaliação do estado geral de uma organização.

Cada uma dessas disciplinas de auditoria, auditoria financeira e auditoria de sistemas de informação, compartilham uma base comum de princípios de auditoria, padrões de prática e processos e atividades de alto nível. Na medida em que, as práticas financeiras e contabilísticas em organizações auditadas usam TI, as auditorias financeiras devem abordar os controlos baseados em tecnologia e a sua contribuição para apoiar efetivamente os controlos financeiros internos (Stoel et al., 2012).

Os avanços na tecnologia têm sido impactantes no dia a dia de todas as organizações. Isto, deve-se a um aumento da dependência de TI para as operações dos negócios, bem como novas regulamentações relacionadas com a garantia de TI para essas operações (Stoel et al., 2012).

A TI é fundamental para o sucesso organizacional, eficiência operacional, competitividade e sobrevivência, tornando-se essencial e com elevado cariz de importância a necessidade de as organizações garantirem a sua utilização correta e eficaz. Nesse contexto, é importante que os recursos sejam alocados de forma eficiente, que a TI funcione com um nível de desempenho e qualidade para apoiar de forma eficaz o negócio e os ativos de informação sejam protegidos de acordo com o risco que a organização permite (Matos, 2018).

Perante a crescente dependência de TI, as organizações investem cada vez mais na segurança de informação, no sentido de garantir que a informação se encontra devidamente protegida.

A segurança de informação refere-se à forma de gerir o acesso, protegendo a informação de acesso não autorizado ou verificando a identidade daqueles que afirmam ter autoridade para aceder à informação (Anderson, 2003).

Assim sendo, a auditoria de sistemas de informação pode ajudar as organizações a atingir todos estes objetivos e analisar a eficácia da segurança de informação implementada nas organizações. Segundo Ron Weber (1999), este define a auditoria a sistemas de informação (SI) como o processo de recolha e avaliação de evidência para determinar se um SI salvaguarda os bens, mantém a integridade dos dados e possibilita que a organização atinja os seus objetivos de forma eficaz e eficiente. No entanto, Chambers & Court, (1991) vão mais longe afirmando que atualmente, num contexto mais complexo, os auditores necessitam de um conhecimento mais profundo em sistemas de informação.

Em suma, os controlos internos contribuem para a integridade e consistência das informações. Como referido, os sistemas de controlo interno devem ser eficazes para proporcionar conforto e solidez quanto à operação correta dos processos de negócio e dos controlos que dependem das tecnologias de informação, tais como, os controlos automáticos, relatórios gerados por um sistema e cálculos realizados por um sistema. Finalmente, e para acrescentar aos exemplos atrás mencionados, existem mais três temas muito relevantes nomeadamente, a segurança, a segregação de funções e as interfaces entre sistemas.

2.2. Service Organization Control: SOC 1, SOC 2 e SOC 3

Muitas organizações dependem da integridade do seu ambiente de controlo para proteger as suas operações, os negócios e também os dos seus clientes. Com a emergência

de novas tecnologias que resultam da própria dinâmica do mercado e, por outro lado, a crescente prevalência de fornecedores terceirizados, essa integridade torna-se mais complicada de proteger de forma robusta (Moss - Adams LLP, 2021).

Uma das formas de garantir que os controlos internos se encontram em vigor e e a operar de forma eficaz é realizar uma auditoria de *System Organization Control* (SOC), ou seja, uma auditoria de controlo ao sistema e organização.

Embora estes relatórios não sejam de cariz obrigatório, os auditores financeiros utilizam-nos para reduzir os procedimentos de auditoria, e certos clientes pressionam as organizações prestadoras de serviço como modo de garantir que os seus dados estão protegidos.

Os relatórios de *System Organization Control*, conhecidos como SOC 1, SOC 2 ou SOC 3, são relatórios desenvolvidos *pelo American Institute of Certified Public Accountants* (AICPA) para avaliação de controlos internos implementados numa organização (AICPA, 2018), podendo ser úteis em:

- Avaliar a eficácia dos controlos relacionados aos serviços executados por uma organização prestadora de serviços;
- Apropriado para compreender como a organização de serviços mantém a supervisão de terceiros que prestam serviços aos clientes; e por fim,
- Melhora a capacidade de obter e reter clientes.

De seguida será apresentado as especificidades de cada SOC demonstrando as diferenças que cada relatório possui entre si.

2.2.1. SOC 1: ICFR – Report on Controls at a Service Organization Relevant to User Entities Internal Control over Financial Reporting

O relatório SOC 1 é projetado especificamente para abordar os controlos na organização de serviços que são relevantes para as demonstrações financeiras das entidades que utilizam o serviço. Eles permitem que os auditores executem procedimentos de avaliação de risco e obtenham evidência de auditoria sobre se os controlos da organização prestadora de serviços encontram-se a operar de forma eficaz (AICPA, 2018).

A auditoria independente é conduzida conforme a instrução sobre normas de certificação, criadas pelo AICPA, de atestados nº18 (*Statement on Standards for*

Attestation Engagements, SSAE 18) e as Normas Internacionais para atestado de certificação nº3402[1] (*International Standard on Assurance Engagements*, ISAE 3402).

A utilização dos relatórios SOC 1 é limitado às administrações de organizações prestadoras de serviços, entidades que sejam clientes e auditores. Existem dois tipos de relatórios que podem ser emitidos:

- *Type I*: relatório sobre a integridade da apresentação da descrição da gestão do sistema da organização de serviços e a adequação do desenho dos controlos para alcançar os objetivos de controlo relacionados incluídos na descrição a partir de uma data especificada (AICPA, n.d.-a); e,
- *Type II*: relatório sobre a integridade da apresentação da descrição da gestão do sistema da organização de serviços e a adequação do projeto e eficácia operacional dos controlos para alcançar os objetivos de controlo relacionados incluídos na descrição ao longo de um período especificado, por norma 6 a 12 meses (AICPA, n.d.-a).

2.2.2. SOC 2: Trust Services Criteria

A maioria das organizações que fornecem serviços de tecnologia, independentemente da área em que atuam, necessitam de auditorias SOC 2, isto porque, estas são fornecedoras terceirizadas que armazenam, processam ou mantêm dados de outras entidades (Moss - Adams LLP, 2021). Logo, estes relatórios visam considerar as necessidades de uma ampla gama de utilizadores que precisam de informações detalhadas e garantia sobre os controlos de uma organização de serviços (AICPA, n.d.-b).

O relatório SOC 2 oferece às organizações uma garantia baseada em controlos com alto nível de detalhe realçando a confiabilidade do sistema, medindo a eficácia dos controlos internos relacionados a cinco princípios de serviços de confiança (*Trust Services Criteria*): segurança, disponibilidade e integridade de processamento dos sistemas que a organização de serviços utiliza para processar os dados dos utilizadores e a confidencialidade e privacidade das informações que esses sistemas processam (AICPA, 2018).

Num relatório desta natureza, é requisito a inclusão de pelo menos um princípio TSC (segurança é o único obrigatório), sendo necessário a execução e validação de todos

[1] ISAE 3402 – relatório sobre os controlos internos de uma organização prestadora de serviços a outras entidades e para o qual estes são relevantes para o relatório financeiro destas entidades (IAASB, 2009a).

os controlos subjacentes ao TSC. Os outros critérios podem ser adicionados ao âmbito do relatório se a organização auditada assim o desejar, mas não são necessários para alcançar a conformidade com o SOC 2.

Em referência, podemos especificar cada critério e o que cada um procura garantir numa auditoria desta natureza (elementos enumerados e descritos em seguida).

1. Segurança: Este TSC trata da proteção de informações contra divulgação não autorizada. Ou seja, visa garantir que os sistemas e o ambiente de controlo de uma organização de serviços encontram-se devidamente protegidos contra acesso e divulgação de informações não autorizados e danos a sistemas que possam comprometer a disponibilidade, a integridade, a confidencialidade e privacidade de dados e informações ou sistemas (AICPA, 2019).
2. Disponibilidade: O critério de Disponibilidade determina se os funcionários e clientes podem confiar nos sistemas para realizar o trabalho. Alguns exemplos são *backups* de dados, recuperações em caso de desastres e planeamento de continuidade de negócios. O TSC de Disponibilidade procura garantir que informações e sistemas estão disponíveis para operação e uso para atender aos objetivos da entidade (AICPA, 2019). Assim sendo, este TSC refere-se à acessibilidade das informações utilizadas pelos sistemas da organização auditada e dos produtos ou serviços fornecidos aos seus clientes.
3. Integridade do Processamento: Determina se o processamento do sistema funciona corretamente, ou seja, é completo, válido, preciso e autorizado para atender aos objetivos da entidade. Este TSC aborda se os sistemas atingem o objetivo ou propósito para o qual existem e se executam as funções pretendidas sem atrasos, erros, omissão ou manipulação acidental (AICPA, 2019).
4. Confidencialidade: Este TSC avalia como as organizações protegem as informações confidenciais, ou seja, limitando o seu acesso, armazenamento e uso. O TSC de confidencialidade poderá auxiliar as organizações a definir quais são os utilizadores que podem aceder a que tipos de dados e de que forma esses dados podem ser partilhados (AICPA, 2019). Portanto, o TSC visa garantir que apenas pessoas devidamente autorizadas possam visualizar informações confidenciais, como documentos legais ou propriedade intelectual.
5. Privacidade: Este critério analisa como as atividades de controlo de uma organização protegem as informações de identificação pessoal dos clientes. Desta forma, garante que as informações pessoais são recolhidas, utilizadas, retidas,

divulgadas e eliminadas para atender aos objetivos da entidade (AICPA, 2019). Também procura garantir que um sistema que utiliza dados pessoais esteja em conformidade com os Princípios de Privacidade Geralmente Aceites da AICPA, tal como pelo RGPD.

Os cinco *Trust Services Criteria* foram alinhados aos 17 critérios apresentados na estrutura do COSO, o "*Internal Control – Integrated Framework*" (COSO, 2013), ao qual se encontram no Anexo B. Os 17 critérios apresentados descrevem especificamente o que é necessário para implementar efetivamente os cinco componentes (ambiente de controlo, avaliação de riscos, atividades de controlo, informações e atividades de comunicação e monitorização) para um controlo interno eficaz.

Ao contrário de outras estruturas de segurança de informação, como por exemplo a ISO 27001, não existe uma lista de verificação universal de requisitos SOC 2. No guia oficial SOC 2 (TSP seção 100) é fornecido para cada TSC pontos de foco (*point of focus*) (AICPA, 2019). Estes *point of focus* são exemplos de como a organização pode satisfazer os requisitos para cada critério. É importante notar que os *point of focus* não são requisitos, mas sim diretrizes para ajudar a organização e o auditor a entender o que é necessário para atender a cada requisito, como evidenciado no Anexo C um exemplo de *point of focus* que discute os padrões de conduta da organização.

À semelhança do relatório SOC 1, existem dois tipos de relatório:

- *Type I*: relatório sobre a descrição da gestão do sistema de uma organização de serviços e a adequação do *design* dos controlos (AICPA, n.d.-b).
- *Type II*: relatório sobre a descrição do sistema de uma organização de serviços e a adequação do projeto e eficácia operacional dos controlos (AICPA, n.d.-b).

Tabela 1 - Tipos de Relatórios SOC

EXAMINATION PERIOD		SOC REPORTS			TESTING COVERAGE		
		SOC 1	**SOC 2**	**SOC 3**	**Design**	**Operating Effectiveness**	**Results of Tests**
TYPE 1	POINT in time	✔	✔		✔		
TYPE 2	PERIOD of time	✔	✔		✔	✔	✔

Fonte: Adaptado de Moss - Adams LLP (2021, p.7)

2.2.3. SOC 3: Trust Services Criteria for General Use Report

O relatório de certificação SOC 3 assim como o SOC 2 cobre todos os cinco princípios de serviço (TSC – *Trust Services Criteria*) de segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade (AICPA, 2019). No entanto, o SOC 3 não fornece o mesmo nível de detalhe que o SOC 2.

O relatório é de uso geral, sendo um resumo executivo do relatório SOC 2 e inclui a opinião do auditor independente sobre o *design* efetivo e as operações dos controlos do cliente (AICPA, n.d.-c).

3. PRINCIPAIS METODOLOGIAS UTILIZADAS

As organizações necessitam de obter um aproveitamento total das ferramentas que possuem. Dessa forma, necessitam de desenvolver mecanismos que lhes possibilitem ter um maior controlo sob os sistemas de informação que usufruem. Para isso, são utilizadas metodologias de sistemas de informação e *frameworks* de boas práticas de sistemas que permitem ao topo de gestão dominar os recursos presentes na organização. Neste âmbito, nas avaliações dos riscos de SI/TI são utilizadas metodologias *standard* como o ISO/IEC 27001, COBIT e/ou COSO.

3.1. ISO/IEC 27001

A Norma técnica ISO/IEC 27001 é uma norma internacional publicada pela *International Organization for Standardization* (ISO) e pela *International Eletrotechnical Commission* (IEC). Atualmente, a Norma vai na sua segunda edição ISO/IEC:2013, revista e confirmada em 2019, pelo que esta versão permanece atual (Mirtsch et al., 2021).

Esta Norma identifica os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança de informação da organização (Culot et al., 2021). A Norma também inclui as condições para que a avaliação e o tratamento sobre os riscos de segurança da informação, sejam adaptados conforme as necessidades da organização.

O objetivo das organizações que adotam a Norma 27001, é garantir um maior compromisso com a proteção da informação, uma das maiores preocupações da atualidade. Desta forma, esta fornece às organizações um modelo de melhores práticas para identificar, analisar e implementar controlos para gerir riscos de segurança de informação e, consequentemente, proteger a confidencialidade, integridade e

disponibilidade de dados essenciais para a organização (Almeida et al., 2018). Isto é feito através da identificação de quais os potenciais problemas que podem ocorrer com a informação (avaliação de risco).

A avaliação de risco é um dos pontos mais importantes da Norma. Esta avaliação deve ser efetuada à *priori*, com a identificação dos riscos, seguido de uma classificação dos riscos, para que sejam implementadas medidas de mitigação. Após efetuada esta identificação aos riscos torna-se necessário efetuar uma análise aos riscos identificados, avaliando e determinando que ações de controlo são apropriadas para a gestão desses riscos (ISO/IEC 27001, 2013).

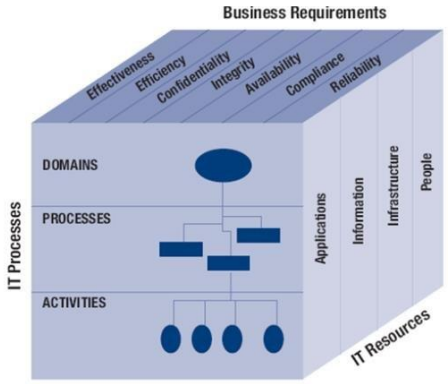
Quando a análise do risco se encontra determinada é necessário ocorrer a mitigação do risco e/ou tratamento do risco, ou seja, a organização deve definir que necessidades devem ser atendidas para prevenir tais problemas de ocorrerem. Assim, um dos principais objetivos desta Norma é baseado na gestão de riscos, ou seja, identificar onde se encontram os riscos para posteriormente tratá-los (ISO/IEC 27001, 2013).

Em conclusão, a Norma propõe um conjunto de objetivos de controlo para as organizações adotarem, documentados no Anexo A, que a Norma disponibiliza (Shojaie et al., 2014). Estes objetivos encontram-se no Anexo A do presente relatório. O Anexo A da Norma 27001 possui um conjunto de 114 controlos de referência divididos em 14 objetivos de controlo, que as organizações devem adotar (ISO/IEC 27001, 2013).

3.2. COBIT: Control Objectives for Information and Related Technologies

O COBIT (*Control Objectives for Information and Related Technologies*) criado pelo ISACA (*Information System Audit and Control Association*), é uma *framework* de boas práticas de gestão e governança de TI (ISACA, 2007). Através dos vários recursos que engloba que podem servir como modelo de referência para a gestão de TI, e com base no modelo é abordado a gestão de sistemas de informação a partir de três dimensões principais: processos de TI, recursos de TI e requisitos de negócio (ISACA, 2007).

Figura 1 - Cubo COBIT



Fonte: ISACA (2007, p.25)

O modelo de referência de processo COBIT 5 é a versão que sucede o modelo anterior de processo COBIT 4.1, com os modelos de processo *Risk IT* e *Val IT* integrados.

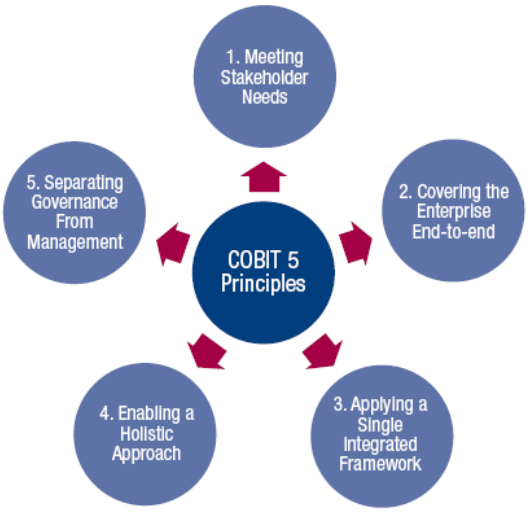
Esta versão do COBIT fornece uma estrutura ampla que auxilia as organizações a atingir os seus objetivos e a entregar valor através de governança e uma gestão eficaz da TI (ISACA, 2012b). Simplificando, o COBIT 5 ajuda a criação de valor para as organizações, mantendo um equilíbrio entre a otimização dos níveis de risco e utilização de recursos com a obtenção de benefícios.

O COBIT 5 permite que a informação e a tecnologia relacionada sejam orientadas e geridas de maneira global para toda a organização, abrangendo todas as áreas de negócios e funcionais, considerando os interesses das partes internas e externas relacionados a TI (ISACA, 2012b).

A estrutura do COBIT 5 é construída em torno de cinco princípios básicos e um conjunto completo de 37 processos de governança e gestão, que permitem às organizações otimizar o investimento e o uso de informações e tecnologia para o benefício das partes interessadas (Almeida et al., 2018).

Os cinco princípios básicos são: responder às necessidades das partes interessadas, cobrir a organização de ponta a ponta, aplicar um modelo único integrado, permitir uma abordagem holística e distinguir a governança da gestão (ISACA, 2012a).

Figura 2 - Princípios COBIT 5



Fonte: ISACA (2012b, p.21)

O modelo de referência de processo COBIT 5 subdivide os processos de governança e gestão de TI em duas áreas de atividade, governança e gestão, divididas por domínios de processos (ISACA, 2012a):

- Governança: Este domínio possui cinco processos de governança. Sendo que para cada processo, são definidas as práticas de avaliação, direção e monitorização (ISACA, 2012a); e,
- Gestão: Com o objetivo de garantir que os quatro domínios estão alinhados com as áreas de responsabilidade e fornecem cobertura de TI de ponta a ponta. Para cada domínio são incluídos vários processos, como nas versões anteriores (ISACA, 2012a). Embora a maioria dos processos necessite de atividades de planeamento, implementação, execução e monitorização dentro do processo ou do problema específico.

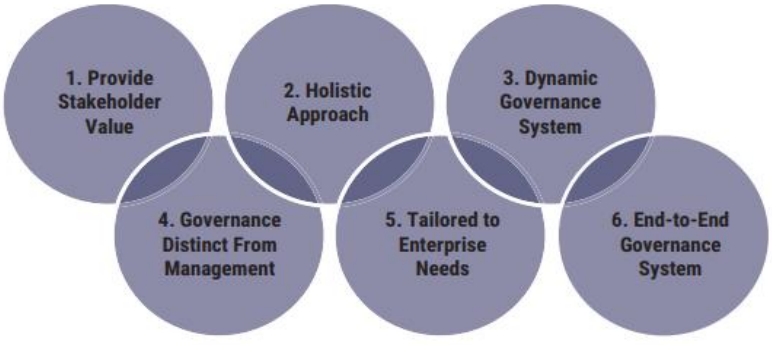
Atualmente, o modelo de referência de processo COBIT 2019 é a versão mais atualizada. Ao contrário do COBIT 5 que descrevia cinco princípios, o COBIT 2019 atualiza os princípios ao mesmo tempo que estabelece a estrutura geral.

O COBIT 2019 foi desenvolvido com base em dois conjuntos de princípios. O primeiro descreve os principais requisitos de um sistema de governança para informações e tecnologia, sendo o segundo conjunto os princípios para uma *framework* de governança que pode ser utilizada para construir um sistema de governança numa organização (ISACA, 2019).

Os princípios de Sistema de Governança, encontram-se descritos em seis princípios (ISACA, 2019), nomeadamente:

1. Fornecer valor para as partes interessadas: Este princípio afirma que cada organização requer um sistema de governança para ir de encontro às necessidades das partes interessadas e criar valor através da utilização de TI;
2. Ter uma abordagem holística: O sistema de governança deve ser construído a partir de componentes, ou seja, processos, estruturas, infraestruturas, arquitetura, informações, pessoas e cultura. Estas componentes podem ser de diferentes tipos, no entanto devem funcionar em conjunto;
3. Sistema de governança dinâmico: A criação de um sistema de governança dinâmico para refletir o estado atual da organização e, essa visão dinâmica criará um sistema que é viável e capaz de reduzir o risco, visto que poderá proporcionar uma visão dinâmica de toda a organização e os sistemas de TI que a engloba;
4. Diferenciar a Governança de Gestão**:** A governança define a direção estratégica de uma organização e, em seguida, a gestão planeia, elabora e executa essa visão;
5. Adaptado às necessidades específicas do negócio: Eventualmente negócios até do mesmo setor, possuem necessidades, objetivos e metas diferentes. Logo, o sistema de governança necessita de ser customizado para as necessidades específicas de cada negócio; e,
6. Sistema de governança de ponta a ponta: O sistema de governança não pode ser concentrado só no departamento de TI. Este precisa de incluir toda a tecnologia e informações localizadas dentro da organização e utilizadas nos negócios para atingir as metas e objetivos.

Figura 3 - Princípios de sistemas de governança

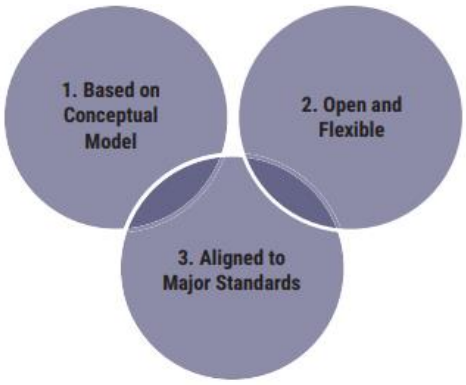


Fonte: ISACA (2019, p.17)

O segundo conjunto de princípios definidos no COBIT 2019, são os princípios de *framework* de governança, sendo definidos três (ISACA, 2019).

1. Baseado em um modelo conceptual: O COBIT 2019 reconhece que uma *framework* de governança deve ser baseada em um modelo conceptual. Este modelo deve identificar os principais componentes e relacionamentos entre os sistemas, de forma que seja possível obter uma visão geral da TI, os seus componentes e como estes interagem entre si;
2. Flexível e aberta: estrutura de governança deve ser aberta e flexível; e,
3. Alinhado aos principais padrões: O terceiro princípio de uma *framework* de governança refere-se ao alinhamento aos principais padrões, estruturas e regulamentações. Garantir a conformidade tem de ser uma prioridade para todas as organizações. Portanto, alinhar o sistema de governança às leis e regulamentos é fundamental (ISACA, 2019).

Figura 4 - Princípios de *framework* de governança



Fonte: ISACA (2019, p.18)

O COBIT 2019 pode ser considerado como uma *framework* que orienta toda a estratégia de TI de uma forma holística, podendo ser executado em conjunto com as principais diretrizes, estruturas e leis, regulamentos ou padrões.

A diferença entre o COBIT 5 e COBIT 2019, são as áreas de cobertura de atualização, em que, com o COBIT 2019 são incluídos novos processos aplicáveis a

projetos, informações de negócios e estruturas regulatórias ou de conformidade globais. Desta forma, o número total de processos COBIT passa de 37 para 40 nesta última versão.

Adicionalmente, com a introdução do conceito das Áreas de Foco, o COBIT 2019 procura acompanhar o cenário de risco de negócios de TI que permanece em constante mudança. Algumas das áreas de foco são o COBIT 2019 para pequenas e médias empresas, para *DevOps*, Risco de Informação e Tecnologia ou Segurança da Informação.

3.3. COSO: Committee of Sponsoring Organizations of the Treadway Commission

O COSO, é uma *framework* que avalia o ambiente de controlo e a sua eficácia. Criado com o objetivo de auxiliar a identificação de relatórios financeiros com fraudes, ou seja, analisando os fatores que podem gerar fraudes nos relatórios financeiros e elaborando recomendações para as organizações, auditores e órgãos reguladores (Park et al., 2021).

O modelo COSO proporciona uma avaliação da gestão sobre controlos internos e relatório financeiros, exemplificado através do seu cubo (McNally S. J., 2013). O COSO providencia orientações de como os sistemas de controlo interno das organizações devem funcionar. Assim, este estabelece diretrizes com o objetivo de proteger a organização dos riscos presentes.

Figura 5 - Cubo COSO

Fonte: McNally S. J. (2013, p.4)

O COSO passou por diversas atualizações ao longo do tempo, sendo que, existem dois modelos. O COSO I que diz respeito ao "*Internal Control – Integrated Framework*", e o "*Enterprise Risk Management – Integrated Framework*", conhecido como COSO II ou COSO ERM.

O COSO I, criado em 1992, procura fornecer uma garantia sobre o alcance dos objetivos de uma organização. Assim, este visa garantir que os objetivos estejam relacionados com a eficácia e eficiência das operações, confiabilidade dos relatórios financeiros e conformidade com a lei e regulamentos que sejam aplicáveis.

O COSO I possui cinco componentes: controlo do ambiente, avaliação de riscos, atividades de controlo, informação e comunicação e por último a monitorização.

O cubo COSO, é uma representação do sistema de controlo interno, sendo as dimensões as seguintes (McNally S. J., 2013):

1. Categorias de objetivos;
2. Níveis da Estrutura Organizacional; e,
3. Componentes de Controlo.

Desta forma, as três dimensões demonstram a relação entre os objetivos de controlo que as organizações precisam alcançar, as componentes do controlo para conseguir alcançar os objetivos traçados e os níveis da estrutura organizacional, o que altera de organização para outra.

O outro modelo do COSO, *Enterprise Risk Management Integrating with Strategy and Performance*, criado em 2017 e com coautoria da PwC, destaca a importância de considerar os riscos para a melhoria da performance, mas também no processo de estabelecer a estratégia (COSO, 2017).

4. DESCRIÇÃO DO ESTÁGIO

4.1. PwC Portugal

A PwC é constituída por uma rede de firmas independentes entre si e uma das maiores multinacionais de consultadoria e auditoria que presta serviços em auditoria financeira e auditoria de sistemas de informação, consultoria financeira e de TI, e fiscalidade. Foi fundada em Londres durante o ano de 1998 a partir da fusão entre *Price Waterhouse* e *Coopers & Lybrand*. No entanto, em 2010 a *PricewaterhouseCoopers* formalmente estabelece a sua marca como PwC, mas legalmente permanece como *PricewaterhouseCoopers*.

O departamento de *Risk Assurance Services* (RAS) da PwC, em Lisboa, presta diversos serviços aos seus clientes ajudando a identificar e a gerir os riscos de negócio associados aos sistemas de informação e melhorar a utilização de TI, estes podem ser observados logo de seguida tais como: trabalho de Auditoria de Sistemas e Tecnologia de

Informação (*IT Security*), Privacidade e Proteção de Dados, Auditoria Interna, entre outros, como é possível observar logo de seguida.

Figura 6 - Serviços prestados pelo *Risk Assurance Services*

Fonte: PwC Portugal

4.2. Objetivos gerais do Estágio

No âmbito dos serviços prestados pelo departamento de RAS, o estágio inicialmente teve por base o acompanhamento de um conjunto de clientes do ramo de Indústria & Serviços, nomeadamente auditoria a Controlos Gerais Informáticos (ITGC). A finalidade dos ITGC é prestar auxílio à equipa de auditoria financeira na emissão de relatórios financeiros, concedendo conforto sobre os sistemas aplicacionais que influenciam diretamente as demonstrações financeiras.

Outro dos serviços prestados é o *Third Party Assurance*, que tem como objetivo apoiar a fornecer conforto necessário aos clientes, fornecedores, reguladores ou outros *stakeholders*, sobre os controlos internos implementados numa organização através da emissão de relatórios objetivos, *Service Organization Control* (SOC), executados de acordo com as melhores práticas atualmente instituídas. A emissão deste tipo de relatório encontra-se alinhado com normas e *frameworks* internacionais, como é o caso do ISO 27001 (para a gestão da Segurança da Informação), COBIT (para governação de TI empresarial) e COSO.

Em suma, é nestes dois tipos de serviços prestados pelo RAS que o atual estágio é desenvolvido, sob a coorientação do *Senior Manager* do projeto André Gomes Araújo.

Assim sendo, este estágio teve os seguintes objetivos principais:

- Participar no processo de auditoria a sistemas de informação;
- Avaliar a adequação dos sistemas de informação utilizados nas organizações;
- Utilização de técnicas para análise de dados;
- Contacto com a equipa de trabalho dos clientes e internas;
- Compreensão das metodologias e ferramentas internas;
- Planeamento e organização do trabalho (gestão de tempo);
- Desenho e caracterização dos testes e procedimentos de avaliação;
- Execução dos testes e procedimentos de avaliação; e,
- Análise e avaliação das conclusões.

4.3. Cronograma

Na tabela 2, encontra-se o planeamento do trabalho geral estipulado para o desenvolvimento do estágio. O estágio realizado na PwC teve uma duração de seis meses, compreendidos entre fevereiro e julho de 2022, percorrendo um conjunto de diversas fases. No Anexo D, encontra-se definido de forma detalhada o cronograma geral do trabalho determinado para o desenvolvimento do estágio.

Tabela 2 - Cronograma macro do estágio

	Meses					
Descrição:	**Fevereiro**	**Março**	**Abril**	**Maio**	**Junho**	**Julho**
1. Formação Inicial (ver Anexo E)						
2. On-The-Job Training - Auditoria de ITGC						
3. Formação: 21ª Edição Digital Academies // Power Tools						
4. Formação: SAP Audit Course						
6. Formação: Risk Assurance Trainning						
7. Auditoria Relatório de Certificação SOC 2 Type I						

Fonte: Elaborado por PwC em janeiro de 2022

Numa primeira fase, o estágio realizou-se por um período de um mês de formação intensa. A formação, nesta fase inicial incidiu sobre as práticas que regem internamente a PwC, metodologias e ferramentas de auditoria. No Anexo E, é apresentado com maior detalhe a formação inicial, assim como todas as atividades e componentes que a englobaram.

Após o período de formação intensa deu-se início à segunda fase de formação, nomeadamente em contexto de trabalho de auditoria. Esta fase inicial, subsistiu pela

integração a diversos projetos, ainda que numa vertente de *On-The-Job-Training*, com o intuito de se familiarizar com as metodologias utilizadas internamente.

De realçar que a formação foi uma componente contínua ao longo do estágio, inclusive com formações mais específicas sobre ferramentas e/ou metodologias.

A segunda fase do estágio, inseriu na participação num trabalho efetivo junto de um cliente do setor de consultoria de tecnologia de informação, para emissão do relatório SOC 2 *Type I*.

No entanto, e considerando o impacto e criticidade do *output* dos trabalhos a participação nestes projetos exigiu a integração em equipas com senioridade e supervisão adequadas, passando por compreender e colocar em prática um conjunto de competências técnicas e comportamentais necessárias para o desenvolvimento ao longo do estágio.

4.4. Formação

Na PwC, sempre que é admitido um novo colaborador, o primeiro mês de trabalho é realizado em formações. O período de formação foi efetuado completamente de forma remota, e é composto por diversas fases, para além de ser um processo contínuo para todas as categorias.

Após a admissão na empresa, como *New Joiner* (colaborador em regime de estágio), o primeiro mês decorre de forma intensa e é composto por diversas etapas:

- ***Pre-Onboarding***: Conjunto de sessões dedicado ao *learning pathway* e às melhores práticas a ter durante o percurso formativo;
- ***Onboarding***: Conjunto de formações de boas práticas comportamentais, morais e éticas. Ainda nesta formação é dado a conhecer todas as áreas em que a PwC opera, como também como a estratégia, cultura, valores, práticas da firma e as diferentes linhas de serviço da PwC;
- ***Relationship Basics***: Somos inseridos num conjunto de dinâmicas de grupo que têm como objetivo envolver os participantes num ambiente de competição saudável, enquanto são promovidos os valores e a cultura PwC. Neste âmbito, foi desenvolvida uma atividade de ação de responsabilidade social;
- ***E-learnings* Obrigatórios:** Conjunto de formações online, denominados como *e-learnings* composto por formações de ética, independência, segurança e confidencialidade. Adicionalmente, são efetuadas formações mais específicas sobre metodologias internas tais como, o PwC *Audit Guide*, *IT Dependencies*, estratégia de auditoria em ITGC e *data analytics*, da mesma forma que são

introduzidas as ferramentas internas utilizadas no âmbito das auditorias como o *Connect* e o *Aura*.

- **Formação das *Line of Service***: Por fim, é iniciada a formação mais técnica, esta formação é dividida em duas fases, uma mais geral, denominada de *Assurance* 1, onde são realizadas formações sobre metodologias (*PwC Audit Guide*), conceitos de auditoria e ferramentas (*Connect*, *Aura*, *Excel*) e por fim, uma formação mais específica direcionada ao departamento de RAS:

1ª fase: *Assurance* 1 – Nesta fase, é transmitido por elementos mais *seniors* um conjunto de conceitos e termos mais técnicos que aborda diversos temas, tais como, Noções Básicas de Auditoria, Visão geral da auditoria da PwC, Gestão de tempo, Ética e Conduta Profissional, Introdução ao *Aura* (ferramenta da PwC de apoio à documentação da auditoria), Documentação de auditoria, ceticismo profissional, entender o negócio dos clientes, introdução à avaliação de risco, fraude, estrutura de controlo interno, reconciliações, testes de controlo, testes substantivos, o processo de revisão, e por fim *interviwing skills*.

2ª fase: RAS**:** Nesta fase, a formação é apenas direcionada ao departamento de RAS. A formação foi composta pela explicação das metodologias e serviços realizados no departamento e engloba os seguintes temas: *overview* do ciclo de auditoria, papéis e responsabilidades do RAS, introdução aos ITGC, introdução aos CAAT (*Computer Assisted Audit Technique*) e tecnologia/ferramentas utilizadas (*ACL - Audit Command Language*). Tudo isto, é finalizado com a realização de um *case study* para um cliente fictício.

No decorrer do estágio ocorreram um conjunto de formações mais específicas que capacitaram a aquisição de técnicas e conhecimento que ajudaram o desenrolar do estágio, nomeadamente a *21ª Edição Digital Academies // Power Tools*, *SAP Audit Course* e *Risk Assurance Training*. O objetivo foi transmitir a usabilidade e utilização de *data analytics* em contexto de auditoria, a consolidação das metodologias e práticas comuns, e por fim aquisição de novas competências. De seguida, são detalhados as formações prestadas e o âmbito ao qual estas compreenderam.

21ª Edição Digital Academies // Power Tools:

Esta formação compreendeu na aquisição de conhecimento, teórico e prático, de 3 ferramentas de análise de dados: *Alteryx*, Tabelas Dinâmicas em *Excel* e *Power BI*. Esta

última ferramenta de análise de dados permitiu uma consolidação de conhecimentos já adquiridos ao longo do mestrado. Adicionalmente, em cada uma das sessões dedicadas a cada ferramenta, foi realizado um conjunto de exercícios de forma a compreender de que forma é que é efetuada a importação, organização e análise à informação de forma a produzir relatórios e *dashboards* para apresentação dos resultados.

SAP Audit Course:

O SAP é um dos sistemas de *software* mais utilizados no mercado, desta forma, o departamento de RAS proporcionou um conjunto de sessões com o objetivo de consolidar a avaliação dos controlos estabelecidos no SAP em contexto de auditoria a ITGC.

A formação incidiu com a aquisição de conhecimentos dos diferentes módulos de SAP, a estrutura, o conceito de segregação de ambientes e funções, perfis com elevadas permissões, conceitos de autorização, gestão de alterações e aberturas de mandantes e/ou processamento *batch*.

No decorrer das sessões foi proporcionado o acesso a uma *Sandbox*, que proporcionou a realização de exercícios ao longo da formação. Foi possível extrair tabelas e relatórios e ainda criar utilizadores. A *Sandbox* permite que exista uma navegação sem qualquer impacto direto em um cliente, pois por esta estar isolada de outros sistemas, dados ou clientes permite total liberdade na execução e prática.

Risk Assurance Training:

Durante uma semana foi realizada uma formação direcionada a todos os colaboradores que pertencem ao departamento de RAS, independentemente da senioridade de cada elemento. Esta formação teve duas vertentes, na primeira foi efetuada um *overview* pelo *partner* do departamento sobre o ano fiscal que terminou em junho de 2022 e apresentação das áreas de atuação do departamento de RAS, nomeadamente o leque de serviços que oferece e perspetivas de crescimento para os próximos anos.

A segunda vertente incidiu na consolidação das metodologias e práticas comuns a todos os elementos de *Risk Assurance Services*. Esta compreendeu em temas como, documentação no Aura, testes a efetuar em contexto de ITGC, PwC *Audit Guide*, assim como a integração na área de especialização, *Digital Assurance*. A área de especialização, *Digital Assurance*, é composta por serviços de auditoria de sistemas de informação e serviços de relatórios de certificação SOC 1, SOC 2, SOC 3 ou ISAE 3402.

Toda a componente da formação é um processo contínuo ao longo da estadia. A PwC ainda dispõe de uma plataforma interna com formações online (*E-learnings*) sobre diversos temas que podem ajudar na execução dos trabalhos desenvolvidos. Além disso,

é disponibilizado uma biblioteca *online* onde pode ser consultado os trabalhos já realizados por outras firmas pertencentes à rede PwC, facilitando o contacto e auxílio à execução dos projetos e desafios que são apresentados ao longo do percurso.

4.5. Metodologia PwC

A PwC como rede internacional adotou uma metodologia que constitui a base para todas as auditorias levadas a cabo pela PwC. A metodologia é baseada no cumprimento das Normas Internacionais de Auditoria (ISAs[2]) e foi desenvolvida com base nas metodologias apresentadas no capítulo 3.

O *PwC Audit Guide* explica a metodologia da PwC e fornece uma abordagem de auditoria comum para todas as firmas-membro da *network* da PwC. Isto com o objetivo de cada firma-membro da PwC compreender a abordagem adotada por outras firmas da PwC na realização de um trabalho ou projeto de outra firma. O *PwC Audit Guide* foi projetado para ser flexível e escalável para todos os tipos de compromissos.

Este guia interno, juntamente com as ferramentas adicionais que complementam a metodologia fornecem *insights* para o desenvolvimento e documentação de cada projeto.

As principais ferramentas usadas no âmbito do presente estágio foram:

- *Connect* - é uma ferramenta de *workflow* que otimiza e monitoriza o fluxo de pedidos e partilha de informação entre a PwC e os seus clientes no decorrer de uma auditoria. Esta ferramenta permite uma coordenação aprimorada e monitorização do status do trabalho, de forma automatizada e em tempo real.
- *Aura* – é um software de auditoria usado para todos trabalhos de auditoria da PwC a nível global. Esta é uma ferramenta que capacita e potencia as auditorias com a capacidade de controlar, rever e reportar progresso e resultados dos trabalhos.

[2] ISA - *International Standards on Auditing*, refere-se a normas profissionais utilizadas nos trabalhos de auditoria e, que, tratam das responsabilidades do auditor independente. As ISAs têm como objetivo, melhorar e padronizar os trabalhos de auditoria, no sentido de fortalecer a confiança do público em geral sobre estes (IAASB, 2009b).

5. DESCRIÇÃO DAS ATIVIDADES DESENVOLVIDAS

5.1. Projetos envolvidos em contexto On-The-Job-Training

Após a formação inicial de um mês, que se insere em um contexto mais teórico, dá-se início à componente prática com a integração progressiva a projetos de auditoria a sistemas de informação, é o chamado *On-The-Job-Training*.

Estes projetos iniciais incidiram no acompanhamento e apoio a equipas de auditorias a Controlos Gerais Informáticos (ITGC), nomeadamente do ramo de Indústria & Serviços. Os projetos incidiram na participação ativa em um conjunto diversificado de clientes de vários setores, tais como, Energia & *Utilities*, Retalho, Marítimo-Portuário, Telecomunicações, Turismo, Saúde, Engenharia & Construções, Bebidas e Distribuição.

A auditoria a ITGC efetuada nestes clientes, passou por identificar e avaliar os riscos sobre a confiança na informação gerada pelos sistemas de informação produzidos pelos clientes para os controlos relevantes. Importa referir que um sistema de informação é considerado no âmbito de auditoria quando se planeia confiar em controlos aplicacionais, ou seja quando são identificadas *IT Dependencies*, tais como:

1. Controlos Automáticos;
2. Relatórios gerados por um sistema;
3. Cálculos realizados por um sistema;
4. Segurança – (Acesso restrito e Segregação de Funções - utilizador possuir o mínimo dos privilégios, ou seja, ter acessos adequados e mínimos de acordo com as suas funções); e,
5. Interfaces entre sistemas.

Aquando da identificação de uma ou mais das *IT Dependencies* supramencionadas ou os contextos dos sistemas de informação assim o justifiquem, é necessário o envolvimento do RAS no sentido de facultar *Audit Support*.

Os envolvimentos nestes projetos passaram por um leque de controlos utilizados para gerir e controlar as atividades de TI e o ambiente computacional, ao qual abrange as seguintes áreas e no qual houve uma participação ativa para garantir a efetividade dos controlos internos:

- Gestão de Acessos: testes a controlos de concessão de acessos, remoção e revisão de acessos, análises a parametrizações de *passwords* de sistemas, bases de dados

e sistemas operativos, e por fim análise de utilizadores com perfil de administração;

- Gestão de Alterações: verificar se as alterações efetuadas a nível aplicacional e a nível de infraestrutura (bases de dados e sistemas operativos) respeitam o correto *workflow*, segundo as políticas internas e as boas práticas internacionais, uma correta segregação de ambientes e funções; e por fim,
- Gestão de Operações: principais ferramentas e monitorização aos *backups* e processos *batch*/*jobs*, políticas e procedimentos de incidentes e continuidade de negócio.

O objetivo era verificar a conformidade e alinhamento dos sistemas em âmbito com os negócios das organizações.

Adicionalmente, e no âmbito de uma auditoria a ITGC no ramo de *Financial Services*, a uma instituição financeira, existiu a oportunidade de participar numa parte de testes e análise realizados, de forma a garantir a efetividade dos controlos internos da instituição.

Os testes realizados no âmbito da auditoria sob coordenação dos elementos mais *seniors* foram:

- Teste ao controlo de preço: analisar se as informações de preços do mercado que não foram corretamente registadas no sistema de informação despoletaram mensagens de erro. Logo, foram realizados um conjunto de testes com base nas evidências facultadas, no sentido de verificar se efetivamente o controlo encontra-se implementado e as mensagens de erro eram despoletadas automaticamente;
- Compreensão da arquitetura do negócio: foram realizadas um conjunto de reuniões de entendimento para compreensão da arquitetura do negócio e dos diversos sistemas em âmbito na auditoria. Toda a documentação foi realizada com suporte do desenho da arquitetura e as interfaces existentes entre os sistemas com auxílio da ferramenta *Microsoft Visio*; e,
- Testes de segregação de funções: para um conjunto de sistemas foram efetuados testes de segregação de funções a partir das listagens de utilizadores e permissões que os mesmos tinham. O objetivo era verificar as permissões que os utilizadores possuíam para criar e alterar por exemplo limites de crédito, no sentido de garantir que quem cria não aprova.

Além disso, no presente estágio foi dada a oportunidade de realização de controlos aplicacionais através de CAAT (*Computer Assisted Audit Technique*), nomeadamente através da ferramenta ACL (*software* que auxilia os auditores na execução de trabalhos de análise de dados), tais como:

- Interfaces entre sistemas, de forma a garantir que os dados que se encontram em um sistema estão registados no outro sistema.
- Análises aos movimentos contabilísticos (*Journal Entries*), que consiste em uma análise aos registos de transações efetuadas por um cliente. O objetivo é garantir que o que se encontra no balancete está devidamente registado no sistema contabilístico da organização, sendo um teste que permite à equipa de auditoria verificar a ocorrência ou não de fraude nos movimentos contabilísticos.
- Análises de sequencialidade de faturação, cujo objetivo é o de detetar a existência de faturas que não se encontram registadas.

Todos os testes e análises realizadas aos controlos foram documentadas no *Aura*.

5.2. Auditoria Relatório de Certificação SOC 2 Type I

O presente estágio após decorrida a primeira fase em contexto de formação e em *On-The-Job-Training*, passou para uma segunda fase que teve como participação num trabalho efetivo no serviço prestado pelo RAS de *Third Party Assurance*, para emissão do relatório de certificação SOC 2 *Type I*.

5.2.1. Enquadramento

A crescente preocupação das organizações com a segurança e proteção dos dados, dos sistemas de informação que processam e armazenam dados, as organizações têm tido cada vez mais solicitações e necessidades contratuais por parte dos seus clientes, para obter relatórios de certificação referente às suas plataformas tecnológicas.

Desta forma, foi solicitado à PwC por uma organização que presta serviços de consultoria de TI e de negócio, a realização de auditoria com vista à obtenção do relatório de certificação SOC 2 *Type* I. O objetivo do relatório é efetuar uma descrição detalhada da gestão do sistema da organização prestadora de serviço e a adequação do *design* dos controlos.

Neste sentido, o *Senior Manager* disponibilizou um conjunto de relatórios de certificação até então realizados pela *network* da PwC, com o objetivo de enquadrar o projeto e o seu objetivo, o que viria a facilitar o processo de conhecimento e o tipo de

projeto em causa. A participação neste projeto foi feita desde o seu início, acompanhando todas as suas etapas.

5.2.2. Equipa

A equipa designada para o projeto é composta por um *Partner*, um *Senior Manager*, uma *Senior Associate* e um *Assistant Associate.* Esta é liderada pelo *Partner* que realiza o planeamento do projeto e posteriormente entrega ao *Senior Manager*, que fica responsável por organizar o planeamento. De seguida, é facultado à *Senior Associate*, que fica com a responsabilidade de partilhar e disponibilizar as atividades a desenvolver entre o *Assistant Associate* de acordo com a experiência de cada um.

O projeto, como será verificado de seguida, contém várias etapas, pelo que cabe ao *Senior Manager* organizar e priorizar o trabalho a desenvolver. Muitas vezes esta priorização faz-se em conjunto com o cliente, de modo que ambos os lados estejam em sintonia.

5.2.3. Abordagem e atividades desenvolvidas durante o projeto

O âmbito do relatório inclui os serviços acordados com o cliente, ou seja, as aplicações para o qual será alvo de auditoria e estará no objeto para certificação incluindo os princípios dos *Trust Services Criteria* (referidos como TSC) para Segurança, Disponibilidade, Confidencialidade e Privacidade definidos no capítulo "*2.2.2. SOC 2: Trust Services Criteria"*.

O projeto foi iniciado com a realização de um conjunto de reuniões, *Kick-of-Meeting*, junto dos interlocutores referenciados pelo cliente para cada área (Segurança, *Privacy*, Recursos Humanos, Desenvolvimento, *Facilities*). Em todas estas reuniões é requisito da equipa de trabalho a elaboração das minutas de reunião, são as atas de reunião, com o propósito de posteriormente documentar no *Aura* e tirar dúvidas que eventualmente surgissem no desenrolar do projeto. As redações destas minutas ficaram a encargo do *assistant associate* e da *senior associate*.

Os propósitos destas reuniões iniciais foram com o intuito de esclarecer e apresentar o projeto aos interlocutores das respetivas áreas, o âmbito de cobertura, apresentação da equipa de trabalho e o cronograma do mesmo.

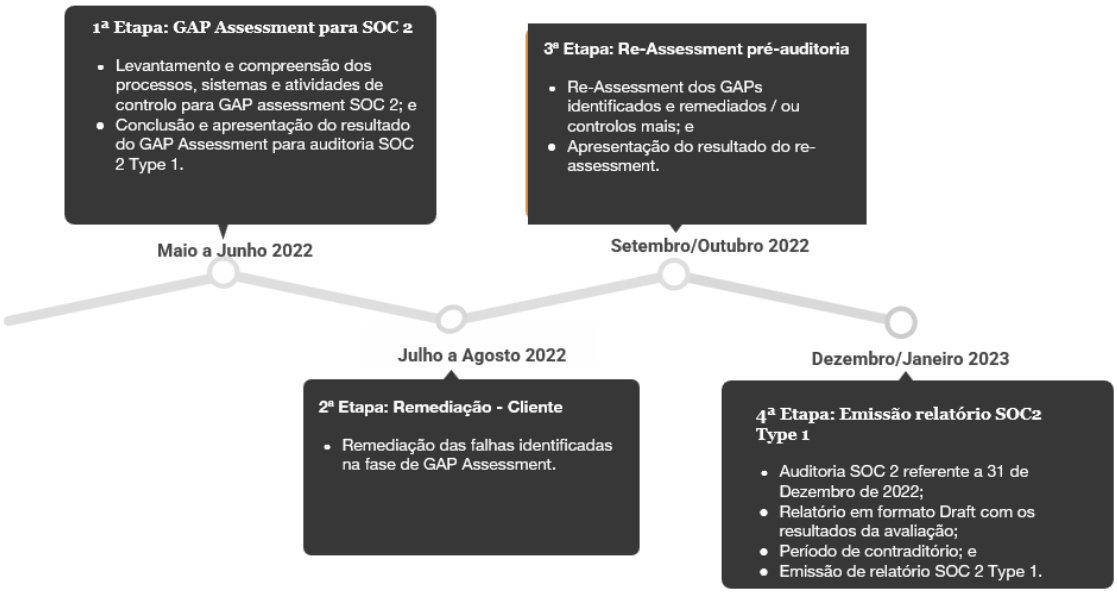
Assim sendo, em cada uma das reuniões, foi efetuada uma introdução sobre o projeto em causa, ou seja, apresentar o SOC 2 e os cinco TSC que o compõem, no sentido de elucidar os intervenientes que para cada TSC existe um conjunto de objetivos de

controlo para os quais a equipa da PwC irá identificar e avaliar as atividades que os endereça.

Outro tópico abordado foi o âmbito do projeto e que sistemas estariam no âmbito para a certificação.

Posteriormente, o responsável do projeto dá a conhecer a equipa que irá realizar o projeto e por fim, é apresentado o cronograma do projeto e as suas diferentes etapas, como descrito na figura abaixo.

Figura 7 - Cronograma do projeto SOC 2



Fonte: Elaborado pelo *Engagement Senior Manager* (2022)

Nota que algumas atividades se encontram em execução, nomeadamente "Remediação - Cliente" e "*Re-Assessment* pré-auditoria". Relativamente à fase de "Emissão relatório SOC 2 *Type* I" é expetável que ocorra entre os meses de dezembro com emissão final do relatório SOC 2 *Type* I a janeiro de 2023.

O projeto subsistiu em diferentes etapas como demonstrado, e pelo qual será demonstrado as principais atividades que foram realizadas em cada uma destas etapas.

1ª Etapa: *GAP Assessment*:

Por forma a validar o desenho e implementação dos controlos, o trabalho foi estruturado nas fases de (1) entendimento, (2) execução e (3) conclusão, onde foram desempenhadas um conjunto de tarefas em conjunto com a *senior associate* sob coordenação do *senior manager*.

1. Entendimento:

Elaboração de um pedido de informação, disponibilizado na plataforma *Connect*, com o intuito de compreender o ambiente de controlo da organização.

No pedido de informação constava uma série de temas que tinham como objetivo responder aos controlos em âmbito para cobrir os cinco TSC, sendo estes estruturados da seguinte forma:

- IT *Governance*: políticas e procedimentos implementados internamente sobre o processo de contratação de colaboradores, avaliação de desempenho e formação de colaboradores, código de ética, conselho de administração, RGPD, criptografia, segurança de rede, testes de intrusão se são efetuados e com que periodicidade, plataformas para monitorização de incidentes de segurança ou de dados pessoais e *firewall* e suas revisões;

  Posteriormente, é efetuado um conjunto de pedidos direcionados à comunicação e informação que é efetuada internamente e externamente, gestão de riscos e atividades de monitorização para os sistemas em âmbito;
- Gestão de Acessos Lógicos e Físicos: políticas e procedimentos de concessão e revogação de acessos, revisões periódicas de acessos, parametrização de senhas para sistemas, bases de dados e sistemas operativos, utilizadores com acessos privilegiados (administradores de sistemas), acesso físico às instalações inclusive *Datacenter*, segregação de funções de acesso, formas de autenticação aos sistemas em âmbito e *logs* de auditoria;
- Gestão de Operações: políticas e procedimentos de *backups* e sua monitorização, processamento de *jobs*/*batch*, gestão e monitorização de incidentes, Plano de Continuidade de Negócio e Plano de Recuperação em Caso de Desastre e respetivos testes; e,
- Gestão de Alterações: política e procedimentos, metodologia de desenvolvimento de sistemas, segregação de ambientes e funções, evidenciar o fluxo do processo de gestão de alterações *standard* e de emergência, evolutivas e corretivas, pós-implementação, ou seja, existência de testes e revisão das alterações com passagem a produtivo.

No sentido de complementar o entendimento, foram efetuadas um conjunto de sessões de trabalho preliminares no sentido de compreender os processos, sistemas e atividades de controlo relevantes para o trabalho e de que forma a organização endereça

os TSC para cada serviço em âmbito no relatório. Para cada reunião com as áreas foram elaboradas as minutas de reunião.

Uma vez efetuado o levantamento e compreensão, foi definida a matriz de controlos, com base nas reuniões tidas e com a leitura exaustiva da documentação existente como forma de compreender e avaliar os serviços prestados, o ambiente de controlo interno da organização e a arquitetura e tecnologia existente.

Posteriormente, de forma a complementar a compreensão do ambiente e procedimentos internos, foi realizada uma visita presencial às instalações da organização para validação dos controlos de segurança física e ambiental, tal como a leitura das políticas e procedimentos implementados internamente.

No seguimento e face a um conjunto de dúvidas no entendimento de alguns processos e controlos foi efetuado um conjunto adicional de pedidos de informação na plataforma *Connect* e reuniões de entendimento junto dos departamentos relevantes para o relatório de certificação *SOC 2 Type I*.

Numa destas reuniões foi providenciada autonomia para coordenar e seguir um conjunto de reuniões para a compreensão de tais controlos. Estas reuniões contaram com a presença do *senior manager*, caso alguma questão ou tema de elevada dificuldade surgisse. Nestas reuniões foram discutidos temas sobre:

- Política e procedimentos de criptografia, de que forma são mantidas e como é feita a gestão de chaves criptográficas;
- Criptografia de canais de comunicação, nomeadamente os protocolos implementados para comunicação com o exterior;
- Limitação de instalação de software em *desktops*, ou seja, compreender como funciona o processo de proteção dos dispositivos de rede local (capacidade de efetuar *boot*[3] aos computadores) e bloqueio de portas USB;
- Revisão de acessos à VPN;
- Existência de sistemas de deteção de intrusão baseado em *host* e que soluções têm implementadas; e,
- Temas relacionados com a proteção e privacidade de dados de clientes, colaboradores e fornecedores.

[3]*Boot* – processo de inicialização do computador durante o carregamento do sistema operacional quando a máquina arranca.

Deste modo, a coordenação e a autonomia concedida nestas reuniões tiveram um impacto relevante no desenvolvimento, pois permitiram uma dinâmica em um conjunto de diversas tarefas ao nível de planeamento, direção e coordenação, além da aquisição de conhecimento profundo sobre os temas o que permitiu um contato com os interlocutores na discussão do ambiente e controlos internos para os temas discutidos.

2. Execução:

Feito o planeamento e entendimento dos procedimentos de avaliação tendo em conta os TSC em âmbito (segurança, disponibilidade, integridade do processamento, confidencialidade e privacidade), deu-se início à fase de execução.

Esta fase teve como objetivo documentar e avaliar os controlos definidos na matriz de controlos, garantindo a efetividade de todos os controlos definidos para cada TSC.

Ao longo desta fase e aquando da identificação de alguma dúvida era feita a realização de reuniões com os responsáveis pelos serviços em âmbito, pela gestão da infraestrutura de suporte do serviço e pelos intervenientes nos processos identificados como relevantes no âmbito do relatório. Posteriormente, foram gerados um conjunto intermédio de pedidos de informação, direcionados para dar resposta aos controlos a avaliar definidos na matriz de controlos.

A avaliação dos controlos definidos, foram executados através de procedimentos de auditoria. Os procedimentos de auditoria de desenho e implementação dos controlos incluíram como principais técnicas: entrevistas, observação, análise de dados, análise documental e inspeção de configurações de sistemas.

1. Entrevista: Reuniões com os interlocutores relevantes com o objetivo de obter conhecimento e informação pertinente para o teste de desenho e implementação de controlo. De acordo com o *PwC Audit Guide* a técnica de auditoria de entrevista não pode ser utilizada de forma exclusiva para validar o desenho de implementação de um controlo, tendo o teste de um controlo de ser complementado por pelo menos uma outra técnica de auditoria;
2. Observação: Observar a existência e implementação de controlos específicos, como no caso de controlos de acessos físicos ou visita ao *Datacenter*;
3. Análise documental: Análise detalhada de documentação interna da organização auditada, incluindo, entre outros, documentação formal e registos documentais de desempenho de controlos; e,

4. Inspeção de configurações de sistemas: Inspeção das configurações de sistemas por forma a avaliar controlos automáticos implementados nos sistemas da organização auditada, tais como, processamento automático de *job/batch*.

Por fim, após efetuada a avaliação e documentação dos controlos definidos na matriz de controlos, foi elaborado um relatório *Draft* de GAP *Assessment* para comunicação dos resultados preliminares e posterior remediação do cliente.

2ª Etapa: Remediação – Cliente e 3ª Etapa: *Re-Assessment* pré-auditoria

No decorrer da 1ª Etapa e aquando da comunicação dos resultados preliminares no relatório *Draft* de *GAP Assessment* foi acordado com o cliente que à medida que o cliente elaborasse as medidas corretivas para cada *GAP* identificado fosse evidenciado à equipa de trabalho com suporte documental através da plataforma *Connect*.

Desta forma foi possível efetuar já o trabalho de compreensão sobre o tratamento e resolução por parte do cliente sobre os GAPs identificados (3ª Etapa). A maioria destes foram essencialmente sobre políticas internas desatualizadas, no qual devem ser formalmente definidos procedimentos e revisão das mesmas com mínimo de periocidade anual. Para GAPs identificadas e com maior criticidade que podem colocar em causa a emissão do relatório, a remediação ainda se encontrava em curso.

4ª Etapa: Emissão do relatório de certificação SOC 2 Type I

Durante esta fase, é planeado a avaliação e revisão do nível de cumprimento dos *Trust Services Criteria* (TSC) em âmbito (do trabalho), bem como dos GAPs (eventuais diferenças ou inconformidades) identificados na fase de Execução. O agendamento desta fase encontra-se planeado para se realizar entre dezembro e janeiro de 2023.

Por fim, é planeado a emissão do relatório final em janeiro de 2023, o qual diz respeito à auditoria realizada sobre o ano de 2022. O relatório SOC 2 (final) no decurso da sua emissão inclui uma secção detalhada dos processos do cliente auditado e todos os controlos adotados para proteger o serviço prestado aos clientes, incluindo os procedimentos de teste do auditor e os resultados de cada controlo. A conclusão dos trabalhos coincide com a emissão do relatório de certificação designado por relatório de certificação *SOC 2 Type I*.

6. CONCLUSÕES

6.1. Considerações Finais

O presente Trabalho Final de Mestrado é o trabalho académico que materializa a realização de um estágio na PwC, no departamento de RAS, e num contexto de aprendizagem nas áreas de risco e segurança da informação. Os principais objetivos visavam a reflexão, a análise, a aquisição de conhecimento nestas áreas e o confronto das atividades desempenhadas ao longo do estágio realizado.

O estágio compreendeu duas grandes fases, numa primeira fase a integração e participação em auditoria a sistemas de informação, nomeadamente ITGC. O que permitiu a aquisição de um leque de conhecimentos, que possibilitaram construir gradualmente uma abordagem crítica na identificação e avaliação dos riscos sobre a confiança na informação gerada pelos sistemas de informação, particularmente no ramo de Indústria & Serviços. Por outro lado, o facto de ter executado um conjunto de testes de segregação de funções, testes ao controlo de preço e compreensão da arquitetura funcional do negócio, junto de um cliente da área de *Financial Services* permitiram também a aquisição de um conjunto vasto de competências técnicas e melhor compreensão do mercado financeiro e da relevância da execução deste conjunto de testes.

A participação neste tipo de projetos (diferentes projetos, diferentes testes e de áreas distintas), possibilitaram o acompanhamento das várias etapas em que consistem uma auditoria a sistemas de informação (SI) e adquirir uma visão mais holística sobre as especificidades de cada ramo e dos diversos clientes que atuam em cada setor. Este envolvimento direto em projetos distintos permitiu realizar trabalhos e funções diferentes de acordo com a especificidade de cada trabalho de auditoria e revisão dos procedimentos.

Adicionalmente, a realização de um conjunto de controlos aplicacionais (interfaces entre sistemas, análises aos movimentos contabilísticos e análises de sequencialidade de faturação) permitiram a aquisição e a consolidação de um conjunto de competências técnicas, particularmente ao nível de análises de dados com recurso a ferramentas como o *Excel Avançado* e *ACL*, materializando ainda mais os conceitos já adquiridos ao longo do mestrado. Estes conhecimentos adquiridos facilitaram a realização deste conjunto de trabalhos, nomeadamente de análise avançada de dados e execução de um conjunto de procedimentos de revisão aplicacional.

Numa segunda fase do estágio, a integração a um projeto para certificação SOC 2, permitiu um aprofundamento sobre as melhores práticas atualmente instituídas. Além

disso, possibilitou a aprendizagem e conhecimento teórico-prático sobre os cinco *Trust Services Criteria* que estão alinhados aos 17 critérios apresentados na estrutura do COSO, o "*Internal Control – Integrated Framework*" (COSO, 2013).

Ao longo do projeto SOC 2 *Type* I, outros aspetos mais relevantes foram a autonomia conferida em diversas fases do projeto para a realização dos testes aos controlos, desde a fase de entendimento, execução e conclusão. A autonomia concedida revelou-se de extrema importância para o desenvolvimento e crescimento profissional ao longo do estágio. Inclusive, a coordenação de reuniões com o cliente possibilitaram a consolidação de temas lecionados ao longo do mestrado, mas também a aprendizagem de outros temas relacionados com *softwares* para deteção de *software* malicioso e deteção de intrusão baseado em *host*, VPN, criptografia, limitação para instalação de software nos *desktops* dos colaboradores e por fim, temas relacionados com a proteção e privacidade de dados de clientes, colaboradores e fornecedores alinhado ao RGPD.

A formação constante e contínua ao longo do estágio, a disponibilidade para o esclarecimento de dúvidas, o trabalho em equipa e o *feedback* constante são outros dos aspetos positivos a destacar e que potenciaram o crescimento pessoal e profissional, bem como a integração nos quadros da PwC, enquanto profissional da área. Finalmente, o trabalho realizado em diferentes projetos permitiu uma consolidação de conhecimentos e a aplicação de capacidades técnicas adquiridas tanto durante o mestrado como posteriormente na formação.

Em síntese, os conhecimentos já adquiridos permitiram enriquecer a experiência de trabalho numa organização de serviços profissionais com recursos a metodologias universais.

6.2. Limitações e Perspetivas Futuras

As principais limitações do estágio prendem-se com o facto de a grande maioria dos clientes privilegiarem ainda o formato remoto. Por outro lado, existe a perspetiva da realização de reuniões de acompanhamento e entendimento para diversos clientes, já em formato presencial, e visitas obrigatórias planeadas aos respetivos *Datacenters*.

Simultaneamente, o facto de na literatura atual e publicada, a presente documentação existente e disponibilizada ainda ser, de algum modo, algo escassa sobre relatórios de certificação *System and Organization Controls*, nomeadamente SOC 1, SOC 2 e SOC 3, faz com que a informação sobre a aplicabilidade em contexto europeu seja mais diminuta em comparação com outros mercados.

Por outro lado, o facto de tanto a PwC como o cliente que, no caso, foi objeto de certificação para o SOC 2 *Type* I, e de acordo com os termos de confidencialidade e privacidade de dados que aplicam internamente, não permitiram a partilha de documentos e informação mais precisa e também mais aprofundada sobre o contexto de todos os controlos realizados. A prossecução dos objetivos planeados e a realização dos procedimentos de revisão constitui uma experiência enriquecedora e de consolidação de um percurso profissional nesta área.

No entanto, de destacar que com a realização do projeto em causa, a perspetiva é de especialização neste tipo de serviço, na medida em que a participação no projeto possibilitou a integração em outro projeto do mesmo tipo, relatório de certificação SOC 2 *Type* I, para uma entidade do setor financeiro.

REFERÊNCIAS

AICPA. (n.d.-a). *SOC 1 - SOC for Service Organizations: ICFR*. Retrieved September 28, 2022. https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc1report.html

AICPA. (n.d.-b). *SOC 2® - SOC for Service Organizations: Trust Services Criteria*. Retrieved September 28, 2022. https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

AICPA. (n.d.-c). *SOC 3® SOC for Service Organizations: Trust Services Criteria for General Use Report*. Retrieved September 28, 2022. https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc3report.html

AICPA. (2018). *CPAs: Helping service organizations build trust and transparency System and Organization Controls (SOC)*.

AICPA. (2019). *TSP Section 100 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy Notice to Readers*. https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocu

Almeida, R., Lourinho, R., Silva, Miguel., & Pereira, R. (2018). COBIT 5 for Information Security. *EEE*, 60–69. https://ieeexplore.ieee.org/abstract/document/8452659

Anderson, J. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308–313. https://www.sciencedirect.com/science/article/pii/S0167404803004073?casa_token=0jHH_Lrl_1MAAAAA:2OfLJ8M8AyZ_tnWKhT6EszEjonDb_FX_fwAksFn19e_gTOSCeRZlLwdo0U4kvrgMFU1x6v53_Q

Chambers, A. D., & Court, J. M. (1991). *Computer Auditing*.

COSO. (2013). *Internal Control - Integrated Framework*. https://www.coso.org/Shared%20Documents/Framework-Executive-Summary.pdf

COSO. (2017). *Enterprise Risk Management Integrating with Strategy and Performance*. https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, *33*, 76–105. https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202/full/pdf?title=the-isoiec-27001-information-security-management-standard-literature-review-and-theory-based-research-agenda

European Comission. (2010). *Audit Policy: Lessons from the Crisis*. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2010)0561_/com_com(2010)0561_en.pdf

IAASB. (2009a). *International Standard on Auditing 320 - Materiality in Planning and Performing an Audit*. https://www.ifac.org/system/files/downloads/a018-2010-iaasb-handbook-isa-320.pdf

IAASB. (2009b). *International Standard on Auditng 200 - Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing*. https://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf

ISACA. (2007). *COBIT 4.1,"Framework Control Objectives Management Guidelines Maturity Models"*. https://www.studocu.com/row/document/polytechnic-college-suriname/governance-and-ict/cobit-41-cap-g/10120802

ISACA. (2012a). *COBIT 5 Enabling Processes*.

ISACA. (2012b). *COBIT 5 for Information Security*.

ISACA. (2019). *COBIT 2019 Framework Governance and Management Objectives*.

ISO/IEC 27001. (2013). *Information technology — Security techniques — Information security management systems — Requirements*.

Matos, B. (2018). *Audit Reform: Impact on Markets* [Work Project, NOVA – School of Business and Economics]. https://run.unl.pt/bitstream/10362/35218/1/Mato_2018.pdf

McNally S. J. (2013). *The 2013 COSO Framework & SOX Compliance*. https://www.coso.org/Shared%20Documents/COSO-McNally-Transition.pdf

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9082865

Moss - Adams LLP. (2021). *Why a SOC Report Makes All the Difference*. https://www.mossadams.com/articles/2021/05/what-is-a-soc-report

Park, K., Qin, J., Seidel, T., & Zhou, J. (2021). Determinants and consequences of noncompliance with the 2013 COSO framework. *Journal of Accounting and Public Policy*, *40*(6). Determinants and consequences of noncompliance with the 2013 COSO framework

PwC. (n.d.). *PwC*. Retrieved October 12, 2022. https://www.pwc.pt/pt/quem-somos.html

Shojaie, B., Federrath, H., & & Saberi, I., (2014). Evaluating the effectiveness of ISO 27001:2013 based on Annex A. *9th International Conference on Availability, Reliability and Security*, 259–264. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6980290

Stoel, D., Havelka, D., & Merhout, J. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*, *13*(1), 60–79. https://www.sciencedirect.com/science/article/pii/S1467089511000662

ANEXOS

Anexo A – Objetivos de controlo ISO/IEC 27001

Tabela A1 - 14 objetivos de controlo definidos na Norma ISO/IEC 27001

· A.5 – Políticas de segurança de informação.
· A.6 – Organização de segurança de informação.
· A.7 – Segurança na gestão de recursos humanos.
· A.8 – Gestão de ativos.
· A.9 – Controlo de acesso.
· A.10 – Criptografia.
· A.11 – Segurança física e ambiental.
· A.12 – Segurança de Operações.
· A.13 – Segurança de comunicações.
· A.14 – Aquisição, desenvolvimento e manutenção de sistemas.
· A.15 – Relações com fornecedores.
· A.16 – Gestão de incidentes de segurança de informação.
· A.17 – Aspetos de segurança de informação na gestão da continuidade do negócio.
· A.18 – Conformidade.

Fonte: Adaptado de ISO/IEC 27001 (2013, p. 16-29)

Anexo B – Critérios COSO relevantes para o SOC 2

Tabela B1 – 17 critérios COSO relevantes para o SOC 2

Componentes	Princípios
Ambiente de Controlo	Princípio 1: Do conselho de administração e gestão até todos os funcionários, a organização prioriza a integridade e os valores éticos. Princípio 2: O conselho de administração, que atua independentemente da gestão, fiscaliza a instituição e a atuação de controlos internos. Princípio 3: A gestão procura objetivos de negócios atribuindo autoridades e responsabilidades adequadas e estabelecendo uma estrutura organizacional definida e linhas de relatórios. Princípio 4: Demonstra o compromisso de contratar e reter uma força de trabalho competente. Princípio 5: Todos os funcionários são responsabilizados por manter os controlos internos.
Avaliação do Risco	Princípio 6: Objetivos claros são definidos para que a organização possa identificar e avaliar riscos relacionados a esses objetivos. Princípio 7: Os riscos aos objetivos de toda a empresa são identificados e analisados, sendo criadas diretrizes para gerir esses riscos. Princípio 8: A avaliação de riscos considera e analisa a possível existência de fraude. Princípio 9: As práticas de organização mudam a gestão.
Atividades de Controlo	Princípio 10: Atividades específicas são implementadas para atender aos objetivos operacionais e mitigar riscos. Princípio 11: São criadas atividades de controlo projetadas para prevenir fraudes e reduzir o risco dentro dos sistemas tecnológicos. Princípio 12: As atividades de controlo são delineadas e explicadas por meio de políticas e procedimentos estabelecidos.
Informação e Comunicação	Princípio 13: As informações relevantes apoiam o funcionamento do controlo interno. Princípio 14: A organização possui canal de comunicação interna. Princípio 15: Os objetivos e responsabilidades de controlo interno que afetam parceiros de negócios externos, fornecedores e outras partes são comunicados efetivamente.

Atividades de Monitorização	Princípio 16: Avaliações contínuas e de verificação são realizadas para determinar a presença e função dos controlos internos. Princípio 17: O conselho de administração e a administração recebem comunicação oportuna sobre quaisquer deficiências no controlo interno.

Fonte: Adaptado de COSO - "*Internal Control – Integrated Framework*"

Anexo C - Point of Focus direcionado ao Princípio 1

Tabela C1 - Princípio 1 e respetivos *Point of Focus*

TSC Ref. #	***Criteria***	***Points of Focus***
	CONTROL ENVIRONMENT	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
		Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behaviour the importance of integrity and ethical values to support the functioning of the system of internal control.
		Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.
		Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
		Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.
		Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.

Fonte: AICPA (2019)

Anexo D – Cronograma geral de alocação a projetos

Tabela D1 - Cronograma detalhado de alocação a projetos

Mês	Fevereiro	Março	Abril	Maio					Junho					Julho			
Semana	Mês completo	Mês completo	Mês completo	1	2	3	4	5	1	2	3	4	5	1	2	3	4
	Formação Inicial (ver cronograma específico)	On-The-Job-Training	On-The-Job-Training	On-The-Job-Training	21ª Edição Digital Academies // Power Tools	On-The-Job-Training	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	SAP Audit Course	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Risk Assurance Training	Auditoria Relatório de Certificação SOC 2 Type I
		Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break
		On-The-Job-Training	On-The-Job-Training	On-The-Job-Training	21ª Edição Digital Academies // Power Tools	On-The-Job-Training	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	SAP Audit Course	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Risk Assurance Training	Auditoria Relatório de Certificação SOC 2 Type I
	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço	Almoço
	Formação Inicial (ver cronograma específico)	On-The-Job-Training	On-The-Job-Training	On-The-Job-Training	21ª Edição Digital Academies // Power Tools	Auditoria Relatório de Certificação SOC 2 Type I	On-The-Job-Training	On-The-Job-Training	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	SAP Audit Course	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Risk Assurance Training	Auditoria Relatório de Certificação SOC 2 Type I
		Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break	Break
		On-The-Job-Training	On-The-Job-Training	On-The-Job-Training	21ª Edição Digital Academies // Power Tools	Auditoria Relatório de Certificação SOC 2 Type I	On-The-Job-Training	On-The-Job-Training	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	SAP Audit Course	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I	Auditoria Relatório de Certificação SOC 2 Type I

Fonte: Elaborado por PwC em janeiro de 2022

Anexo E – Cronograma Formação Inicial

Tabela E1 - Formação Inicial Semanas 0 e 1

		Semana 0	*Semana 1*				
Dia da Semana		**Sexta-feira**	**Segunda-feira**	**Terça-feira**	**Quarta-feira**	**Quinta-feira**	**Sexta-feira**
Horas						**Assurance 1**	**Assurance 1**
09:00	09:15	Pre-Onboarding	Welcome Message	E-learnings	Protocolo e Imagem	Introduction	Ethics and Business Conduct
09:15	09:30		Onboarding			Audit Basics	
09:30	09:45						Introduction to Aura
09:45	10:00	Break	Break			Break	Break
10:00	10:15	Pre-Onboarding				Audit Basics	Introduction to Aura
10:15	10:30						
10:30	10:45		Onboarding		Break		
10:45	11:00						Audit Documentation
11:00	11:15				Brand		
11:15	11:30	E-learnings					
11:30	11:45		Break				
11:45	12:00						
12:00	12:15		Onboarding				
12:15	12:30						
12:30	12:45	Almoço		Almoço		Almoço	Almoço
12:45	13:00						
13:00	13:15		Almoço		Almoço		
13:15	13:30						
13:30	13:45		Get to know your Line of Service		Risk Assurance Introduction	PwC Audit Overview	Audit Documentation
13:45	14:00	E-learnings		E-learnings			
14:00	14:15		Break		Break	Break	Break
14:15	14:30						
14:30	14:45		Get to know your Line of Service and Q&A		Risk Assurance Introduction	PwC Professional	Audit Documentation
14:45	15:00						Independence
15:00	15:15						
15:15	15:30		Closing Session			Time Management	
15:30	15:45						
15:45	16:00						
16:00	16:15						
16:15	16:30						
16:30	16:45						
16:45	17:00						

Fonte: Elaborado por PwC em janeiro de 2022

Tabela E2 - Formação Inicial Semana 2

Dia da Semana		*Semana 2*				
Horas		Segunda-feira	Terça-feira	Quarta-feira	Quinta-feira	Sexta-feira
		Assurance 1	Assurance 1	Assurance 1	Assurance 1	Assurance 1
09:00	09:15	Professional Scepticism	Fraud	Controls Testing	Substantive Testing	Substantive Testing
09:15	09:30					
09:30	09:45	Understanding the Business				
09:45	10:00					
10:00	10:15					
10:15	10:30					
10:30	10:45	Break	Break	Break	Break	Break
10:45	11:00					
11:00	11:15	Understanding the Business	Internal Control Framework	Controls Testing	Substantive Testing	Substantive Testing
11:15	11:30					
11:30	11:45					
11:45	12:00					
12:00	12:15					
12:15	12:30					
12:30	12:45	Almoço	Almoço	Almoço	Almoço	Almoço
12:45	13:00					
13:00	13:15					
13:15	13:30					
13:30	13:45					
13:45	14:00					
14:00	14:15	Introduction to Risk Assessment	Reconciliations	Controls Testing	Substantive Testing	Substantive Testing
14:15	14:30					
14:30	14:45					The Review Process
14:45	15:00			Substantive Testing		
15:00	15:15					
15:15	15:30	Break	Break	Break	Break	Break
15:30	15:45	Fraud	Reconciliations	Substantive Testing	Substantive Testing	Audit Trail and Referencing FS
15:45	16:00					
16:00	16:15					
16:15	16:30					
16:30	16:45					
16:45	17:00					

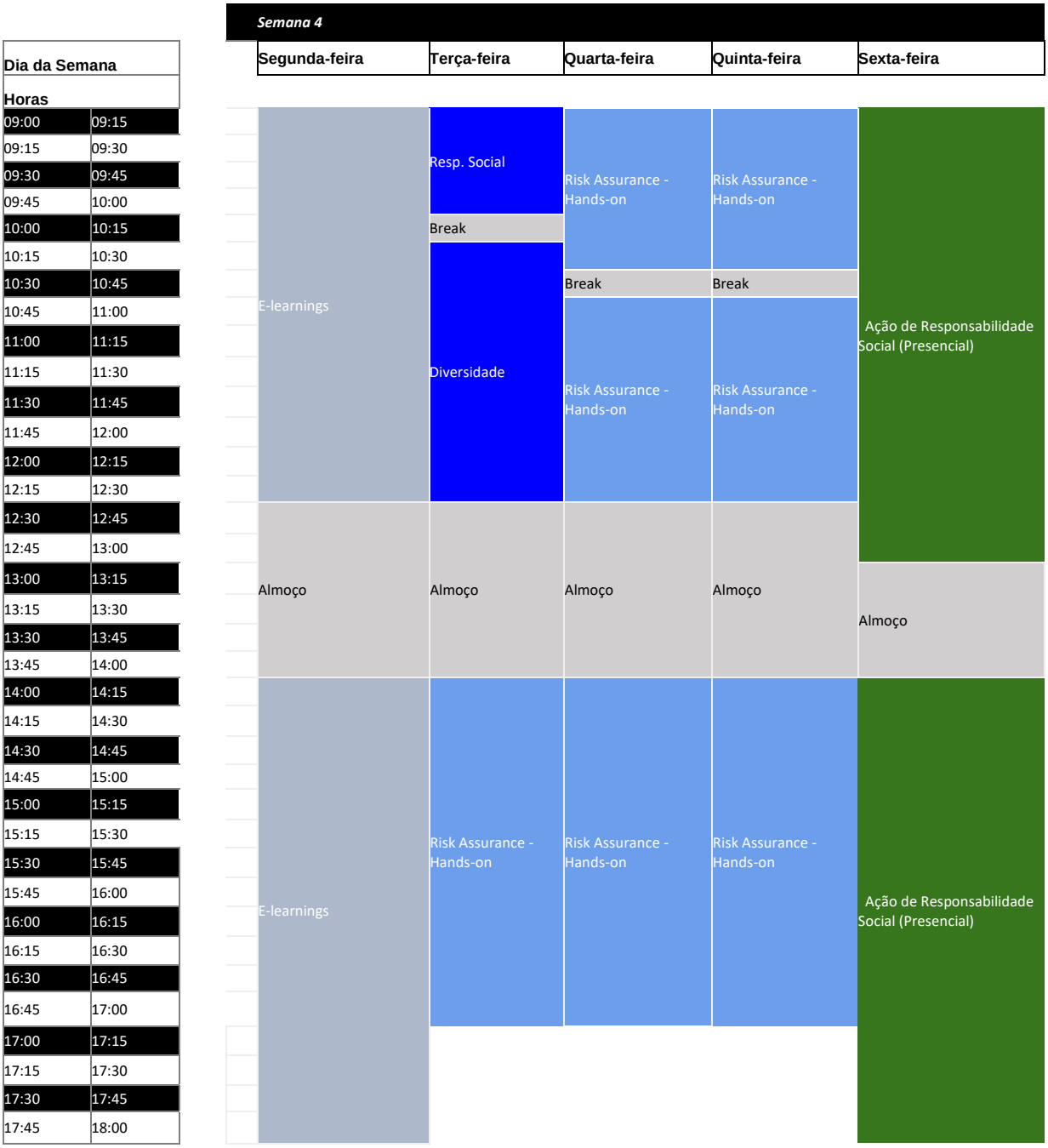
Fonte: Elaborado por PwC em janeiro de 2022

Tabela E3 - Formação Inicial Semana 3

Dia da Semana		*Semana 3*				
Horas		Segunda-feira	Terça-feira	Quarta-feira	Quinta-feira	Sexta-feira
			Assurance 1	Formação das LoS	Formação das LoS	Formação das LoS
09:00	09:15	Relationship Basics	Introducing Related Parties	Risk Assurance - Training Debrief & Next Steps	Risk Assurance - Hands-on	Risk Assurance - Hands-on
09:15	09:30					
09:30	09:45					
09:45	10:00					
10:00	10:15					
10:15	10:30		Introducing Estimates			
10:30	10:45		Break	Break	Break	Break
10:45	11:00		Introducing Estimates	Risk Assurance - Training Debrief & Next Steps	Risk Assurance - Hands-on	Risk Assurance - Hands-on
11:00	11:15					
11:15	11:30					
11:30	11:45					
11:45	12:00		Blackout			
12:00	12:15					
12:15	12:30					
12:30	12:45	Almoço	Almoço	Almoço	Almoço	Almoço
12:45	13:00					
13:00	13:15					
13:15	13:30					
13:30	13:45					
13:45	14:00					
14:00	14:15	E-learning	Blackout	Risk Assurance - Training Debrief & Next Steps	Risk Assurance - Hands-on	Risk Assurance - Hands-on
14:15	14:30					
14:30	14:45		Assurance Start - Foundations Block Assessment			
14:45	15:00					
15:00	15:15					
15:15	15:30		Break	Break	Break	Break
15:30	15:45		Assurance Start - Foundations Block Assessment Conclusion	Risk Assurance - Training Debrief & Next Steps	Risk Assurance - Hands-on	Risk Assurance - Hands-on
15:45	16:00					
16:00	16:15					
16:15	16:30					
16:30	16:45					
16:45	17:00					
17:00	17:15					
17:15	17:30					
17:30	17:45					
17:45	18:00					

Fonte: Elaborado por PwC em janeiro de 2022

Tabela E4 - Formação Inicial Semana 4



Fonte: Elaborado por PwC em janeiro de 2022