Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade
e Administração de Coimbra

Mónica Filipa Marques da Silva

Auditoria de Sistemas de Informação e a Utilização de CAATs

Coimbra, julho de 2021

Auditoria de Sistemas de Informação e a Utilização de CAATs
Mónica Filipa Marques da Silva
ISCAC | 2021

Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade
e Administração de Coimbra

Mónica Filipa Marques da Silva

Auditoria de Sistemas de Informação e a Utilização de CAATs

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria Empresarial e Pública, realizada sob a orientação da Professora Dra. Isabel Maria Mendes Pedrosa e Coorientação do Professor Dr. Francisco Santana Guimarães.

Coimbra, julho de 2021

TERMO DE RESPONSABILIDADE

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

"O período de maior ganho em conhecimento e experiência é o período mais difícil da vida de alguém."

Dalai Lama

AGRADECIMENTOS

A realização da presente Dissertação de Mestrado não seria possível sem o apoio das pessoas às quais expresso o meu profundo agradecimento:

Aos meus pais e irmão por todo o, indispensável, apoio e motivação que me transmitiram durante a elaboração deste trabalho e ao longo de toda a minha vida académica.

À minha orientadora Isabel Pedrosa pela disponibilidade, incentivo e cooperação no sentido de tornar o meu conhecimento em auditoria mais vasto, um sincero agradecimento pela dedicação em orientar a elaboração desta dissertação.

Ao meu coorientador Francisco Santana Guimarães por toda a colaboração, disponibilidade e apoio na divulgação do estudo empírico realizado nesta dissertação e pelo seu incentivo em tornar este trabalho mais completo.

Às minhas primas Anabela Azenha e Clarinda Azenha por sempre me incentivarem a seguir os meus sonhos e me ajudarem nesse sentido.

À minha grande amiga Inês Duarte que me acompanha sempre e é para mim um exemplo a seguir de garra e determinação.

Por fim, um agradecimento a todos aqueles que possibilitaram e contribuíram para a realização desta dissertação.

RESUMO

O rápido desenvolvimento tecnológico tem provocado, continuamente, grandes transformações na vida das pessoas e na sociedade organizacional e empresarial atual. Assim, podem verificar-se, em todas as áreas empresariais, inúmeras alterações, e a auditoria e os sistemas de informação não constituem exceção.

Neste contexto, verificou-se a importância de catalogar as diversas Ferramentas Informáticas de Suporte à Auditoria (*Computer-assisted Audit Techniques*, CAATs) que os auditores de Sistemas de Informação podem aplicar nas etapas de trabalho de campo e análise, em auditoria à integridade de dados, à segurança, à gestão de risco, entre outras. Deste modo, averiguar-se-á os impactos que a utilização das CAATs pode apresentar numa auditoria e as análises que podem ser executadas pelos Auditores de Sistemas de Informação através do uso dessas ferramentas.

Optou-se pela realização de um questionário, administrado aos membros do ISACA Lisbon Chapter, enquanto capítulo em Portugal da ISACA, método considerado o mais adequado para atingir os objetivos definidos relativamente ao uso de CAATs.

Concluiu-se que as ferramentas mais conhecidas e mais utilizadas entre os inquiridos são as de utilidade geral (Microsoft Excel, Microsoft Access e MySQL). Como mais conhecidas são também referidas CaseWare IDEA Analytics, TeamMate Audit Management, Galvanize e o Nessus. Os inquiridos mencionam que utilizam mais frequentemente CaseWare IDEA Analytics, Pentana Audit, Access, Excel, MySQL e ferramentas desenvolvidas pela própria empresa. Quanto às vantagens da utilização de CAATs para auditoria, os inquiridos destacam "maximização de tempo" e "agregação de valor ao trabalho de auditoria", bem como o contributo positivo no trabalho realizado.

Este estudo pretende contribuir para um melhor entendimento do uso das ferramentas e dos seus contextos de utilização por parte dos Auditores de Sistemas de Informação, com o propósito de trazer esse conhecimento para a Academia e para as empresas, em geral, mas também para qualquer auditor que pretenda aprofundar o seu conhecimento neste tema, em especial através do entendimento das vantagens e benefícios que as CAATs podem trazer ao trabalho destes profissionais.

Palavras-chave: Auditoria de Sistemas de Informação; Desenvolvimento Tecnológico; CAATs; Ferramentas para Auditoria.

ABSTRACT

The rapid technological development has continually caused great changes in people's lives and in the current organizational and business society. Thus, numerous changes can take place in all business areas, and auditing and information systems are no exception.

In this context, the importance of cataloging the various Computer-assisted Audit Techniques (CAATs) that Information Systems auditors can apply in the fieldwork and analysis stages, in auditing the integrity of data, security, risk management, among others. Thus, the impacts that the use of CAATs may have in an audit and the analyzes that can be performed by Information Systems Auditors through the use of these tools were investigated.

It was decided to carry out a questionnaire, administered to the members of the ISACA Lisbon Chapter, as a chapter of ISACA in Portugal, a method considered to be the most adequate to achieve the defined objectives regarding the use of CAATs.

It was concluded that the best-known and most used tools among the respondents are those of general utility (Microsoft Excel, Microsoft Access, and MySQL). As best known are also referred to CaseWare IDEA Analytics, TeamMate Audit Management, Galvanize, and Nessus. Respondents mention that they most frequently use CaseWare IDEA Analytics, Pentana Audit, Access, Excel, MySQL, and company-developed tools. As for the advantages of using CAATs for auditing, respondents highlight "maximization of time" and "adding value to the audit work", as well as the positive contribution to the work performed.

This study aims to contribute to a better understanding of the use of tools and their contexts of use by Information Systems Auditors, with the purpose of bringing this knowledge to the Academy and to companies in general, but also to any auditor who intends to deepen their knowledge on this topic, in particular by understanding the advantages and benefits that CAATs can bring to the work of these professionals.

Keywords: Information Systems Audit; Technological Development; CAATs; Audit Tools.

ÍNDICE GERAL

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

Lista de abreviaturas, acrónimos e siglas

ACL – *Audit Command Language*

AICPA – *American Institute of Certified Public Accountants*

ARM – *Access Rights Manager*

BDO – *Binder Dijker Otte*

CAAT – *Computer Assisted Audit Techniques*

CAATT – *Computer Assisted Audit Tools and Techniques*

CDPSE – *Certified Data Privacy Solutions Engineer*

CGEIT – *Certified in the Governance of Enterprise IT*

CIA – *Certified Internal Auditor*

CISA – *Certified Information Systems Auditor*

CISM – *Certified Information Security Manager*

CPA – *Certified Public Accountant*

CRISC – *Certified in Risk and Information Systems Control*

CSX-P – *Cybersecurity Practitioner*

DRAI – Dossier de Revisão/Auditoria Informatizado

EDP – *Electronic Data Processing*

EPA – *Environmental Protection Agency*

FDA – *Food and Drug Administration*

GAS – *Generalized Audit Software*

IDEA – *Interactive Data Extraction and Analysis*

IFAC – *International Federation of Accountants*

IIA – *Institute of Internal Auditors*

IPAI – Instituto Português de Auditoria Interna

IPPF – *International Professional Practices Framework*

ISA – *International Standards on Auditing*

ISACA – *Information Systems Audit and Control Association*

ISO – *International Standard Organization*

KPIs – *Key Performance Indicator*

NUTS – Nomenclatura das Unidades Territoriais para Fins Estatísticos

OSHA – *Occupational Safety and Health Administration*

POC – Plano Oficial de Contabilidade

SAS – *Statement on Audit Standards*

SI – Sistemas de Informação

SIPTA – Sistema Informático de Papéis de Trabalho de Auditoria

SNC – Sistema de Normalização Contabilística

TAAC – Técnicas de Auditoria Assistidas por Computador

TI – Tecnologias de Informação

INTRODUÇÃO

O grande e rápido desenvolvimento tecnológico tem provocado continuamente grandes transformações na vida das pessoas e na sociedade organizacional e empresarial atual onde impera a velocidade de processamento de dados, o volume de dados e a adoção de novas tecnologias com impacto ao nível dos processos e riscos associados. Assim, a partir deste desenvolvimento pode verificar-se em todas as áreas empresariais inúmeras alterações e vantagens, e a auditoria não é exceção, quer pela necessidade de adoção de tecnologia para otimizar os seus processos, quer porque o âmbito da auditoria depende da análise de dados e de tecnologias de suporte aos processos.

Desta forma, com todo o desenvolvimento tecnológico, as empresas recorrem ao uso de meios informáticos para processar e guardar os seus dados o que traz inúmeras vantagens, como por exemplo em termos de acessibilidade aos dados, na rapidez do processamento da informação, na estruturação dos dados, entre outras. Posto isto, também os auditores na realização de uma auditoria, têm a possibilidade de tirar partido das vantagens das novas tecnologias. No entanto, é necessário conhecer as ferramentas informáticas de apoio à auditoria (CAATs), as suas potencialidades e como estas podem apoiar o trabalho do auditor.

Numa organização é importante que a informação seja fiável, tanto para a tomada de decisões, quer como forma de controlo de gestão, quer para a divulgação desta perante os restantes *stakeholders*. Deste modo, é importante para o auditor de sistemas de informação (SI) aprimorar-se na sua forma de atuação de extração e análise de dados.

Motivação

A motivação para a realização deste trabalho provém da existência de muitas ferramentas de suporte à auditoria de Sistemas de Informação e da importância de as catalogar para que possa ser mais fácil, por parte do auditor, identificar a(as) ferramenta(as) que mais se enquadram na auditoria que pretende realizar, com o intuito de tornar o trabalho de auditoria mais eficiente e eficaz.

Outra motivação foi a de verificar como as empresas e os auditores utilizam estas ferramentas de TI de suporte à auditoria.

Objetivos de investigação

A presente investigação tem como principais objetivos de estudo responder às seguintes questões:

- Quais as áreas de enfoque de uma auditoria de sistemas de informação?

- Quais os impactos de uma auditoria de sistemas de informação na organização auditada?

- Que CAATs podem os auditores de sistemas de informação aplicar nas etapas de trabalho de campo e análise?

- Que análises podem os auditores de sistemas de informação realizar através destas ferramentas de auditoria auxiliadas por computador?

- Que vantagens podem trazer as CAATs para o trabalho dos auditores?

Metodologia

Como metodologia utilizada para responder aos objetivos definidos, este estudo será realizado através de uma revisão sistemática da literatura sobre o tema em análise, recorrendo a livros, artigos, sites institucionais e dissertações. Por fim, realizar-se-á um questionário junto dos membros do ISACA (*Information Systems Audit and Control Association*) Lisbon Chapter já que, atendendo ao facto de ser o *Chapter* Português de um organismo representante dos profissionais da área de Auditoria de Sistemas de Informação, considerou.se ser a melhor forma de se recolher as perceções dos profissionais da área. Posteriormente, realizou-se a análise das respostas às questões realizadas e a discussão dos resultados.

Estrutura do trabalho

A presente dissertação é composta por quatro capítulos: após este primeiro capítulo introdutório, o capítulo seguinte apresenta a revisão da literatura, ao qual se segue o capítulo correspondente ao estudo empírico e, por fim, o capítulo onde se enunciam as principais conclusões e limitações desta dissertação, contributos e uma exposição sobre trabalhos futuros.

No capítulo 1 é realizada a introdução ao trabalho através de um breve enquadramento e contextualização do tema em estudo. Segue-se a motivação para a realização deste trabalho, uma breve apresentação dos objetivos, com a apresentação das questões

propostas para estudo, metodologia de estudo e, no final do capítulo, é apresentada a estrutura deste trabalho e a contribuição que se pretende dar com a elaboração do mesmo.

O capítulo da revisão da literatura apresenta-se subdividido em 4 partes. Numa primeira fase serão estudados os conceitos de auditoria e auditoria de sistemas de informação, seguidamente identificadas quais as áreas de SI, como é classificada uma auditoria e quais as tipificações de auditorias de sistemas de informação existentes. Numa segunda parte será realizada uma abordagem relacionada com os auditores de SI no que respeita à evolução do papel do auditor de SI, aos contributos dos SI para o trabalho do auditor, aos impactos da auditoria de SI para a organização auditada e referidas algumas das certificações que podem ser obtidas pelo auditor de SI.

Numa terceira parte dar-se-á enfase às Computer Assistted Audit Tools (CAATs), nomeadamente a sua origem, evolução e definição, quais as classificações existentes relativas às CAATs. Serão também destacadas ferramentas informáticas que podem ser utilizadas para apoiar o trabalho realizado pelos auditores, apresenta-se a relação entre os tipos de auditoria de SI e as tipologias de CAATs e, por último, serão abordados quais custos e benefícios associados à utilização das CAATs numa auditoria.

Por fim, serão apresentadas as conclusões referentes à revisão da literatura, o que permitirá destacar os aspetos mais relevantes, de modo a permitir uma melhor discussão dos resultados do questionário.

No capítulo sobre o estudo empírico será indicada a metodologia de investigação, o instrumento para recolha dos dados. Seguidamente será realizada a análise de dados obtidos e, por fim, a discussão dos resultados obtidos através do questionário e a conclusão do estudo, com os aspetos fundamentais e principais a reter do estudo realizado.

No capítulo correspondente à conclusão, serão expostas as principais conclusões da dissertação sobre o tema em estudo, será feita referência aos contributos e limitações encontradas durante a elaboração da presente dissertação. E, por fim, será apresentada uma reflexão sobre trabalhos futuros que poderão ser vir a ser considerados pelos investigadores interessados neste tema.

Contribuição

Com este trabalho pretende-se auxiliar, principalmente, auditores e interessados nas temáticas de auditoria de Sistemas de Informação e CAATs para Auditoria a SI, de modo

a dar conhecimento de e sobre ferramentas de apoio à auditoria e de que modo estas contribuem para os trabalhos de auditoria.

Desta forma, pretende-se que, com o conhecimento da existência de várias ferramentas disponíveis no mercado e das suas funcionalidades, seja possível a escolha da mais adequada, tendo em conta os objetivos e as necessidades da auditoria que se pretende realizar.

Por outro lado, com esta investigação espera-se contribuir para impulsionar o desenvolvimento de trabalhos futuros, relacionados com este tema, motivando outros alunos desta área a investir neste domínio de investigação.

1 Revisão da Literatura

Após uma introdução, na qual é realizada, nomeadamente, uma contextualização dos objetivos propostos para estudo, é através de uma análise bibliográfica e exploratória que neste capítulo irá ser feita a revisão da literatura.

Assim, neste capítulo serão abordados, através de um enquadramento teórico, alguns conceitos sobre auditoria e técnicas de auditoria assistida por computador (*Computer-assisted Audit Techniques*, CAATs), será feita referência às áreas de SI e aos tipos de auditoria e tipos de auditoria de SI.

Com base em vários tipos de bibliografia, segue-se uma abordagem à origem, evolução, definição e classificação de CAATs. Seguidamente, será realizada uma apresentação de algumas CAATs, identificando que análises os auditores poderão realizar através destas técnicas, seguido da referência a custos e benefícios da utilização destas técnicas para a auditoria e para a organização.

Por fim, será dada ênfase à evolução do papel do auditor, serão mencionados os contributos dos SI para o trabalho do auditor, quais os impactos de uma auditoria de SI para uma organização e mencionadas algumas das certificações que podem ser obtidas pelo auditor de SI.

1.1 Auditoria

Nesta secção serão abordados os conceitos de auditoria e auditoria de sistemas de informação, serão identificadas as áreas de SI, será feita referência a como pode ser classificada uma auditoria, fazendo por isso referência aos diversos tipos de auditorias e ainda à tipificação de auditorias de sistemas de informação.

1.1.1 Conceito de auditoria

O conceito de auditoria tem evoluído com o decorrer dos anos, refletindo as alterações relativas ao desenvolvimento e aos objetivos das organizações. No entanto, embora existam várias definições de auditoria, estas possuem uma aceitação generalizada.

Segundo Morais e Martins "*A auditoria é o processo sistemático de objetivamente obter e avaliar prova acerca da correspondência entre informações, situações ou*

procedimentos e critérios preestabelecidos, assim como comunicar conclusões aos interessados." (Morais & Martins, 2013, p. 19).

No glossário do ISACA (2015) a auditoria é definida como uma inspeção/verificação formal para apurar se o *standard* ou conjunto de normas estão a ser implementadas e seguidas, se os registos são precisos e as metas a ser atingidas com eficiência e eficácia. É mencionado ainda que uma auditoria pode ser efetuada por auditores internos e/ou externos.

Para Teruel a auditoria deve atuar de forma sistemática na organização, priorizando a "*avaliação dos processos de governança, gestão de risco e controle"* e deve aturar de "*forma complementar, na avaliação das principais actividades, processos e produtos da organização*" (Teruel, 2010, p. 2), com especial atenção para os tidos em conta como vitais para o alcance dos objetivos estratégicos.

Por fim, para o Tribunal de Contas, *"na esfera financeira a auditoria é um exame ou verificação das contas, da situação financeira e/ou da gestão, realizada por um auditor com vista à emissão de um parecer."* (Tribunal de Contas, 1999, p. 22).

1.1.2 Áreas de sistemas de informação

Segundo Guimarães (2018), através da menção a Laudon e Laudon (2012), os SI correspondem a "*um conjunto de componentes interligados que permitem recolher, processar, armazenar e distribuir informação para a tomada de decisão e controlo da própria organização*" (Guimarães, 2018, p. 58).

Ainda para Guimarães (2018), segundo Keri et al. (2006) os SI são uma combinação de tecnologia, pessoas e processos de forma a facilitar a comunicação de dados, informação e conhecimento.

Relativamente às áreas de SI, Guimarães (2018) faz referência a Potter et al. (2005) que indica como componentes/áreas de SI o *hardware, software*, base de dados, redes de comunicações e ainda procedimentos e as pessoas. Também Bourgeois (2021) refere que os SI são combinações de *hardware*, *software* e redes de comunicações.

Desta forma, serão considerados como áreas de SI o *hardware, software*, base de dados e redes de comunicações enquanto base da tecnologia aplicada às empresas, sendo que os procedimentos remetem para a formalização de forma de trabalhar onde os controlos

aplicáveis face a riscos estão sistematizados, e as pessoas são intervenientes que interagem com os SI.

1.1.3 Conceito de auditoria de sistemas de informação

Segundo Morais e Martins (2013) uma auditoria de sistemas de informação inclui-se numa auditoria interna, uma vez que é uma atribuição desta assegurar a fiabilidade da informação gerada pela organização, informação essa que é utilizada pelos diversos *stakeholders*. No entanto, no que diz respeito ao sujeito que efetua a auditoria, nenhum dos autores a seguir mencionados indica a auditoria de SI como uma auditoria interna ou externa, podendo esta, na minha perspetiva, realizar-se em qualquer um dos âmbitos.

Uma auditoria de SI é considerada um exame aos controlos de gestão dentro de uma infraestrutura de TI e essa avaliação das evidências obtidas indica se os SI protegem os ativos, mantendo a integridade dos dados de uma organização. Estas avaliações "*podem ser realizadas em conjunto com uma auditoria de demostração financeira, uma auditoria interna*" (ISACA, 2014, p. 47) ou outro tipo de auditoria.

Assim, uma auditoria de SI tem como objetivo avaliar se os SI estarão disponíveis para a empresa o tempo todo (disponibilidade), se a informação presente nos sistemas é divulgada apenas a pessoas autorizadas (segurança e confidencialidade) e se a informação fornecida pelo sistema é sempre precisa, confiável e oportuna (integridade). Desta forma, a auditoria de SI pretende avaliar os riscos relacionados com a informação, um ativo muito valioso para as empresas e indicar recomendações para minimizar esses riscos (ISACA, 2014).

Segundo Sayana, Ron Weber define auditoria de sistemas de informação como o "*processo de recolha e avaliação de evidências para determinar se um SI protege os ativos, mantém a integridade dos dados, alcança os objetivos organizacionais de forma eficaz e consome recursos de forma eficiente*" (Sayana, 2002, p. 1).

Sayana refere ainda que uma auditoria de SI "*faz parte do processo geral de uma auditoria*" (Sayana, 2002, p. 1), sendo esta um dos facilitadores de uma boa gestão organizacional.

Teruel indica que esta auditoria pressupõe uma avaliação aos sistemas de informação e aos recursos tecnológicos que abrangem "*o processo de geração, guarda e disponibilização da informação*" na organização (Teruel, 2010, p. 2).

Assim, para que a informação, utilizada pelos *stakeholders* na tomada de decisão, seja fiável é de extrema importância a função de auditoria, para uma promoção da adequação, revisão, avaliação e indicação de recomendações para um aperfeiçoamento dos controlos internos no que diz respeito aos SI da organização.

Para Teruel (2010) uma auditoria de SI engloba ainda uma avaliação relativamente à utilização dos recursos humanos, materiais e recursos tecnológicos relativamente aos SI utilizados. Desta abordagem, entende-se que o autor faz referência não só a uma auditoria aos dados armazenados, mas também à adequação dos SI (recursos tecnológicos), à formação dos recursos humanos para fazer uma correta utilização dos SI. Estas referências à auditoria aos dados armazenados e aos recursos tecnológicos é também tida em consideração pelo Tribunal de Contas, como iremos constatar na referência feita seguidamente ao Tribunal de Contas. No entanto entende-se também que o autor faz referência ao acondicionamento dos sistemas de informação (recursos materiais).

Teruel salienta ainda que os recursos informáticos são utilizados para auditar a informação presente em meios tecnológicos, no entanto estes meios permitem também "*automatizar todos os processos de auditoria*" (Teruel, 2010, p. 2). Assim sendo, são utlizados como recursos informáticos, técnicas de auditoria assistida por computador (CAATs).

O Tribunal de Contas considera que uma auditoria de sistemas de informação consiste no "*exame de dados registados em suporte informático, incluindo a avaliação do próprio sistema informático: aplicações, sistema de gestão e programas*." (Tribunal de Contas, 1999, p. 62).

Na auditoria, em especial na avaliação do controlo interno, é importante referir que o "*auditor pode ser afectado no seu trabalho não só por erros nos dados (...) recolhidos, tratados, arquivados ou emitidos pela informática como também por erros dos programas informáticos ou na utilização da informática"* (Tribunal de Contas, 1999, p. 62).

Desta feita, é considerado relevante pelo Tribunal de Contas (1999), uma avaliação dos sistemas informáticos existentes na organização, na fase de análise, programação e execução.

1.1.4 Tipos de auditoria

Segundo Morais e Martins (2013) a auditoria pode ser classificada considerando diferentes e vários critérios:

a) Quanto ao conteúdo e fins;
b) Quanto à amplitude;
c) Quanto à frequência;
d) Quanto ao período temporal;
e) Quanto à obrigatoriedade;
f) Quanto ao sujeito que a efetua.

De acordo com o Tribunal de Contas (1999) os critérios de classificação de uma auditoria são os seguintes:

a) Quanto ao objetivo;
b) Quanto ao sujeito que a realiza;
c) Quanto à amplitude;
d) Quanto à periodicidade;
e) Quanto à profundidade.

Assim, seguidamente irão ser feitas algumas considerações aos critérios indicados anteriormente, comparando as diferentes fontes e tendo por base a classificação das autoras Morais e Martins (2013).

Quanto ao **conteúdo** incluem-se auditorias financeiras, auditoria das demonstrações financeiras e auditorias não financeiras, nomeadamente auditorias de conformidade e auditorias operacionais. Segundo Morais e Martins (2013) existem ainda auditorias de gestão e auditorias estratégicas. Por sua vez o Tribunal de contas faz referência a "*auditorias de contas, da situação financeira, de legalidade e regularidade e auditorias de gestão*" (Tribunal de Contas, 1999, p. 24).

Auditoria das demonstrações financeiras "*consiste num exame às demonstrações financeiras com o objetivo de expressar uma opinião sobre a conformidade, ou não, de acordo com os critérios preestabelecidos*" (Morais & Martins, 2013, p. 20). O relatório destas auditorias é comunicado a todos os *stakeholders.*

Uma auditoria de conformidade incide sobre a verificação do cumprimento por parte da entidade auditada, de condições, regras e regulamentos especificados por várias fontes, externas ou internas. Os resultados de uma auditoria de conformidade são comunicados geralmente à autoridade que definiu os critérios a cumprir.

Uma auditoria operacional possui o objetivo de avaliar a economia, a eficiência e eficácia das atividades e/ou operações de uma entidade, com base numa revisão sistemática das áreas operacionais desta. O resultado deste tipo de auditoria é comunicado somente à entidade que a solicitou.

Quanto a uma Auditoria de gestão, esta consta "*na avaliação da performance da entidade e o desempenho dos gestores*." (Morais & Martins, 2013, p. 21).

No que diz respeito a uma auditoria de estratégia, esta consta de uma avaliação da conformidade das decisões tendo em conta as políticas estratégicas anteriormente estabelecidas.

Quanto à **amplitude**, uma auditoria pode ser considerada geral ou parcial. Uma auditoria geral envolve a totalidade da entidade auditada, deste modo pretende-se obter uma visão global da entidade. Assim, como refere o Tribunal de Contas no caso de uma "*auditoria financeira, obriga a examinar todas as parcelas contabilísticas mas não exige um exame completo e integral de cada uma delas.*" (Tribunal de Contas, 1999, p. 24).

Por sua vez, uma auditoria parcial cinge-se apenas a uma parte da entidade, e pode referir-se a uma ou várias atividades, áreas, setores ou projetos. O Tribunal de Contas faz ainda referência a que auditorias parciais podem ser orientas, realizando exames profundos sobre setor, área ou procedimento; horizontal, que consta no exame de um tema específico junto de várias áreas ou serviços; de projetos e programas, onde é englobado o acompanhamento, exame e avaliação da execução de programas e projetos governamentais específicos.

Quanto à **frequência,** Morais e Martins (2013) referem que uma auditoria pode ser permanente, isto quando é realizada por diversas vezes ao longo do período, de forma regular ou irregular, possibilitando um acompanhamento contínuo; ou ocasional/única

quando é realizada de forma pontual, quando ocorre algo imprevisto ou é necessário solucionar algum tema especial.

Ainda relativamente à frequência, o Tribunal de Contas (1999) faz, ainda, referência a uma auditoria de fim de exercício cujo objetivo é apurar a seriedade dos documentos de prestação de contas.

Quanto ao **período temporal**, apenas Morais e Martins (2013) faz referência podendo uma auditoria considerar-se de informação histórica ou de informação previsional ou prospetiva. Relativamente à auditoria da informação histórica, esta possui como objeto um conjunto de informação do passado, sendo desta forma a auditoria elaborada à *posteriori.* Numa auditoria da informação previsional o objeto é um conjunto de informação prospetiva/futura, sendo a auditoria elaborada à *priori*. Desta forma, a auditoria "*baseia-se em técnicas de avaliação acerca da validade de previsões*" (Morais & Martins, 2013, p. 21).

Quanto à **obrigatoriedade** apenas Morais e Martins (2013) faz referência, referindo que uma auditoria pode classificar-se de fonte contratual, ocorrendo esta com base "*num contrato de prestação de serviços, sendo facultativa*" (Morais & Martins, 2013, p. 21) ou auditoria de fonte legal, estando está baseada num normativo legal. Por exemplo, nos hospitais EPE (Entidades Públicas Empresariais) as auditorias internas são obrigatórias, com base legal no Decreto-Lei n.º 244/2012 de 9 de novembro.

Quanto ao **sujeito que a efetua** uma auditoria pode classificar-se interna "*se efetuada por quadros da entidade ou não, normalmente organizados num departamento, subordinados à autoridade máxima"* (Morais & Martins, 2013, p. 22) ou externa se elaborada por profissionais externos que estão numa posição de independência relativamente à entidade auditada. Neste tema constata-se que ambas as fontes estão em concordância.

Em norma, uma auditoria enquadra-se, em vários critérios classificativos. Assim, por exemplo uma auditoria de conformidade pode ser também uma auditoria parcial, uma auditoria ocasional.

O Tribunal de Conta (1999) faz ainda referência à **profundidade**, onde uma auditoria pode ser completa ou por provas/sondagens. Uma auditoria completa consiste na análise de todas as operações efetuadas no período em causa, podendo ocorrer numa auditoria geral ou parcial. Uma auditoria por provas ou sondagens "*consiste em comprovar a*

exactidão de um certo número de lançamentos, cálculos ou registos, escolhidos ao acaso de entre o conjunto a examinar." (Tribunal de Contas, 1999, p. 26).

Deste modo, constata-se que embora existam algumas divergências/diferenças, os critérios de classificação de auditoria referidos pelas autoras Morais e Martins (2013) e pelo Tribunal de Contas (1999) são idênticos.

Quanto aos tipos de abordagem de auditoria de sistemas de informação Duque e Arias (2012) refere a auditoria ao redor do computador, a auditoria com o computador e a auditoria através do computador.

1.1.5 Tipos de auditoria de SI

Duque (2017) classifica a auditoria de SI em três enfoques gerais, nomeadamente, auditoria ao redor do computador, auditoria com o computador e auditoria através do computador.

Desta forma, a auditoria ao redor do computador caracteriza-se por conciliar e auditar os documentos que deram origem aos registos de entrada no computador com os resultados gerados pelo computador. Esta é a abordagem mais simples, uma vez que o conhecimento requerido de TI é pouco.

A auditoria com o computador consiste no uso de *software* de auditoria generalizado, GAS (*Generalized Audit Software*), que implica o uso do computador para realizar tarefas de auditoria nas suas diferentes fases, através do uso de diferentes aplicações especializadas ou genéricas. Desta forma, Duque (2017) afirma que nesta tipologia é realizado um uso mais intensivo das ferramentas tecnológicas do que de técnicas de auditoria.

Por fim, a auditoria através do computador está associada diretamente ao uso de CAATs, e consiste na avaliação, por parte do auditor, da tecnologia para determinar a confiabilidade das operações que não podem ser vistas através de olho humano e também no teste de eficácia operacional dos controlos tecnológicos. Assim, esta tipologia, ao contrário das anteriores, realiza um uso mais intensivo das técnicas de auditoria do que das ferramentas tecnológicas e é nesta tipologia que se enquadra a auditoria contínua.

Realizando uma análise mais profunda, Gelbstein (2017) apresenta os seguintes tipos de auditoria de SI:

- Governance – estratégia de SI/TI, políticas, decisões de fornecimento, recursos humanos, acompanhamento de desempenho;
- Operações 1 – relacionadas com *data centers*, redes locais e amplas, segurança física e lógica, recuperação de desastres e continuidade de negócios, redes locais e acesso à Internet por filiais longe da sede;
- Operações 2 – Sistemas e tecnologias não gerenciados pela função SI/TI, sistemas tipicamente industriais de automação e controle de supervisão e aquisição de dados;
- Prestadores externos de serviços – Telecomunicações, terceirização, prestadores de serviços em nuvem, empresas de manutenção, consultores, auditores, gestão de contratos e relacionamentos, acompanhamento de desempenho e gestão (tanto na sede quanto delegados a escritórios remotos);
- Aplicativos de negócios – *Software*, aplicativos móveis, gestão de licenças, atualizações, *patches* e correções, gestão de alterações, certificação;
- Mobilidade – Acesso a dados corporativos confidenciais, participação em redes sociais, divulgações de informações confidenciais, relacionado com o acesso à informação da organização em qualquer lugar, através de qualquer dispositivo com acesso à internet;
- Segurança – *frameworks* (ex. ISO 27001), certificações, violações/fraudes;
- Gestão de riscos – avaliação do risco, medidas de mitigação, revisões;
- Dados – qualidade, classificação, modelos de dados, administração de banco de dados;
- Projetos SI/TI – desvios relativos ao planeamento em termos de tempo/orçamento, gestão de mudanças, gestão de projetos, mudanças de áreas de risco.

Ambos os autores, Duque e Gelbstein, apresentam tipologias relacionadas com a auditoria de SI distintas, no entanto a meu ver Gelbstein apresenta uma abordagem mais aprofundada e que se pode relacionar com as áreas de enfoque que podem ser alvo de uma auditoria de SI, numa organização.

Realizando agora uma ligação entre os tipos de auditoria de SI, abordados nos parágrafos anteriores e as áreas de SI (ver tópico 1.1.2 - Áreas de sistemas de informação), pode estabelecer-se uma relação entre o governance e todas as áreas, uma vez que o governance está relacionado com a estratégia da organização, o que a meu ver está relacionado com

todas as áreas de SI, nomeadamente *software, hardware*, banco de dados e redes de comunicações.

As operações 1, por estarem relacionadas com *data centers*, segurança física, redes locais e acesso à internet por filiais longe da sede estabelecem por isso uma ligação com as áreas de redes de comunicações e *hardware,* por sua vez o tipo de auditoria de SI operações 2, relacionado com sistemas, está relacionado com a área de SI de *software.*

Relativamente ao tipo de auditoria de SI a prestadores externos de serviços, relacionados com telecomunicações e prestação de serviços em nuvem, pode estabelecer-se uma ligação com a área de SI de redes de comunicações. O tipo de auditoria de SI a aplicativos de negócios estabelece ligação com a área de SI de *software* e o tipo de auditoria de SI, mobilidade, ou seja, o acesso à informação da organização em qualquer lugar estabelece principalmente uma ligação com a área de SI de redes de comunicações.

No que diz respeito aos tipos de auditoria de SI à segurança e à gestão de riscos, na minha perspetiva abrangem todas as áreas de SI, uma vez que são temas/tipos de auditoria de SI transversais a todas as áreas. Por fim, os tipos de auditoria de SI aos dados e a projetos de SI/TI estão maioritariamente interligados às áreas de SI de base de dados.

1.2 Auditores de Sistemas de Informação

Este ponto será dedicado maioritariamente aos auditores de SI e nele será feita referência à evolução do papel do auditor, aos SI para o auditor, ou seja, quais os contributos dos SI para o trabalho do auditor, será também referido de que forma os auditores têm de se por a par da evolução tecnológica para retirar um melhor partido desta para a auditoria e consequentemente para a organização. Neste tópico serão ainda abordados os impactos da auditoria de SI para a organização e por fim serão referidas algumas das certificações que podem ser obtidas pelo auditor de SI.

1.2.1 Evolução do Papel do Auditor

A utilização de CAATs e a auditoria, como verificado anteriormente, têm sofrido uma evolução ao longo dos anos, e por isso, para que exista um acompanhamento destas evoluções, também o papel do auditor tem evoluído e sofrido alterações.

A partir de uma análise realizada por Silva (2007) que distingue a Era da auditoria e o papel do auditor em cada Era, podemos verificar a evolução do seu papel na auditoria. Desta forma, o autor apresenta-nos a Era da auditoria baseada na inspeção, em que o papel do auditor estava focado na inspeção, na recontagem e na realização de testes substantivos (evidências suficientes, confiáveis e relevantes sobre os dados).

Seguidamente indica-se a Era da auditoria com base no controlo, na qual o papel do auditor passou a ser focado na adequação aos controlos e às políticas definidas e na execução de auditorias operacionais, levando a auditoria para uma forma mais abrangente ao nível organizacional. (Silva, 2007)

Na Era da auditoria baseada no risco, o papel do auditor foca-se "*na mitigação dos riscos verificando a definição e a execução dos controlos ao nível das entidades e dos processos de negócio*" (Silva, 2007, p. 23) e passa também a fazer parte do papel do auditor não assumir à partida que os controlos que estão implementados são os mais adequados. Nesta Era os auditores passam também a ver o risco de um forma mais holística, ou seja, mais abrangente, muito para além dos riscos financeiros, passando a considerar outros riscos organizacionais, como os riscos associados por exemplo aos sistemas e tecnologias de informação, entre outros.

Por fim, é-nos apresentada na abordagem realizada por Silva (2007) a auditoria baseada na continuidade, onde os auditores necessitam de acompanhar o elevado ritmo de mudança nos negócios e necessitam também de apresentar relatórios de conformidade de forma cada vez mais rápida e continua. Nesta Era, os auditores, no desempenho do seu papel intensificam o uso de CAATs e são também levados a detetar e reportar aos comités de auditoria e aos *stakeholders* de forma quase imediata violações ou quebras nos controlos.

Ao nível do risco, nesta Era é identificada a necessidade de os auditores compreenderem os crescentes riscos associados à informação e aos sistemas e tecnologias de informação e comunicação, a necessidade de adaptarem a avaliação dos riscos de modo a incorporar os riscos associados aos ativos intangíveis, como a relação com o cliente, o capital humano, a gestão da marca e ainda compreender e considerar na avaliação do risco fatores que recaem sobre a continuidade de negócio, fatores externos ou a responsabilidade social corporativa, entre outros.

Por fim, nesta Era focada na continuidade, pode identificar-se a necessidade de os auditores realizarem desenvolvimentos e implementações no que diz respeito a sistemas de monitorização que permitam um continua avaliação do risco e consequente atualização do plano e das prioridades das auditorias.

Desta forma, pode concluir-se que estas evoluções ao nível da auditoria levaram a alterações e evoluções no que diz respeito ao papel que o auditor desempenha, sendo requerido um acompanhamento das competências dos auditores, nomeadamente através de formação específica (certificações e especializações tecnológicas) e conhecimentos abrangentes, a nível operacional e de negócio (gestão, comunicação, etc.).

1.2.2 Os SI para o Auditor

Ribeiro (2017, p. 68) defende que utilização de *software* em auditoria tem como "*objetivo (…) proporcionar aos profissionais uma garantia de consistência e plenitude na aplicação das normas, ao mesmo tempo que reduzem o tempo de trabalho."*

Segundo o mesmo autor, este afirma que o *software* de gestão documental de auditoria pretende proporcionar "*meios para apoiar os auditores ao longo de todo o trabalho, assegurando o cumprimento dos requisitos de documentação, bem como das normas específicas associadas a cada uma das fases do processo de auditoria. Contudo, ao nível de cada entidade a auditar, nomeadamente quanto aos seus factores de risco e às especificidades do setor de atividade, exige-se ao auditor que este aplique o seu conhecimento e experiência para garantir que decisões tomadas em algumas matérias são as mais adequadas (por exemplo materialidade, natureza e extensão dos procedimentos, avaliação da evidência recolhida).*" (Ribeiro, 2017, p. 68).

Posto isto, a par da evolução tecnológica que se pode observar ao longo dos anos e do apoio proporcionado aos auditores através de *software* é importante, segundo Marques, referido por Brito (2015, p. 62) que os auditores desenvolvam "*um esforço continuado de formação e de aperfeiçoamento profissional, com o objectivo de ir acompanhando e utilizando as vantagens dessa evolução tecnológica.*"

Porto (2011) refere ainda a importância de os auditores de TI possuírem e desenvolverem aptidões e habilidade (através de formações, certificações, etc.) para a utilização das CAATs de forma a estarem preparados para obter o máximo de benefícios para uma

auditoria. É igualmente importante os auditores conhecerem as CAATs disponíveis no mercado, saberem avaliar as necessidades da auditoria, de modo a identificarem o ajuste adequado entre as ferramentas a utilizar e os objetivos da auditoria.

Os auditores possuem a responsabilidade, entre outras, de análise, planeamento e execução dos procedimentos e testes a serem realizados numa auditoria, assim torna-se importante os auditores conhecerem as CAATs disponíveis no mercado, uma vez que os testes a serem realizados são projetados consoante o seu conhecimento do negócio e das CAATs a serem utilizadas. Assim, serão destacadas seguidamente algumas análises que os auditores podem realizar através e dependendo das CAATs que utilizam.

Sayana (2003) destaca como análises realizadas através de CAATs, a consulta de dados, a estratificação de dados, extração de amostras, identificação de dados em falta, análises estatísticas, cálculos, realização de operações após combinar e juntar arquivos e tabelas. O autor ressalta também a utilização de ferramentas que permitem verificar configurações de parâmetros relacionados com a segurança.

Segundo Duque (2012), outros procedimentos e análises que podem ser realizados com uso de CAATs são provas detalhadas de transações e balancetes, realizando recálculos e analises de valores, que se encontram acima de um certo valor, realização de procedimentos analíticos, testes aos controlos gerais, extração de amostras, cruzamento de registos extraídos de múltiplas fontes de dados e deteção de resultados não válidos.

Através de um estudo mais profundo, Francisco (2013) apresenta as seguintes análises possíveis de realizar com base na utilização de CAATs, nomeadamente a análise de campos de dados vazios, em branco ou de caracteres inválidos, análise de duplicações, de lacunas (como falta de pagamentos/recebimentos, ordens de compra não registadas) e de exceções para valores nominais (transações fora do normal, como quantidade negativas de stocks, compras com o mesmo valor, compras em dias de fim-de-semana ou feriados).

Francisco (2013) faz também a referência à análise de rácios e de tendências. A análise de tendências foca-se apenas na evolução temporal dos dados a analisar, no entanto esta análise não é a mais adequada de utilizar em períodos de instabilidade ou alterações no contexto em que a organização se insere.

No que diz respeito à análise de rácios, esta pode ser realizada entre o valor mais alto e o valor mais baixo, entre o valor mais alto e segundo valor mais alto e entre o ano corrente e anos anteriores. Desta forma, é possível realizar comparações e verificar alterações

significativas nos valores dos rácios, que podem indicar erros materiais ou fraude. Desta abordagem é possível também realizar uma comparação entre rácios da empresa com rácios do setor, bem como a comparação de rácios, de dados equivalentes, com empresas concorrentes.

Em ferramentas de extração e análise de dados, mencionadas seguidamente no subcapítulo 1.3.4.1, destacam-se ainda análises através da identificação de padrões, *outliers*, análise de quebras em sequências, sumarização de dados a fim de obter médias, mínimos ou máximos, análise de KPIs, análise de resultados dos testes de auditoria por risco, análises através da comparação de duas versões da mesma folha de cálculo, extração de dados através da indicação de critérios específicos, análise de dados não correspondentes a um formato pré-definido, identificação de padrões incomuns nos dados (teste de Benford) e o cálculo de diferenças absolutas e percentuais entre dados.

Como será possível constatar no subcapítulo 1.3.4.2, relativamente às ferramentas de gestão de papéis de trabalho destaca-se o planeamento e agendamento de auditorias, a gestão de recursos, a possibilidade de definição de lembretes relativamente a prazos, gestão de tempo, de despesas, de papéis de trabalho, de evidências. Através destas ferramentas é ainda possível a obtenção de relatórios detalhados e a avaliação da evolução e do grau de execução dos trabalhos de auditoria.

Em relação a ferramentas de segurança de SI, seguidamente mencionadas no subcapítulo 1.3.4.3, é possível destacar ainda a análise a autorizações de usuário e permissões de acesso, analise de fontes de tráfego de rede, análise de potenciais ameaças à segurança, análise de vulnerabilidades, de *malware*, acessos não autorizados e violação de dados.

Por fim, através de ferramentas de utilidade geral, seguidamente abordadas no subcapítulo 1.3.4.4, é possível através destas a ordenação de dados, a filtragem de dados, realização de fórmulas, utilização de formatação condicional, criação de listas de dados, realização de resumo de dados em tabelas dinâmicas e elaboração de gráficos.

Desta forma, pode referir-se que o *software* apoia o trabalho dos auditores e contribui para uma melhoria e eficiência do trabalho apresentado por estes, no entanto é importante a aposta na formação contínua dos auditores em *software* específico para que possam tirar um melhor partido destes para o seu trabalho.

1.2.3 Impactos da Auditoria de SI na organização

Relativamente aos impactos que uma auditoria SI pode ter na organização, Silva (2007), com referência a Davis et al (2007), indica que esta possui benefícios, uma vez que ajuda "*a organização a identificar vulnerabilidades nos controlos e a desenvolver soluções eficientes para gerir essas vulnerabilidades*" (Silva, 2007, p. 42) A auditoria de SI possui impacto no controlo interno da organização revelando, com base na execução de testes suficientes, a garantia que os controlos se encontram adequadamente desenhados e que funcionam de forma eficaz e continua.

No ponto de vista do ISACA (2005), segundo Silva (2007, p. 42), a auditoria de SI "*é responsável por efectuar uma revisão e avaliação dos riscos do ambiente de trabalho dos SI que suportam os processos de negócio*". Desta forma, a atividade de auditoria de SI auxilia a organização na identificação e avaliação de exposições ao risco que se revelem significativas, como contribui ainda "*para a melhoria dos mecanismos de gestão de risco e de controlo dos SI*". (Silva, 2007, p. 42)

Na perspetiva do IIA (Institute of Internal Auditors) (2005), segundo Silva (2007), a auditoria de SI irá avaliar a capacidade dos controlos de SI protegerem a organização de ameaças significativas e "*deve fornecer evidência de que os riscos residuais são pouco prováveis de causar danos significativos à organização e às suas partes interessadas*" (Silva, 2007, p. 42), ou seja, possui impactos relacionados com a imagem da organização perante os *stakeholders*.

Em suma a auditoria de SI traz impactos para a organização a nível da estrutura funcional, impactos a nível de imagem pois transmite confiança aos *stakeholders*, impactos na tomada de decisão, no controlo interno, na gestão de risco e de vulnerabilidades. Desta forma, a auditoria de SI possibilita inúmeros benefícios que possibilitam mais facilmente o alcance dos objetivos organizacionais, bem como operar de um modo mais eficiente o que consequentemente favorece e promove a viabilidade da organização.

1.2.4 Certificações

O mundo atual exige auditores dinâmicos, que consigam antever riscos emergentes e agir de encontro à sua resolução. Um programa de certificação permite ao auditor ficar mais enriquecido com a experiência educacional, informação e ferramentas. (IPAI, 2019a)

Assim, segundo o Instituto Português de Auditoria Interna (IPAI), a obtenção de uma certificação "*demonstra conhecimento e competência profissional em nível internacionalmente reconhecido, permite verificar o grau de experiência e habilitação profissional em temas específicos, assegura uma maior uniformidade na forma de atuação"* (IPAI, 2019a, p. 2) e permite uma melhor credibilidade e valorização profissional do auditor. De tal forma, a obtenção de uma certificação é uma mais-valia.

Seguidamente serão apresentadas, do ponto de vista da área profissional, certificações que um auditor de SI pode obter.

A Certificação em Auditoria de Sistemas de Informação (CISA – *Certified Information Systems Auditor*) é disponibilizada pelo ISACA e pretende validar a capacidade para auditar e gerir controlos em todas as áreas relacionadas com SI. Esta certificação "*é mundialmente conhecida como um padrão de conquista para quem audita, controla, monitora e avalia a tecnologia de informação e os sistemas de negócios de uma organização.*" (ISACA, 2020c)

A certificação CISA abrange os módulos: O Processo de Auditoria de SI; Governança e Gestão de TI; Aquisição, Desenvolvimento e Implementação de SI; Operações de SI e Resiliência de Negócios; e Proteção de Ativos de Informação. (ISACA, 2020c)

A Certificação em Risco e Controlo de Sistemas de Informação (CRISC – *Certified in Risk and Information Systems Control*), emitida pelo ISACA, "*é a única certificação que posiciona os profissionais de TI para o crescimento futuro da carreira vinculando a gestão de riscos de TI à gestão de riscos corporativos e posicionando-os para se tornarem parceiros estratégicos dos negócios.*" (ISACA, 2019a)

A certificação CRISC abrange as seguintes temáticas: Identificação de Risco de TI; Avaliação de Risco de TI; Resposta ao Risco e Mitigação; Relatório e Monitorização de Risco e Controle. (ISACA, 2020e)

A Certificação em Gestão de Segurança da Informação (CISM - *Certified Information Security Manager*) disponibilizada pelo ISACA está focada na gestão de segurança da informação. Esta certificação é aceite globalmente como "*referência para profissionais que protejam, construam e gerenciem programas de segurança das informações corporativas."* (ISACA, 2019b)

A certificação CISM abrange os domínios relacionados com: Governança de Segurança da Informação; Gestão de Risco da Informação; Desenvolvimento e Gestão de Programas

de Segurança da Informação; e Gestão de Incidentes de Segurança da Informação. (ISACA, 2020d)

A Certificação em Governança Corporativa de TI (CGEIT – *Certified in the Governance of Enterprise IT*), emitida pelo ISACA, reconhece profissionais com conhecimento aplicado aos princípios e práticas de governança corporativa de TI e confere credibilidade aos profissionais para discutirem questões relacionadas com governança e alinhamento estratégico. (ISACA, 2019c)

A certificação CGEIT abrange os módulos de: Governança de TI Corporativa; Recursos de TI; Realização de Benefícios; e Otimização de Risco. (ISACA, 2020b)

A certificação de profissionais de cibersegurança (CSX-P – *Cybersecurity* Practitioner), emitida pelo ISACA, abrange cinco funções de segurança, são elas: identificar, proteger, detetar, responder e recuperar, sendo que esta certificação pretende testar as capacidades de os profissionais executarem funções que tenham em vista a segurança cibernética. (ISACA, 2020f)

A certificação CSX-P abrange os módulos: Ambiente de Negócios e Segurança, Prontidão de Segurança Operacional, Deteção e Avaliação de Ameaças e Resposta e Recuperação de Incidentes. (ISACA, 2020f)

A certificação em soluções de privacidade de dados (CDPSE - *Certified Data Privacy Solutions Engineer*) pretende ir ao encontro da grande aposta das organizações na criação de soluções de privacidade que se encontrem alinhadas com os objetivos organizacionais e apetite ao risco. (ISACA, 2020a)

A certificação CDPSE abrange três domínios relacionados com: Governança de Privacidade; Arquitetura de Privacidade e Ciclo de Vida de Dados. (ISACA, 2020a)

Os auditores que obtenham a Certificação de Auditor Interno (CIA – *Certified Internal Auditor*) constituem um apoio para os gestores de topo e para os Conselhos de Administração no alcance das metas e objetivos estratégicos. Esta certificação é emitida pelo IIA. (IPAI, 2019b)

No exame para CIA é realizado em três partes e tem como objetivo testar os conhecimentos do auditor em áreas como: Fundamentos de Auditoria Interna; Independência e Objetividade; Programa de Garantia e Melhoria de Qualidade; Governação, Gestão de Risco e Controlo; Planeamento e Condução do Trabalho; Visão

de Negócio; Segurança da Informação; Tecnologia da Informação; entre outras e abrange assim todas as outras certificações disponibilizadas pelo IIA. (IPAI, 2019a)

Tabela 1 – Certificações para o auditor de SI.

Certificação	Entidade promotora	Ano da 1ª certificação	Nº de pessoas certificadas
CIA	IIA	1974	160.000+
CISA	ISACA	1978	151.000+
CRISC	ISACA	2010	26.000+
CISM	ISACA	2003	46.000+
CGEIT	ISACA	2007	8.000+
CSX-P	ISACA	2015	N/A
CDPSE	ISACA	2020	N/A

Como análise à Tabela 1 apresentada anteriormente, podemos referir que foi no início da década de 70 que surgiram as primeiras certificações para auditores, nomeadamente a certificação CIA (emitida pelo IIA) e a certificação CISA (emitida pelo ISACA), a par, como referido anteriormente, das primeiras referências ao termo CAATs (IIA, 2017a) (Andrade, 2013).

Seguidamente, só no ano de 2003 surgiu a certificação CISM e mais tarde no ano de 2007 a certificação CGEIT, posteriormente, em 2010, surgiram certificações como CRISC, em 2015 a CSX-P e mais recentemente, em 2020, a certificação CDPSE, todas elas emitidas pelo ISACA (Andrade, 2013) (Business Wire, 2015).

Relativamente ao número de pessoas certificadas pode constatar-se que são as certificações que surgiram na década de 70, que possuem um maior número de auditores certificados. A certificação CIA conta com mais de 160 mil certificados e a CISA com mais de 151 mil pessoas certificadas (IIA, 2020) (ISACA, 2020c).

A certificação CRISC, lançada no ano de 2010, é mais recente que a certificação CGEIT, lançada no ano de 2007, no entanto a certificação CRISC possui um maior número de pessoas certificadas, com mais de 26 mil (ISACA, 2020e) e 8 mil certificações (ISACA, 2020b), respetivamente.

Desta forma, podemos concluir que existem várias certificações que podem ser obtidas pelos auditores de SI, sendo estas uma mais-valia para estes, uma vez que possibilitam o reconhecimento dos seus conhecimentos. De salientar ainda que, a certificação aliada à formação contínua, por parte dos auditores, é essencial para uma maior obtenção de vantagens da evolução do *software*, um melhor desempenho profissional e um maior contributo, a vários níveis, para os objetivos da organização.

1.3 Computer-assisted Audit Techniques – CAATs

Neste tópico será abordada a origem e evolução das CAATs, indicado o entendimento sobre o que se pode definir como uma CAAT, quais as classificações existentes relativas às CAATs, será dada uma grande ênfase a ferramentas informáticas que podem ser utilizadas para apoiar o trabalho realizado pelos auditores, será ainda realizada uma relação entre os tipos de auditoria de SI e as tipologias de CAATs. Por fim serão indicados custos e benefícios associados à utilização das CAATs na auditoria.

1.3.1 Origem e Evolução

A origem das CAATs, segundo Silva (2007), através da menção a Díaz y Vera (2006), situa-se na década de 1970, inícios de 1980, acompanhando ao longo dos anos o desenvolvimento em diversas áreas como as ciências da informação, ciências económicas e tecnologias de informação e comunicação.

Pedrosa (2015) indica mais concretamente uma das primeiras referências encontradas para o termo "técnicas de auditoria assistida por computador" no ano de 1974. Esta referência foi realizada pelo AICPA (*American Institute of Certified Public Accountants*), na SAS (*Statement on Audit Standards*), Declaração sobre as Normas de Auditoria, onde se faz referência aos efeitos do EDP (*Electronic Data Processing*), Processamento Eletrónico de Dados, no estudo do auditor e na avaliação do controlo interno, ou seja, "*a necessidade de avaliar os registos (que irão gerar as demostrações financeiras) produzidos pelos sistemas informatizados*" (Pedrosa, 2015, p. 23).

No ano de 1978, realizou-se a introdução ao programa de certificações para auditores de SI, com a certificação CISA (*Certified Information Systems Auditor*) (Silva, 2007). Este programa de certificação pretendia, e pretende ainda hoje, avaliar e reconhecer as

competências e conhecimentos dos profissionais e garantir a atualização periódica dos profissionais certificados.

As primeiras referências a "técnicas de auditoria assistida por computador" foram realizadas pelo AICPA. Em 1979 um documento completo dedicado a técnicas de auditoria assistida por computador. Em 1984, na SAS, uma análise aos efeitos do processamento por computador no exame de demonstrações financeiras. (Pedrosa, 2015)

Com o decorrer dos anos e aumento significativo do uso de sistemas financeiros baseados em computador e o aparecimento de novas ferramentas, foram sendo feitas mais referências ao termo. Pedrosa (2015), com referência a Lovata (1988), "*afirma que o impacto no ambiente de auditoria devido ao aumento da tecnologia de informação é significativo*" (Pedrosa, 2015, p. 23) e o GAS, *software* de auditoria generalizado é reconhecido como o mais comummente utilizado à data da referência.

A nível mundial, ao longo dos anos, generalizaram-se varias ferramentas para o uso no meio profissional da auditoria, e atualmente entre as mais conhecidas temos o IDEA (*Interactive Data Extraction and Analysis*) e o ACL (*Audit Control Language*) (Silva, 2007). De notar que a partir de maio de 2019, o *software* ACL passou a designar-se de Galvanize. Estas e outras ferramentas serão abordadas com mais detalhe, seguidamente no ponto 1.3.4 - Tipos de Ferramentas.

Para Duque & Arias (2017), as CAATs também surgiram na década de 70, e tal como a tecnologia, também estas têm vindo a evoluir. Nos dias de hoje a utilização de CAATs encontra-se presente nas diferentes fases de uma auditoria, não sendo o uso destas exclusivo da fase de execução, para a obtenção de evidências, como era inicialmente, ou seja, estas técnicas encontram-se presentes nas diferentes fases, desde o planeamento até ao seguimento da auditoria (Tabela 2).

Tabela 2 – Evolução das Técnicas e Ferramentas de Auditoria.

1970's	1980's	1990's	2000's
Aplicações com linguagens de programação	Aplicações com linguagens de programação de terceira geração	Aplicações com linguagens de programação de quarta geração	*Software* habilitado para a web (XBRL)
Software de auditoria de primeira geração (*batch*)	*Software* de auditoria de segunda geração (interativo e em *batch*)	*Software* de auditoria de terceira geração (interativo e em	Auditoria Continua

1970's	1980's	1990's	2000's
		batch baseado em PC's)	
Simulações em paralelo simples	Simulações em paralelo extensas	Análises de dados e provas exaustivas	Análise Digital
Lotes de testes/ utilitários de teste integrados	Lotes de testes/ utilitários de teste integrados	Auditoria de *Software*	*Software* de garantia de auditoria
Testes de entrada/saída	SCARF/SARF (Definição em texto)		
Revisão de controlo interno	Questionários de revisão de controlo interno automatizados	Questionários de revisão de controlo interno automatizados	Autoavaliação de controlo
Questionários de controlo de diagramas de fluxo	Diagramas de fluxo do programa	Fluxos de processo com ênfase na auditoria de dados	Visualização do *Software*
Primeiro computador – com base na amostragem de unidades monetárias	Unidade de amostragem em dólares mais desenvolvida	Várias opções de amostragem, incluindo estratificação	Menor ênfase na amostragem
Matrizes de controlo	Um controlo melhor	Sistemas especializados	Redes neuronais e matrizes de inteligência artificial

Fonte: (Duque & Arias, 2017, p. 465)

Numa análise à tabela anterior podemos verificar que as CAATs têm vindo a evoluir a par da tecnologia, desde a sua origem, na década de 70. Desta forma, pode destacar-se que atualmente um *software* está apto a trabalhar via web estando disponível em qualquer lugar com acesso à web e a qualquer momento, o que anteriormente só era possível trabalhando através de aplicações com linguagem de programação.

Nos dias de hoje, a auditoria continua alterou o paradigma da auditoria, estando focada numa revisão permanente de todas as transações por oposição a uma anterior revisão periódica de uma amostra de transações. Existindo por isso atualmente, nos testes de auditoria, uma menor ênfase na amostragem e uma maior enfase na população, ou seja, nos dados como um todo.

A auditoria continua permite também, segundo Duque & Arias (2017), com base no referido pelo ISACA, analisar a evolução de riscos e controlos de uma forma continua, quando anteriormente era realizada apenas uma revisão de controlos e utilizadas apenas matrizes de controlo. Na minha perspetiva, esta análise continua dos riscos e controlos está também relacionada e é também impulsionada pela utilização de redes neuronais e matrizes de inteligência artificial.

Na década de 70 eram realizadas apenas simulações em paralelo simples, com base somente em alguns campos de dados, o que com a variedade de dados e tipos de arquivos veio a revelar-se uma necessidade de desenvolvimento desta área e evoluiu-se para uma auditoria digital generalizada.

Em conclusão, pode afirmar-se que todos os autores acima mencionados indicam a década de 70 como a altura em que foram feitas as primeiras referências ao termo CAATs e assim a altura em que estas surgiram.

A par do aumento da utilização de SI está o seu desenvolvimento e o aparecimento de novas ferramentas de auditoria, com vista ao acompanhamento desse desenvolvimento tecnológico. Assim, verifica-se com o passar das décadas a utilização de técnicas cada vez mais sofisticadas e uma maior utilização destas na auditoria, uma vez que atualmente a utilização de CAATs se encontra presente nas diferentes fases de uma auditoria.

1.3.2 Definição

Na literatura é feita referência às ferramentas tecnológicas na auditoria através dos termos Computer-assisted Audit Techniques, CAATs, ou Computer-assisted Audit Tools and Techniques, CAATTs, ou em português Técnicas de Auditoria Assistida por Computador, TAACs, que consiste na utilização de qualquer ferramenta informática de suporte à auditoria. Segundo Sayana (2003) pode definir-se CAATs como o uso de determinado *software* por parte do auditor para realizar e alcançar os objetivos de uma auditoria.

Segundo Lungu & Vatuiu (2007) citados por Duque & Arias (2012, p. 101) CAATT "*são técnicas utilizadas pelos auditores, utilizando o computador como um instrumento para recolher e analisar dados necessários para a auditoria*".

As diferentes designações acima referidas são utilizadas para fazer referência às técnicas e ferramentas tecnológicas na auditoria, e estão presentes nas orientações fornecidas por alguns órgãos internacionais, nomeadamente: (1) o ISACA, *Information Systems Audit and Control Association,* que promove o uso de diretrizes e recomendações para auditores de sistemas de informação*;* (2) o IFAC, *International Federation of Accountants,* que utiliza normas internacionais de auditoria (ISA – *International Standards on Auditing*) para auditores de demonstrações financeiras*;* (3) o AICPA, *American Institute of*

Certified Public Accountants, que estabelece padrões de auditoria para contabilistas públicos certificados (CPAs - *Certified Public Accountants*)*;* (4) o IIA, *Institute of Internal Auditors,* um instituto profissional internacional para auditores internos, que aplica um quadro internacional de práticas profissionais (IPPF – *International Professional Practices Framework*)*;* (Pedrosa, 2015).

O ISACA utiliza o termo Computer-assisted Audit Techniques, CAATs, *"qualquer técnica de auditoria automatizada, tal como software de auditoria generalizado (GAS), geradores de dados de teste, programas de auditoria informatizados e utilitários de auditoria especializados"* (ISACA, 2015, p. 17).

O IFAC, tal como o ISACA, também emprega o termo Computer-assisted Audit Techniques, CAATs, *"aplicações de procedimentos de auditoria utilizando o computador com uma ferramenta de auditoria"* (IAASB, 2009, p. 15).

O AICPA, desde 1979 que tem vindo a aplicar o termo Computer-assisted Audit Tools and Techniques, CAATTs, para técnicas que permitem testes diferentes dos executados manualmente, procedimentos substantivos e outras operações como testes de dados, segundo Pedrosa (2015).

O IIA, aplica o termo Technology-based Audit Techniques, *"qualquer ferramenta de auditoria automatizada, tal como software de auditoria generalizado, geradores de dados de teste, programas de auditoria informatizados, utilitários de auditoria especializados, e técnicas de auditoria assistida por computador (CAATs)."* (IIA, 2017b, p. 24). Esta definição é em muito semelhante à utilizada pelo IFAC.

No meu entendimento CAATs são quaisquer ferramentas informáticas que auxiliam os trabalhos realizados numa auditoria, facilitando desta forma o trabalho dos auditores e possibilitando uma melhor qualidade do trabalho, uma melhoria da eficiência e o alcance dos objetivos da auditoria. Ao longo da dissertação será empregue o termo CAATs para fazer referência à utilização de ferramentas informáticas na auditoria.

1.3.3 Classificação

Existem diversas ferramentas que tem como objetivo potenciar o trabalho do auditor, em diferentes áreas, desde o planeamento aos procedimentos de auditoria. Desta forma, as CAATs podem ser categorizadas, tendo em conta as suas funcionalidades.

Seguidamente serão categorizadas algumas técnicas que possibilitam a segurança da informação, a construção de modelos de análise financeira, a elaboração de relatórios e pareceres em processamento de texto, mas também a constituição de bases de dados agregando informação relevante para o trabalho de auditoria a realizar, auxiliando na extração, sorteio, seleção de dados e transações. Deste modo, poderá verifica-se que são inúmeras as possibilidades de aplicação das novas tecnologias de informação e que estas poderão trazer mais valias para a atividade de auditoria.

Estas ferramentas possibilitam ao auditor o alcance de metas definidas no planeamento de auditoria e podem ser utilizadas independentemente do tipo de auditoria praticada.

Segundo Lanza (1998), citado por Correia (2017) as ferramentas que o auditor pode utilizar no processo de auditoria são categorizadas em três tipos.

1. Ferramentas de extração e análise de dados: cujo objetivo consiste em "*investigar o conteúdo de tabelas em bases de dados e gerar relatórios comparativos*". (Correia, 2017, p. 16)
2. Ferramentas de gestão de auditoria: "*incorporam funcionalidades específicas de auditoria, como a análise e avaliação do risco, controlo de procedimentos e de verificações, criação de listas e questionários automatizados de controlo interno para fazer o acompanhamento da auditoria*". (Correia, 2017, p. 16)
3. Utilidades instrumentais: englobam todas as ferramentas genéricas, não específicas de auditoria, no entanto com um potencial para utilização em auditoria, por exemplo, folhas de cálculo, processadores de texto e extratores de dados com base em linguagem SQL (Structured Query Language).

Para Teruel (2010) as ferramentas de auditoria são classificadas em três tipos, nomeadamente generalistas, especializadas e de utilidade geral.

1. Ferramentas generalistas – *software* que permite "processar, simular, analisar amostras, gerar dados estatísticos, sumarizar, apontar duplicidade" (Teruel, 2010, p. 3) entre outras funções.

Segundo o autor, podem indicar-se como principais ferramentas generalistas o *software* Audit Command Language (ACL), Interactive Data Extraction & Analisys (IDEA), Galileo e Pentana.

Tabela 3 – Vantagens e desvantagens de ferramentas generalistas em auditoria

Vantagens	Desvantagens
- Processamento de diversos arquivos em simultâneo	- Para que os dados sejam analisados em ambientes distintos, é necessário a gravação de dados em separado, poucas aplicações poderiam ser feitas em ambiente *on-line*
- Processamento de vários tipos de arquivos em diferentes formatos	- O *software* não suporta a necessidade de realização de cálculos complexos, pois sendo este uma ferramenta generalista evita aprofundar lógicas e matemáticas muito complexas
- Possibilidade de integração sistemática com *software* e *hardware* diversos	
- Possibilita uma redução da dependência do auditor relativamente aos especialistas de informática	

Fonte:(Teruel, 2010, p. 3)

2. Ferramentas especializadas – *software* com vista a executar determinadas tarefas em circunstâncias definidas. Este *software* pode ser desenvolvidos pelo auditor, por especialistas da empresa ou através da contratação de terceiros.

Tabela 4 – Vantagens e desvantagens de ferramentas especializadas.

Vantagens	Desvantagens
- O *software* irá atuar em áreas específicas, como crédito imobiliário, leasing, entre outras funções que exijam tarefas especializadas	- Os custos destas ferramentas poderão ser elevados, uma vez que o seu uso será limitado a um cliente
- O auditor pode desenvolver um *software* especializado numa área complexa, possibilitando-lhe assim ter uma vantagem competitiva	- Futuras atualizações também poderão tornar inviável esta ferramenta

Fonte:(Teruel, 2010, p. 6)

3. Ferramentas de utilidade geral – estas ferramentas não são específicas para a atividade de auditoria, no entanto são utilizadas com esse propósito, permitindo executar funções comuns de processamento, como sorteio de arquivos, sumarizar, concatenar, gerar relatórios, entre outras.

Segundo Teruel (2010), podem indicar-se como principais ferramentas de utilidade geral folhas eletrónicas, como o Excel, *software* de gerenciamento de banco de dados, como o Access e MySQL, ferramentas de Business Inteligence, como Business Objects, *software* estatísticos, entre outros.

Tabela 5 – Vantagens e desvantagens de ferramenta de utilidade geral em auditoria

Vantagens	**Desvantagens**
- Possibilidade de utilização, como suporte à auditoria, na ausência de outros recursos	- Estas ferramentas não possuem os recursos necessários para a execução de uma auditoria completa

Fonte:(Teruel, 2010, p. 6)

Segundo o Tribunal de Contas (1999), as CAATs são essencialmente de dois tipos:

1. *Audit software* – recurso a programas informáticos de auditoria para realizar testes de conformidade ou testes substantivos com uma extensão que não é viável por métodos manuais.
2. *Data tests* – utilização de testes de dados de modo a avaliar como funcionam os controlos internos do sistema informático, nomeadamente através da resposta que este dá à introdução de dados fictícios ou dados com diversos tipos de erros.

Duque & Arias (2012) fazem referência a Louwers et al. (2011), que classifica as técnicas e ferramentas a utilizar em dados reais ou em dados simulados, ou seja, dados fictícios.

Concluindo, tanto Correia (2017) como Teruel (2010) fazem uma classificação semelhante, fazendo ambos uma classificação das ferramentas em três tipos, nomeadamente ferramentas generalista que permitem a extração e análise de dados, ferramentas especializadas de auditoria, que incorporam funcionalidades específicas de auditoria e ferramentas de utilidade geral, ou seja, ferramentas genéricas, não específicas para a atividade de auditoria. Por outro lado, o Tribunal de Contas (1999) faz uma classificação em termos de testes a realizar com apoio das CAATs, ou seja, testes de

conformidade ou substantivos e testes induzindo o erro para verificar qual a resposta do SI e que em parte Duque & Arias (2012) estão de acordo.

Por fim, no seguinte subcapítulo, 1.3.4 - Tipos de Ferramentas , ter-se-á em conta a categorização das ferramentas feita por Lanza (1998), citado por Correia (2017), que refere nomeadamente três tipos de categorias, nomeadamente ferramentas de extração e análise de dados, ferramentas de gestão de auditoria, denominadas de ferramentas de gestão de papéis de trabalho e utilidades instrumentais, designadas de ferramentas de utilidade geral. No entanto, verificou-se ao longo da revisão da literatura a lacuna na referência a ferramentas de segurança de sistemas informáticos, que também serão tidas em conta ao longo desta dissertação.

1.3.4 Tipos de Ferramentas

Existem várias ferramentas informáticas que podem ser utilizadas para apoiar o trabalho realizado pelos auditores e para tal neste capítulo será feita referência a algumas dessas ferramentas e será analisado de que forma estas podem apoiar o trabalho de auditoria.

Para tal análise as CAATs foram divididas em ferramentas de extração e análise de dados, gestão de papéis de trabalho, segurança de sistemas informáticos e ferramentas de utilidade geral.

1.3.4.1 Extração e análise de dados

Como referido anteriormente, a auditoria com base na extração e análise de dados consiste em verificar o conteúdo de tabelas em bases de dados, nomeadamente para verificar a integridade dos dados, a existência ou não de fraudes e também para posterior indicação de procedimentos que não estão a ser realizados de acordo com o definido.

Como ferramentas de extração e análise de dados são de destacar: Active Data, ASD Auditor, CaseWare IDEA Analytics, Magique Galileo e TeamMate Analytics.

- ✓ **Active Data**

Active Data possui funcionalidades ao nível de análise de dados e planeamento de trabalho. Esta aplicação poderá ser adicionada, como suplemento, a outro *software* de

análise de dados ou CAATs, como por exemplo o Microsoft Excel, ACL e IDEA. (InformationActive, 2020)

Através desta ferramenta pode realizar-se consultas, resumos, estratificação de dados, comparações, estatísticas, identificar *outliers*, detetar lacunas e extração através de amostragem, nomeadamente amostragem aleatória e aleatória estratificada. (InformationActive, 2020)

- ✓ **ASD Auditor**

Auditing Software Distributor Auditor é um *software* de auditoria e análise financeira, que está totalmente adaptado às necessidades atuais de qualidade que exigem as normas internacionais de auditoria ISA. (Auditing Software Distributor, 2020a)

O ASD Auditor agrega valor à organização e aos clientes da organização, possibilitando uma otimização de recursos, uma garantia de cumprimento normativo e uma melhoria da qualidade do produto final. Esta é uma solução desenvolvida para uma gestão completa da auditoria, de acordo com as ISA, com base nos riscos e nos requisitos de controlo de qualidade e possibilita uma gestão dos processos de auditoria de forma ordenada, eficiente e ágil. Assim, o processo de auditoria parte de um planeamento baseado em riscos, passando pela execução, onde se analisa e obtêm evidências e por fim a emissão do relatório. (Auditing Software Distributor, 2020b)

De entre as principais características deste *software* pode destacar-se o facto de ser 100% adaptado aos padrões internacionais de auditoria e requisitos internacionais de qualidade, possibilitar uma total conectividade entre escritórios, equipas de auditoria, controlo de nível e acesso, este *software* possui um sistema de mensagens internas, um arquivo completo da auditoria, que possibilita uma visão global desta, numa perspetiva de supervisão e controlo. Destaca-se também uma criação automática de programas de trabalho baseados em riscos, possibilidade de cálculo e análise de amostragem estatística de materialidade, cálculo e seleção automática de amostras para circularização, controlo e análise, possibilidade de exportação e importação de documentos em qualquer etapa da auditoria, estrutura de papéis de trabalho e diversas ferramentas para a execução do trabalho do auditor e ainda uma revisão da auditoria com todos os recursos com vista ao cumprimento das normas técnica e de *compliance* da organização auditada. (Auditing Software Distributor, 2020b)

- ✓ **CaseWare IDEA Analytics**

CaseWare IDEA Analytics (CaseWare International, 2020b) é uma ferramenta de análise de dados abrangente, com uma interface moderna, intuitiva e de fácil utilização, projetada por auditores. Esta ferramenta garante a integridade dos dados, uma vez que o acesso é somente de leitura, acelera o processo de auditoria e possibilita decisões de negócio mais informadas.

Com este *software* poderá realizar-se a importação de dados de várias fontes, como por exemplo PDF, Excel, CSV, mais de 50 *software* de contabilidade como Quickbooks, Sage, Xero e *software* de gestão de papéis de trabalho como CaseWare working papers, entre outros. O IDEA permite também criar gráficos e estatísticas para que seja possível identificar com maior rapidez padrões, tendências e *outliers*. (CaseWare International, 2020b)

O autor Teruel (2010) refere que este *software* possibilita a extração e análise de dados e é utilizado para controlos internos e deteção de fraudes. Através desta ferramenta é assim possível ler, exibir, analisar e manipular amostras ou arquivos de dados.

Coelho (2010) faz referência a algumas funções do IDEA, nomeadamente através destas funções é possível a deteção de chaves duplicadas, a deteção de quebras na sequência, por exemplo falta de faturas, a sumarização de dados a fim de obter médias, mínimos ou máximos de um determinado campo, a verificação de campos vazios ou com valores nulos, a verificação da existência de vendas ao fim-de-semana ou feriados, entre outros.

- ✓ **Magique Galileo**

Galileo é um *software* de gestão de auditoria totalmente integrado, adaptado às necessidades de uma auditoria interna, investigações, conformidade ou projetos orientados a departamentos, através de papéis de trabalho, rastreamento de ações e relatórios. (Magique Galileo, 2019)

Este *software* permite uma vinculação total de riscos à auditoria para fins de planeamento, uma criação de tarefas a realizar com base em riscos, controlos e testes, é também possível uma análise de resultados dos testes por risco, uma criação automática de estatísticas e relatórios oportunos de progresso de auditoria e desempenho, análises de

KPIs conforme necessidade e existe também a possibilidade de acesso para que os clientes da auditoria possam participar nos processos de gestão de risco e na auditoria. (Magique Galileo, 2019)

Como principais características do *software* Magique Galileo (2019) podem destacar-se:

- Planeamento estratégico de atividades ao longo de vários períodos;
- Plano anual de trabalho para uma auditoria baseada em riscos;
- Diversas opções para vincular riscos ao universo de auditoria;
- Funções para emissão de relatórios de fim de ano;
- Gestão de recursos e competências da equipa;
- Agendamento de funcionários com alocações de trabalho, disponibilidade e conflitos de tempo;
- Papéis de trabalho com opções para *links* incorporados, *hiperlinks* e anexos.
- Rastreamento de problemas e ações com vários níveis;
- Biblioteca de testes padrão;
- Alertas por e-mail de ações atrasadas e alerta proativo de itens pendentes;
- Questionário pós-atividade para obter *feedback*.

✓ **TeamMate Analytics**

O *software* TeamMate Analytics fornece uma maior visão através de análises mais aprofundadas. Através desta ferramenta é possível planear, realizar testes sobre um conjunto completo de dados, localizar riscos ocultos e agregar valor aos relatórios. (Wolters Kluwer, 2020b)

Ao nível de recursos de análise o TeamMate Analytics possui uma variedade de ferramentas que podem ser utilizadas, no entanto antes de iniciar a análise dos dados é necessária uma preparação dos dados, sendo assim possível analisar dados de diferentes formatos e fontes de arquivo. Desta forma, através do TeamMate Analytics é possível converter relatórios e arquivos de texto em Excel pronto para análise. (Wolters Kluwer, 2020a)

Seguidamente, a análise dos dados pode ser realizada com base, principalmente, em recursos como manipulação de folhas de cálculo, resumos, extração, análise numérica, fórmulas, amostragem, entre outros. Através da manipulação de folhas de cálculo é

possível juntar várias folhas com a mesma estrutura e analisar o conjunto da informação ou separar essas folhas e realizar uma análise mais detalhada, por exemplo por vendedor ou armazém. É ainda possível comparar duas versões da mesma folha de cálculo para destaque de diferenças entre fórmulas ou valores. (Wolters Kluwer, 2020a)

Ainda na fase de análise de dados é possível realizar um resumo dos dados com base numa coluna ou agrupamento, realizar um resumo dos dados para identificar quais os valores mais altos ou mais baixos e é também possível dividir os dados de forma a selecionar amostras aleatórias em cada grupo de dados. Através da ferramenta de extração é possível extrair registos conforme a indicação de critérios específicos, desta forma, pode combinar-se até três critérios e realizar comparações com valores fixos, colunas ou lista de datas, existe também a possibilidade de extrair registos duplicados, com base em linhas ou com base em até seis campos específicos ou extrair registos com seleção de até seis colunas duplicadas, mas uma é diferente. Com esta ferramenta é ainda possível extrair registos em que um campo não corresponde a um formato pré-definido e identificar casos em que um fornecedor tenha emitido várias notas fiscais com referências sequenciais. (Wolters Kluwer, 2020a)

Através de ferramentas de análise numérica pode realizar-se o Teste de Benford, que possibilita a identificação de padrões incomuns nos dados, é possível identificar *outliers*, ou seja, registos onde a quantidade se desvia significativamente da média, comparar duas colunas com dados numéricos e calcular as diferenças absolutas e percentuais entre elas e comparar entre duas a quatro colunas para identificar correlações, *outliers* ou prever valores futuros. Relativamente à ferramenta de amostragem é possível realizar várias seleções de dados, nomeadamente uma amostra de dados aleatória simples ou também uma amostra estratificada. Pode ainda identificar-se outros recursos como o uso de fórmulas ou a utilização de filtros. (Wolters Kluwer, 2020a)

Desta forma, pode indicar-se ainda que o TeamMate Analytics inclui uma seleção de módulos personalizados pré-construídos para auditoria, onde cada módulo contém muitos testes projetados especificamente para determinada área a auditar. De salientar que existe a possibilidade de utilizar as ferramentas de teste como são, modificá-las, utilizando-as como base para os seus próprios módulos ou criar os seus próprios testes e partilhá-los com a equipa. (Wolters Kluwer, 2020a)

1.3.4.2 Gestão de papéis de trabalho

Ferramentas de gestão de papéis de trabalho têm em vista o planeamento e agendamento de uma auditoria e englobam ferramentas que permite gerir as atividades da equipa de auditoria agregando dados para que se possa obter uma visão adequada do trabalho de auditoria.

Como ferramentas de gestão de papéis de trabalho são de destacar: CaseWare Working Papers, DRAI, MetricStream, MyWorkpapers, Pentana Audit, SAP Audit Management, SIAUDI, SIPTA, SE Audit, SiAudit e TeamMate Audit Management.

- ✓ **CaseWare Working Papers**

O *software* CaseWare Working Papers é flexível em termos de gerenciamento de projetos e possui ferramentas para a realização de contratos de garantia e emissão de relatórios. Através desta ferramenta o acesso aos dados realiza-se num único local o que permite entre outros aspetos, uma colaboração em tempo real, digitalização direta e uma revisão *on-line*. (CaseWare International, 2020a)

Como principais características deste *software* pode indicar-se uma colaboração em tempo real de diferentes membros da equipa, no mesmo papel de trabalho; relatórios inteligentes, como demostrações financeiras, relatórios e programas de trabalho com base em necessidades; gestão simples de documentos; importação e exportação de dados; supervisão integrada através da criação, atribuição e rastreamento de problemas, revisão de notas e monitoramento de listas de tarefas; aprovações, com a possibilidade de gestão da revisão e aprovação das atividades concluídas, utilizando até oito aprovações e também a possibilidade de encaminhar arquivos e informações identificadas para o próximo ano. (CaseWare International, 2020a)

- ✓ **DRAI**

O *software* DRAI (Dossier de Revisão/Auditoria Informatizado) é uma ferramenta integrada desenvolvida pela BDO (Binder Dijker Otte & Co) (2020c). Esta é uma ferramenta de apoio ao planeamento e execução do trabalho de auditoria.

O DRAI (BDO, 2020c) está disponibilizado em várias versões, DRAI SAF-T que utiliza como base de análise ficheiros SAF-T, DRAI3 2010 similar ao DRAI3, no entanto compatível com o Excel 2007 e 2010, não sendo compatível com versões anteriores do Excel e DRAI3 resultado de uma revisão, atualização e melhoramentos sobre o DRAI2.

Como principais características do DRAI SAF-T (BDO, 2020b) destaca-se:

- Testes de auditoria à totalidade dos registos contabilísticos de forma automática;
- Preenchimento automático de um conjunto de informação contabilística e financeira, importante para a auditoria;
- Complemento às atuais aplicações informáticas de revisão e auditoria;
- Procedimentos automáticos de auditoria sobre todas as transações, nomeadamente:
    - Validação de integridade e estrutura de ficheiros e de registos;
    - Validação de NIF's de clientes e fornecedores;
    - Testes aos saldos de abertura;
    - Cruzamento de informação entre registos contabilísticos e faturação;
    - Análise de duplicações;
    - Recálculo de valores (faturação e IVA).
- Compilação automática de informação vs revisão analítica:
    - Mapas e relatórios (contabilidade e faturação);
    - Balanço e demostração de resultados;
    - Comparação e evolução de saldos;
    - Rácios e KPI's;
    - Informação gráfica.

Como principais características do DRAI3 (BDO, 2020a) destaca-se a:

- Conformidade com o Sistema de Normalização Contabilística (SNC);
- Conformidade com as atualizações das ISA's;
- Revisão analítica e principais rácios adaptados ao SNC;
- Compatibilidade com Office 2007 e Windows 7 / Vista;
- Planeamento e programas de trabalho;
- Papéis de trabalho utilizados no trabalho de campo;
- Importação automática de balancetes;

- Informação financeira detalhada para cinco exercícios económicos;
- Conversor de balancetes POC (Plano Oficial de Contabilidade) em SNC;
- Controlo de aspetos administrativos do trabalho de auditoria;
- Programas de trabalho e planeamento baseado em asserções (afirmações tidas como verdadeiras, sobre as quais o auditor terá de validar).

✓ **MetricStream**

O *software* MetricStream (2020a) possui dois produtos, sendo que um deles tem em vista a gestão de auditoria interna e o outro a gestão da auditoria operacional.

O MetricStream (2020a) orientado para a gestão de auditoria interna foi projetado para ajudar no planeamento e gestão de auditorias internas de forma a simplificar, aumentar a produtividade e otimizar oportunidades. Esta ferramenta permite agilizar o planeamento e o agendamento de auditorias, bem como a execução, revisão e análise de resultados da auditoria e facilitar a criação de relatórios de auditoria e atividades de acompanhamento.

Como principais características do MetricStream (2020a) orientado para a gestão de auditoria interna para além das referidas anteriormente, destaca-se a documentação, gestão e avaliação de riscos em toda a organização; o planeamento da auditoria e alocação de auditores com base nas suas competências e disponibilidade e por fim o registo de observações, recomendações e possibilidade de anexar evidências.

Por sua vez, o MetricStream (2020b) orientado para a gestão da auditoria operacional permite avaliar a qualidade e eficiência de sistemas, processos e procedimentos internos em toda a organização. Esta ferramenta vai ao encontro do cumprimento de normas de autoridades como FDA (*Food and Drug Administration*), EPA (*Environmental Protection Agency*), OSHA (*Occupational Safety and Health Administration*) e ISO (*International Standard Organization*), fornece *insights* relevantes para a tomada de decisões informadas e oportunas, com vista a uma melhoria das operações e satisfação do cliente e é ainda possível a utilização de recursos de auditoria *off-line* e de forma móvel, o que permite aumentar a produtividade e eficiência de uma auditoria.

De entre as principais características do MetricStream (2020b) orientado para a gestão da auditoria operacional destaca-se o agendamento, a definição de planos de auditoria, a definição de objetivos, a criação de listas de verificações; a gestão de recursos com

rastreamento de tempo e de orçamento e a obtenção de resultados de auditoria operacional qualitativa e quantitativa em formatos pré-definidos.

- ✓ **MyWorkpapers**

A solução MyWorkpapers (2020) possui entre outros, um pacote de conteúdo de auditoria que possibilita uma simplificação do fluxo de trabalho de auditoria, desde a recolha de dados até à criação de relatórios.

Este *software* permite sobretudo uma visão completa da auditoria, desde o trabalho de campo à documentação, uma atribuição de tarefas de trabalho, definição de lembretes relativamente a prazos e possui padrões atualizados, *checklists*, planilhas e procedimentos com vista à agilização e conformidade do trabalho de auditoria. (MyWorkpapers, 2020)m

Através do portal MyWorkpapers (2020) é possível a comunicação com os clientes para a troca de informações e através do armazenamento em nuvem é possível o acesso ao MyWorkpapers em qualquer lugar, computador ou dispositivo inteligente, apenas para utilizadores aprovados.

- ✓ **Pentana Audit**

A solução Pentana Audit (Ideagen, 2020) é um *software* de gestão de auditoria baseado no risco e possibilita um alinhamento entre a auditoria e os objetivos estratégicos do negócio, possibilita também a centralização de operações e a realização de trabalho em modo *off-line*.

Esta ferramenta inclui, nomeadamente, as seguintes atividades: gestão do risco e do controlo, gestão de tempo e de despesas, gestão de papeis de trabalho, planeamento e agendamento da auditoria, gestão de evidências, através de testes, amostras e observações num único local e relatórios detalhados, internos e externos e acionáveis automaticamente. (Ideagen, 2020)

- ✓ **SAP Audit Management**

A ferramenta SAP Audit Management possibilita uma automatização de procedimentos internos de auditoria e um alinhamento de todo o negócio através de gestão de riscos e controlos críticos. (SAP, 2020)

Através da ferramenta SAP Audit Management, com utilização de recursos móveis é possível agilizar a auditoria e simplificar atividades como documentação de evidências, organização de documentos de trabalho eletrónicos, criação de relatórios de auditoria e otimização e planeamento de recursos. (SAP, 2020)

Como principais benefícios destaca-se a análise de uma auditoria em tempo real, uma avaliação de riscos mais fácil e rápida, uma automatização da auditoria e consequentemente uma redução de tempo no ciclo necessário para gerar relatórios. (SAP, 2020)

- ✓ **SIAUDI**

O SIAUDI (Software Público Brasileiro, 2020), Sistema de Auditoria Interna, é um *software* público brasileiro e foi desenvolvido sobre os princípios de eficiência e foco em resultados; descentralização; delegação de competências; gestão compartilhada; segurança de dados e informação; economia, redução de burocracias e anulação da utilização de papel.

Esta ferramenta está desenhada de forma que as suas funcionalidades comtemplem todas as etapas do processo de auditoria. Deste modo, o SIAUDI é composto por cinco módulos, nomeadamente, módulo de risco, módulo para elaboração do plano anual das atividades da auditoria interna, módulo de planeamento específico, módulo de relatório e módulo para elaboração do relatório anual das atividades da auditoria interna. (Software Público Brasileiro, 2020)

Por fim, pode referir-se que a acessibilidade a esta ferramenta é compartilhada, remota e *on-line*.

- ✓ **SIPTA**

O Sistema Informático de Papéis de Trabalho de Auditoria, SIPTA (WIS 4, 2018) é um *software* de auditoria que funciona em ambiente *on-line* e que possui origem portuguesa. Nesta ferramenta destacam-se as principais características, no que diz respeito à eficácia da auditoria, de supervisão e *report* do trabalho desenvolvido, confidencialidade da informação, uniformidade dos papéis de trabalho, equipa e carregamento de dados.

No que diz respeito à eficácia da auditoria pode destacar-se o acesso por parte dos auditores a toda a informação histórica, previamente introduzida; mapas de controlo que permitam avaliar a evolução e o grau de execução dos trabalhos de auditoria, por área; o registo de observações anexado a ficheiros e a possibilidade de visualização de um mapa de ajustamentos de auditoria com situações quantificadas, não quantificadas, relevantes, que serão consideradas automaticamente na emissão de relatórios.

Relativamente à supervisão e *report* do trabalho desenvolvido, este trabalho pode ser catalogado através de referências, que podem indicar um período de tempo, sendo possível posteriormente, por referência, visualizar listagens que resumem o trabalho de todos os auditores. Já no que concerne ao controlo e confidencialidade da informação é possível limitar o acesso de auditores com menores responsabilidades a diversos menus e é também possível controlar o acesso dos auditores à carteira de clientes, permitindo o acesso ou bloqueio, total ou em determinados anos, a um determinado cliente.

Ao nível da uniformidade de papéis de trabalho e programas de auditoria pode referir-se que os programas de auditoria podem ser replicados para o ano seguinte, possibilitando alterações no ano corrente; possibilidade de anexar papéis de trabalho a procedimentos específicos e a possibilidade de criação de três tipos de procedimentos, nomeadamente, procedimentos padrão (disponíveis para o planeamento de qualquer auditoria e associados ao normativo contabilístico), específicos (associados por exemplo a um determinado setor de atividade) e livres (na execução do trabalho, não estão disponíveis a auditores com perfil júnior).

Por fim, outras características do SIPTA (WIS 4, 2018) são ao nível da equipa, o controlo de tempos por empresa e por auditor e a possibilidade de controlo da evolução de trabalhos atribuídos a cada auditor, por área e procedimento de auditoria. Ao nível de carregamento e exportação de dados destaca-se o recarregamento de dados disponíveis em histórico, permitindo que sejam refeitas análises a esses dados, também a obtenção de

extratos em Excel, através de dados introduzidos em SAFT e um relatório de comparação de SAFTs importados, evidenciando registos novos, eliminados ou alterados.

- ✓ **SE Audit**

O SoftExpert Audit é um *software* corporativo que auxilia no controlo de todo o processo de auditoria. Através de uma única plataforma é possível gerir todas as etapas de uma auditoria desde o seu planeamento, preparação, definição de cronogramas, desenvolvimentos de planos e listas de verificação, até à sua execução, registo de constatações, emissão de relatórios e acompanhamento. Este *software* suporta todos os tipos de auditoria, internas, operacionais, de TI, de fornecedores de risco/controlo e de qualidade e existe a possibilidade de conexão com outras ferramentas do SoftExpert, como gestão de ativos, gestão de projetos e gestão de processos de negócio. (SoftExpert Software, 2020)

Através da ferramenta é possível realizar uma gestão de todas as competências do auditor, bem como da sua agenda de trabalho e as partes interessadas podem acompanhar o *status* das atividades da auditoria por meio de portais e em tempo real. Ao nível regulamentar, o SE Audit comtempla todos os controlos com o intuito de ir ao encontro dos requisitos de regulamentos internacionais relacionados com responsabilidade social, governaça, meio ambiente, saúde e segurança. (SoftExpert Software, 2020)

Ao nível de recursos do SE Audit (SoftExpert Software, 2020) pode indicar-se principalmente:

- Automatização de todo o processo de auditoria;
- Permite que a auditoria seja planeada a partir do zero ou a partir de modelos;
- Auxilia no planeamento de uma única auditoria ou de um programa anual de auditoria;
- Através de uma atribuição automática de tarefas, escalonamento, alertas e notificações por e-mail é possível uma otimização de tempo;
- Garantia de consistência da auditoria através de um único ambiente com todas as informações, documentos e evidências relacionadas com a auditoria;
- Gestão de perfis dos auditores, possibilitando uma correta atribuição deste, uma vez que são tidos em conta os requisitos da auditoria;
- Permite trabalhar *off-line* nas listas de verificação de auditoria;

- Geração automática de relatórios e compartilhamento de informações através de web ou ficheiros PDF.

✓ **SiAudit**

A SiAudit (2020), solução integral de auditoria, é uma ferramenta disponibilizada em ambiente web, projetado para sistematizar processos relacionados com auditorias financeiras ou revisões fiscais. Este *software* permite o cumprimento de conformidade normativa, padronização de atividades e papéis de trabalho, documentação de auditoria, com armazenamentos em nuvem para consulta em qualquer lugar/dispositivo, com segurança da informação e armazenamento ilimitado.

Neste *software* é disponibilizado um módulo de planeamento, auditoria, certificações e impostos. O módulo de planeamento é projetado para documentar nomeadamente uma avaliação do controlo interno, de risco e de fraude. O módulo de auditoria inclui programas de auditoria, papéis de trabalho e as evidências para documentar as conclusões do trabalho realizado, este módulo está subdividido em auditoria de conformidade, de encerramento e revisão periódica. O módulo de certificações está desenhado para documentar os pedidos de certificação, para que a qualquer momento possam ser consultados pelos auditores. Por fim, o módulo de impostos com papéis de trabalho que permitem documentar e apoiar revisões resultantes de uma auditoria a declarações fiscais. (SIAUDIT, 2020)

A ferramenta SiAudit (2020) possui ainda segregação de funções, controlo, através do qual é possível o acompanhamento de atividades e tarefas em tempo real, possui relatórios com informações de processos e indicadores de gestão, foi também projetado para cumprimento das ISA e fornece segurança nos processos, reduzindo a possibilidade de perda de informações, devido à informação estar armazenada em nuvem e com vários *backups*.

✓ **TeamMate Audit Management**

Team Mate Audit Management (Wolters Kluwer, 2020c) é um *software* que permite a gestão de uma auditoria em todo o fluxo de trabalho, nomeadamente, avaliação de riscos,

planeamento, execução da auditoria, relatórios e rastreamento de problemas para uma maior supervisão de riscos.

Através da integração é possível colaborar com as partes interessadas e recolher dados em tempo real, com o intuito de fornecer *insights*, ou seja, entendimento sobre os desafios enfrentados pelas empresas, aos *stakeholders.*

Com esta ferramenta existe a possibilidade de desenvolver planos de trabalho flexíveis para diversas equipas de auditoria, tipos de projetos e universos de auditoria, indo ao encontro, através de transparência e confiabilidade, dos requisitos regulamentares e legislativos exigidos.

1.3.4.3 Segurança de sistemas informáticos

Ferramentas de segurança de sistemas informáticos possibilitam a realização de auditorias às infraestruturas de TI da organização, com o intuito de garantir a confidencialidade, integridade e disponibilidade da informação, ou seja, de uma forma geral a segurança desta.

Como ferramentas de segurança de informação são de destacar: Galvanize, Access Rights Manager, Nagios, Nessus e Tripwire.

- ✓ **Galvanize**

Galvanize, até 2019 designado de ACL Data Analytics, desenvolve um *software* para profissionais de segurança, gestão de risco, conformidade e auditoria.

Este é um *software* de ponta a ponta composto por vários produtos diferentes, cada um referente a uma área diferente da governança organizacional, nomeadamente gestão de risco, conformidade, implementação de controlos, planeamento de auditoria, fraude, avaliação de TI, gestão de ciclo de vida e risco de terceiros, continuidade de negócio, política empresarial, gestão de incidentes de segurança, risco cibernético e análise de dados avançada. (Galvanize, 2020b)

Ao nível da auditoria esta é uma solução flexível de gestão que permite aumentar a eficiência em todo o seu fluxo de trabalho, planeamento, avaliações de risco, trabalho de

campo para análise e gestão de problemas e por fim possibilita a geração de relatórios. (Galvanize, 2020b)

Ao nível do planeamento de auditoria e fluxo de trabalho é possível, com a Galvanize, criar planos de auditoria com base no risco, programar e gerir projetos de auditoria para uma gestão eficiente de projetos, manter uma "biblioteca" de auditorias anteriores, modelos de fluxo de trabalho e matrizes de risco e controlo. (Galvanize, 2020a)

Relativamente à gestão de problemas e relatórios é possível uma visualização de todas as auditorias em tempo real, criar relatórios rapidamente com o intuito de informar as partes interessadas e uma consolidação de todos os "problemas" encontrados para indicar correções por departamento com acompanhamentos programados, lembretes e notificações. Ainda, no que diz respeito a uma análise integrada é possível rastrear e automatizar KPIs (Key Performance Indicator) em tempo real para um acompanhamento de desempenho e risco. (Galvanize, 2020a)

- ✓ **Access Rights Manager**

O Access Rights Manager (ARM) permite gerir e auditar os direitos de acesso de usuários a sistemas, dados e arquivos, possibilitando esta gestão e auditoria em toda a infraestrutura de TI. O ARM permite integrações com o Active Directory, servidores de arquivos, SharePoint, Exchange e OneDrive. (SolarWinds, 2020a)

Ao analisar autorizações de usuário e permissões de acesso, é possível verificar, através do ARM, que usuário tem acesso ao quê e quando ocorre esse acesso, é ainda possível criar relatórios personalizáveis para demonstrar conformidade com vários requisitos normativos, uma vez que estes requisitos requerem um monitoramento detalhado do acesso dos usuários, com enfâse para os usuários que têm acesso a dados críticos e confidencias. Desta forma, o ARM contribui para uma proteção das organizações contra os riscos potenciais de violação e perda de dados. (SolarWinds, 2020b)

- ✓ **Nagios**

O Nagios é um sistema de monitoramento que permite identificar e resolver problemas de infraestrutura de TI. Esta ferramenta monitora todos os componentes da infraestrutura de TI, nomeadamente aplicativos, sistemas operacionais, protocolos de rede e métricas

de sistema e infraestrutura de rede, de modo a garantir que estes estão a funcionar corretamente. (Nagios, 2020)

Desta forma, o Nagios (2020) permite nomeadamente o monitoramento de rede, do servidor e de aplicativos. O monitoramento de rede é realizado através de uma análise profunda de todas as fontes de tráfego de rede e potenciais ameaças à segurança. O monitoramento do servidor, nomeadamente Microsoft Windows e Linux, é realizado ao nível de métricas do sistema operacional, estado de serviço, estado de processos, desempenho, registo de logs, uso do sistema de arquivos, etc.

Por fim, o monitoramento de aplicativos, inclui análises em aplicativos Windows, Linux, UNIX e aplicativos Web, nos quais é possível o monitoramento completo de sites, aplicações web e serviços web, nomeadamente monitoramento de URL, de conteúdo, status HTTP, arquivos de log e logs do sistema.

- ✓ **Nessus**

A solução Nessus é uma ferramenta de avaliação e gestão de vulnerabilidades de TI baseadas em riscos. Este *software* é atualizado automaticamente em tempo real, fornecendo informações sobre *malware*, vulnerabilidades mais recentes, incluindo falhas de *software, patches* ausentes e configurações incorretas. (Tenable, 2020)

A solução contempla modelos pré-configurados que incluem auditorias de configuração e gestão de *patches* levando a um entendimento de quais as vulnerabilidades existentes. Este *software* inclui mais de 450 modelos de conformidade e configuração para possibilitar uma auditoria de conformidade e de configuração no que diz respeito a práticas recomendadas. Ao nível de visualização de resultados estes são apresentados em lista e agrupados por problemas ou categorias semelhantes. Por fim, os relatórios são personalizáveis, sendo possível criá-los com base em visualizações personalizáveis, criá-los em vários formatos e enviá-los a cada verificação. (Tenable, 2020)

- ✓ **Tripwire**

O *software* Tripwire é uma solução de gestão de risco e vulnerabilidades, que pretende reduzir o risco de ameaças cibernéticas. Esta solução fornece uma avaliação de

vulnerabilidade baseada no impacto e em riscos que incluem *data centres*, nuvens privadas e nuvens públicas. (Tripwire, 2020c)

Inicialmente o Tripwire foi projetado para realizar um monitoramento de integridade de arquivos, ou seja, detetar quando ocorrem alterações, maliciosas ou acidentais, em arquivos. Mais recentemente é possível uma deteção mais rápida de violação de dados, através de uma classificação dos dados de forma a sinalizar os eventos mais importantes a serem investigados. Este *software* também satisfaz os requisitos de conformidade para o registo de dados de log. (Tripwire, 2020a)

O Tripwire permite ainda a identificação de vulnerabilidades através de testes de penetração, seja em ambiente de rede ou aplicacional. Assim, é possível testar se o acesso não autorizado ou outras atividades maliciosas são possíveis. (Tripwire, 2020b)

Desta forma, o compromisso da Tripwire é contribuir para uma manutenção da segurança cibernética e integridade de sistemas, o que passa por detetar ameaças, identificar/gerir vulnerabilidades, gestão de log e gestão de configuração do sistema, com uma abrangência a ambientes físicos, virtuais e em nuvem.

1.3.4.4 Utilidade Geral

Ferramentas de utilidade geral englobam ferramentas genéricas, não específicas de auditoria, no entanto com potencial para utilização em auditoria.

Como ferramentas de utilidade geral são de destacar: Microsoft Access, Microsoft Excel e MySQL.

- ✓ **Microsoft Access**

O Microsoft Access é uma ferramenta de gestão de banco de dados da Microsoft. Através deste *software* é possível integrar múltiplas origens de dados, criar formulários e relatórios, criar pedidos de busca através de parâmetros e criar aplicações empresariais. (Microsoft, 2020b)

- ✓ **Microsoft Excel**

O Microsoft Excel é uma ferramenta para gestão de folhas de cálculo que permite realizar inúmeras tarefas, entre elas algumas com relevância para o trabalho do auditor. Desta forma, é possível nomeadamente detetar dados duplicados, dados em branco, ordenar dados, utilizar filtros, realizar fórmulas para realizar cálculos, utilizar formatação condicional, criar listas de dados, realizar resumo dos dados em tabelas dinâmicas ou elaboração de gráficos para uma melhor compreensão dos dados e criar previsões para prever tendências. Ao nível de partilha, e possível partilhar o documento com outras pessoas, possibilitando uma colaboração em tempo real. (Microsoft, 2020a)

- ✓ **MySQL**

O MySQL Database Service é um banco de dados que possui um mecanismo de análise integrado que permite a execução de análises complexas realizadas diretamente no banco de dados MySQL, eliminando assim a elaborada necessidade de movimentação e integração de dados. Este é um *software* disponível exclusivamente em Oracle Cloud Infrastructure. (Oracle, 2020a)

Este *software* possui também uma solução de auditoria baseada em políticas, o que possibilita às organizações a implementação de controlos de segurança mais fortes e a satisfação no que diz respeito à conformidade normativa. Para uma proteção contra o uso indevido de informações é exigido que as organizações rastreiem o acesso às informações, desta forma as organizações devem se capazes, e através do MySQL é possível rastrear e identificar quem fez o que, onde, quando, como e também realizar tentativas de *login* e tentativas de aceder a um banco de dados ou a uma tabela, realizar alterações desses dados e muito mais. (Oracle, 2020b)

1.3.5 Relação entre tipos de auditoria de SI e tipologias de CAATs

No subcapítulo 1.1.5 - Tipos de auditoria de SI, é feita a referência aos tipos de auditoria de SI considerados por Gelbstein (2017), para agora no presente subcapítulo ser feita uma relação entre esses tipos de auditoria de SI e as 4 tipologias de CAATs consideradas nesta dissertação (ver 1.3.4 - Tipos de Ferramentas), nomeadamente extração e análise de

dados, gestão de papéis de trabalho, segurança de sistemas informáticos e ferramentas de utilidade geral.

O governance é um tipo de auditoria de SI, auditoria essa que para ser realizada pode apoiar-se em ferramentas de gestão de papéis de trabalho e de utilidade geral. As ferramentas de gestão de papéis de trabalho são tidas em consideração, uma vez que possibilitam a compilação automática de informação, por exemplo de mapas e relatórios (contabilidade e faturação), balanço e demonstração de resultados, comparação e evolução de saldos, rácios e KPI's, o que pode originar informação gráfica.

As ferramentas de gestão de papéis de trabalho, numa auditoria de governance permitem ainda um alinhamento entre a auditoria e os objetivos estratégicos de negócio e possibilitam também realizar uma avaliação da qualidade e eficiência de processos e procedimentos internos, fornecendo com essa avaliação *insights* relevantes para a tomada de decisões informadas e oportunas por parte dos *stakeholders*.

Por sua vez, as ferramentas de utilidade geral, numa auditoria de governance permitem a elaboração de gráficos para uma melhor compreensão dos dados e também a criação de previsões de modo a prever tendências, o que é importante nesta área/tipo de auditoria de SI.

O tipo de auditoria de SI, operações 1, está relacionado com *data centers*, redes locais e amplas, segurança física e lógica, recuperação de desastres e continuidade de negócios, redes locais e acesso à Internet por filiais longe da sede. Este tipo de auditoria, na minha prestativa relaciona-se com ferramentas de segurança de sistemas informáticos, pois estas permitem nomeadamente realizar uma avaliação de vulnerabilidades baseada no impacto e em riscos que incluem *data centres*, nuvens privadas e nuvens públicas.

O tipo de auditoria de SI, operações 2, relacionado com sistemas e tecnologias não gerenciados pela função SI/TI, sistemas tipicamente industriais de automação e controle de supervisão e aquisição de dados, por estar ligado a sistemas deduz-se que a tipologia de CAATs sejam as ferramentas de segurança de sistemas informáticos.

Ao nível de auditoria a prestadores externos de serviços, nomeadamente contratos e acompanhamento de desempenho e gestão, os auditores podem recorrer a ferramentas de gestão de papéis de trabalho devido principalmente à facilidade de comunicação com o cliente auditado, à possibilidade de anexar evidências, nomeadamente contratos e ao planeamento de um acompanhamento de desempenho e gestão.

Entende-se por auditoria a aplicativos de negócios, uma auditoria principalmente a *software*, aplicativos móveis, atualizações, *patches* e correções, gestão de alterações, certificação, desta forma, as ferramentas de segurança de sistemas informáticos são relevantes uma vez que é possível obter informações sobre *malware*, vulnerabilidades mais recentes, incluindo falhas de *software, patches* ausentes, configurações incorretas, é também possível realizar uma auditoria de conformidade e de configuração, no que diz respeito a práticas recomendadas. Por fim, é importante referir que estas ferramentas permitem monitorar todos os componentes da infraestrutura de TI, de modo a garantir que estes estão a funcionar corretamente.

Relativamente à auditoria de SI em mobilidade, ou seja, a participação em redes sociais, o acesso à informação da organização em qualquer lugar, através de qualquer dispositivo com acesso à internet, podem destacar-se as ferramentas de segurança de sistemas informáticos. Estas ferramentas são destacadas neste tipo de auditoria de SI, uma vez que permitem gerir e auditar os direitos de acesso de usuários a sistemas, nomeadamente que usuário tem acesso ao quê e quando ocorre esse acesso.

A auditoria de SI em segurança é principalmente suportada por ferramentas de segurança de sistemas informáticos, uma vez que estas ferramentas permitem auditar os direitos de acesso de usuários a sistemas, dados e arquivos, possibilita o monitoramento de integridade de arquivos, permite o monitoramento de rede, que tem em vista a deteção de potenciais ameaças à segurança e permite também uma identificação/gestão de vulnerabilidade baseada no impacto e em riscos, através por exemplo de testes de penetração.

Por sua vez a auditoria de SI à gestão de riscos, a meu ver pode suportar-se em ferramentas de gestão de trabalho, pois algumas destas possibilitam a realização de uma auditoria baseada no risco, pode também suportar-se em ferramentas de segurança de sistemas informáticos, uma vez que estas são consideradas soluções de gestão de risco e por fim, suportar-se em ferramentas identificadas nesta dissertação de extração e análise de dados, pois é possível realizar um planeamento da auditoria baseado em riscos, criar tarefas com base em riscos, obter uma análise de resultados dos testes por risco e localizar riscos ocultos.

Em relação à auditoria de SI em dados as principais ferramentas de apoio são as ferramentas de extração e análise de dados, pois através destas é possível verificar o

conteúdo de tabelas em bases de dados, nomeadamente para verificar a integridade dos dados e a existência ou não de fraudes. Através destas ferramentas de extração e análise de dados pode, por exemplo, realizar-se consultas, comparações, estatísticas, identificar *outliers*, padrões, tendências, detetar lacunas e extrair dados através de amostragem.

Ainda relativamente à auditoria de SI em dados, as ferramentas de segurança de SI destacam-se, uma vez que possibilitam uma deteção da violação de dados, com o intuito de garantir a confidencialidade, integridade e disponibilidade da informação/dados. Por sua vez as ferramentas de utilidade geral destacam-se principalmente porque permitem realizar inúmeras análises aos dados, para uma melhor compreensão destes, e permitem também criar previsões para prever tendências.

Por fim, a auditoria a projetos SI/TI, é principalmente suportada por ferramentas de gestão de papéis de trabalho, com o intuito de registar observações, recomendações, anexar evidências, criar *checklists/*listas de verificações e facilitar a criação de relatórios de auditoria e atividades de acompanhamento, onde é possível planear um acompanhamento dos projetos SI/TI.

Desta forma, a Tabela 6, – Relação entre tipos de auditoria de SI e tipologias de CAATs., resume a tipologia de ferramentas que a meu ver podem ser utilizadas nos diferentes tipos de auditoria de SI, como descrito anteriormente.

Tabela 6 – Relação entre tipos de auditoria de SI e tipologias de CAATs.

Tipos de auditoria de SI	**Tipologia de ferramentas**
Governance	• Gestão de papéis de trabalho • Utilidade geral
Operações 1	• Segurança de sistemas informáticos
Operações 2	• Segurança de sistemas informáticos
Prestadores externos de serviços	• Gestão de papéis de trabalho
Aplicativos de negócios	• Segurança de sistemas informáticos
Mobilidade	• Segurança de sistemas informáticos
Segurança	• Segurança de sistemas informáticos

Tipos de auditoria de SI	Tipologia de ferramentas
Gestão de riscos	• Segurança de sistemas informáticos • Gestão de papéis de trabalho • Extração e análise de dados
Dados	• Extração e análise de dados • Segurança de sistemas informáticos • Utilidade geral
Projetos SI/TI	• Gestão de papéis de trabalho

Em conclusão, uma nota importante sobre as ferramentas de utilidade geral, que foram referidas em apenas 2 tipos de auditoria de SI, no entanto a meu ver e como o próprio nome indica estas ferramentas são de uso transversal/geral, podendo apoiar todos os tipos de auditoria de SI. De referir ainda que, algumas ferramentas podem enquadrar-se numa determinada tipologia e no entanto ser possível através delas realizar procedimentos considerados noutras tipologias de ferramentas, por exemplo ferramentas de gestão de papéis de trabalho que possibilitam a análise a dados.

1.3.6 Custos/Benefícios da utilização das CATTs na auditoria

Na aposta em tecnologias de suporte à auditoria é importante ter conhecimento e analisar quais os ganhos e custos, iniciais e contínuos que da implementação de um *software* de auditoria pode trazer não só para a auditoria, mas também e principalmente, como um todo, para a empresa que irá aplicar a auditoria.

Lima e Souza (2001) consideram que a automação da auditoria não surgiu para alterar a essência dos objetivos que envolvem os trabalhos, na verdade esta procura "*contribuir para o aperfeiçoamento da metodologia (...) em prol de uma maior produtividade, confiabilidade e qualidade*" (Lima & Souza, 2001, p. 69), possibilitando simultaneamente reduzir custos e melhorar a eficiência, a qualidade da documentação, a qualidade do trabalho de auditoria, reduzindo os níveis de risco, "*metas fundamentais à excelência dos serviços em um mundo globalizado em torno da tecnologia da informação*" (Lima & Souza, 2001, p. 69).

Deste modo, Lima e Souza (2001, p. 68) indicam os seguintes custos e benefícios:

A nível de custos/dificuldades:

- Formação do pessoal e superação de resistência à tecnologia;
- Decisão de que tarefas devem ser automatizadas primeiro;
- Avaliação, escolha e implementação das tecnologias (*hardware* e *software*);
- Manutenção das tecnologias;
- Gestão dos dispositivos de segurança e *back-up*;
- Equipamentos para os auditores.

A nível de benefícios:

- Redução de custos;
- Redução de níveis de risco;
- Maior partilha de conhecimento;
- Diminuição das limitações impostas pelos arquivos em papel;
- Maximização de tempo;
- Melhor qualidade de apresentação;
- Disponibilização de profissionais mais experientes para áreas mais técnicas e de maior risco;
- Agregação de valor ao trabalho de auditoria;
- Maior especialização dos profissionais;
- Fluxo de informações mais rápido;
- Maior satisfação profissional;
- Aumento da produtividade;
- Possibilidade de realização de um maior número de tarefas por parte de profissionais mais jovens /menos experientes.

Fargason (2001) faz referência a benefícios como:

- Economia de quantias substanciais de dinheiro para a empresa;
- Capacidade de realizar testes específicos para encontrar erros, na população;
- Possibilidade de realizar testes a toda a população;
- Diminuição significativa dos riscos de amostragem;

- Capacidade de executar análises adicionais, análises de maior volume e relatórios personalizados;
- Maior garantia dos resultados da auditoria;
- Aumento da confidencialidade, uma vez que o departamento de SI não sabe o que está a ser testado;
- Deteção precoce de riscos e avaliação mais abrangente destes, melhorando assim o planeamento da auditoria;
- Independência por parte da auditoria interna, uma vez que antes de usar o *software* era necessário solicitar formalmente os relatórios ad-hoc específicos do departamento de SI.
- Capacidade de limitar a amostra, tendo em conta a seleção de determinados dados como o departamento, conta, cliente ou fornecedor, etc;
- Maior rapidez na obtenção e análise de dados.

Segundo o manual CISA um auditor de SI deve ter em consideração os custos e os benefícios do uso de CAATs. Desta forma, o ISACA (2019d, p. 166) considera que as questões a serem consideradas, para a seleção do *software* de auditoria, devem incluir:

- Facilidade de uso para a equipa de auditoria atual e futura;
- Requisitos de treinamento;
- Complexidade de codificação e manutenção;
- Flexibilidade de uso;
- Requisitos de instalação;
- Eficiências de processamento;
- Esforço necessário para trazer os dados de origem para as CAATs para análise;
- Garantir a integridade dos dados importados, protegendo a sua autenticidade;
- Gravação da data e hora dos dados exportados em pontos críticos de processamento para sustentar a credibilidade da revisão;
- Obter permissão para instalar o *software* nos servidores da organização auditada;
- Confiabilidade do *software;*
- Confiabilidade dos dados processados.

Os autores Lima e Souza (2001) e Fargason (2001) fazem referência a benefícios comuns, da utilização das CAATs na auditoria, nomeadamente redução de custos; redução de riscos, devido a uma deteção precoce destes, melhorando assim o planeamento da auditoria; uma maior rapidez na obtenção e análise de dados, uma vez que o fluxo de informações é mais rápido, o que pressupõe um aumento da produtividade e por sua vez a maximização do tempo; e uma melhor qualidade de apresentação dos resultados da auditoria.

Feita a referência aos custos e benefícios, seguidamente na seleção do *software* de auditoria são vários os critérios a ter em conta. Os principais requisitos a que o ISACA (2019d) faz referência, é que o *software* deve ser de fácil utilização, processamento eficiente e ainda garantir a integridade dos dados importados, protegendo a sua autenticidade e os resultados que este *software* produz devem ser de alta confiabilidade e precisão. Assim, nesta perspetiva, segundo Sayana (2003) é preferível utilizar um produto comercial bem estabelecido.

Por fim, segundo Brito (2015) é importante e "*necessário, avaliar os benefícios e ganhos na sua implementação e considerar os custos no investimento em formação inicial e contínua sobre o software de auditoria*".

1.4 Conclusões da Revisão da Literatura

Esta dissertação foi desenvolvida com o intuito de catalogar ferramentas de suporte à auditoria, para que seja possível mais facilmente por parte do auditor identificar a/as ferramenta/as que mais se enquadram na auditoria que pretende realizar, com o intuito de tornar o trabalho de auditoria mais eficiente e eficaz.

Assim, a fim de catalogar algumas das CAATs existentes foram estudadas diversas ferramentas, nomeadamente ao nível de extração e análise de dados, gestão de papéis de trabalho, segurança de sistemas informáticos e ferramentas de utilidade geral.

Com o estudo de diversas ferramentas foi possível verificar as suas vastas aplicações nas diferentes fases de uma auditoria, desde o planeamento e agendamento da auditoria passando pela verificação de integridade de dados, identificação de fraudes, identificação de procedimentos que não estão a ser realizados de acordo com o definido, bem como a

garantia de confidencialidade, integridade e disponibilidade da informação ou até mesmo de ferramentas genéricas com potencial para utilização em auditoria.

Relativamente à evolução das CAATs foi possível verificar que a par de uma crescente utilização de SI está o aparecimento e o desenvolvimento de novas e sofisticadas ferramentas de auditoria, possíveis de utilizar nas diferentes fases de uma auditoria. Assim sendo, tudo isto contribui para uma maior utilização das CAATs nos trabalhos de auditoria, uma vez que estas ferramentas informáticas auxiliam os trabalhos realizados numa auditoria, facilitam o trabalho dos auditores e possibilitam uma melhor qualidade e eficiência do trabalho realizado e o alcance dos objetivos da auditoria.

Toda esta evolução ao nível da auditoria leva a alterações e evoluções no que diz respeito ao papel que o auditor desempenha. Assim, por forma aos auditores estarem preparados para obter o máximo de benefícios para uma auditoria é importante conhecerem as CAATs disponíveis no mercado e saberem avaliar as necessidades da auditoria, de modo a identificarem o ajuste adequado entre as ferramentas a utilizar e os objetivos da auditoria.

Para além do conhecimento, por parte do auditor, das CAATs disponíveis no mercado é importante a aposta na formação contínua em *software* específico para que os auditores possam tirar um melhor partido da evolução do *software* no desempenho do seu trabalho. Por outro lado, é também importante a aposta na formação específica e em conhecimentos abrangentes, a nível operacional e de negócio, não esquecendo a importância da aposta em certificações que permitem o reconhecimento das competências e conhecimentos obtidos pelos auditores.

Para a organização, ao nível da estrutura organizacional, a realização de auditoria de SI transmite confiança aos *stakeholders* e acarreta impactos positivos ao nível da tomada de decisão, controlo interno, gestão de riscos e gestão de vulnerabilidades. Desta forma, a auditoria de SI possibilita inúmeros benefícios que tornam mais fácil o alcance dos objetivos organizacionais, bem como operar de um modo mais eficiente o que consequentemente favorece e promove a viabilidade da organização.

Em suma, com a realização deste trabalho de revisão da literatura pode verificar-se que as CAATs podem ser aplicadas a vários níveis e desta forma utilizadas nas diversas fases de uma auditoria, acarretando assim, a sua utilização, diversas vantagens para o trabalho realizado pelo auditor bem como para a organização.

2 Estudo empírico

A presente investigação centra-se na utilização de CAATs na auditoria de SI. Desta forma, pretende-se conhecer as ferramentas informáticas de apoio à auditoria de SI, mais concretamente, perceber a sua utilização entre os auditores de SI e perceção destas ferramentas por parte dos membros do ISACA Lisbon Chapter.

2.1 Metodologia

Como metodologia de investigação optou-se pela aplicação de um inquérito, nomeadamente pela elaboração de um questionário a ser aplicado aos membros do ISACA Lisbon Chapter.

As questões presentes no questionário realizado foram formuladas com base na revisão da literatura anteriormente investigada.

Desta forma, com a aplicação do questionário, pretende-se responder aos objetivos inicialmente propostos, nomeadamente quais os impactos da utilização de CAATs para a organização auditada, averiguar que análises podem os auditores de SI realizar através de ferramentas de auditoria auxiliadas por computador e verificar quais as vantagens associadas à utilização de CAATs, no trabalho dos auditores.

Da aplicação do questionário realizada a 16 de janeiro de 2021 resultaram 3 insistências a fim de obter um maior número de respostas (ver apêndice 3 – Aplicação do Questionário – Fluxo Temporal).

2.2 Instrumento para recolha de dados

Para a recolha de dados e para ir de encontro aos objetivos propostos foram elaboradas 20 questões. Neste sentido, foram colocadas as seguintes e principais questões:

- Tendo em conta as ferramentas com as quais trabalhou no último ano, indique com que frequência utiliza as seguintes ferramentas?
- Tendo em conta algumas vantagens da utilização de CAATs para a auditoria, indique de que forma se identifica com as vantagens seguidamente enumeradas.
- Através das CAATs que utiliza com mais frequência indique as principais análises que estas lhe permitem realizar?

- Tendo em conta os impactos de uma auditoria de SI para a organização auditada, indique qual a sua concordância com os impactos seguidamente indicados.
- Atualmente possui alguma certificação, com relevância para a auditoria de SI?

Nas questões onde se questiona uma posição relativamente a um fator, foi utilizada uma escala de concordância de 1 a 5, uma escala tipo de Likert de 5 pontos, onde o nível 1 corresponde a "discordo totalmente" e o nível 5 equivale a "concordo totalmente", de modo a conhecer o grau de concordância dos inquiridos às perguntas colocadas. No entanto, para analisar a utilização de ferramentas por parte dos auditores inquiridos foi utilizada uma escala de Likert de 1 a 7, onde o nível 1 representa "não utiliza" e o nível 7 corresponde a "várias vezes por dia". O questionário aplicado pode ser consultado no apêndice 2.

2.3 Recolha de dados

Com o intuito de responder às questões referidas anteriormente, a recolha de dados realizou-se através de um questionário na aplicação *on-line* LimeSurvey. O questionário foi administrado com a colaboração e a membros do ISACA Lisbon Chapter, à data de 16 de janeiro de 2021.

O questionário encontra-se divido em cinco partes, com um total de 20 questões. A primeira parte correspondente à caracterização do perfil do auditor e da organização em que trabalha, a segunda parte encontra-se reservada à utilização e frequência de utilização de CAATs, a terceira parte relacionada com a perceção de vantagens, impactos e análises realizadas através de CAATs, a quarta parte é relativa à formação e certificação dos inquiridos e por fim a quinta parte onde foi apresentado um espaço para comentários/observações e espaço para indicação de e-mail, caso o inquirido pretenda ter acesso aos resultados.

Aos inquiridos foi garantido que todas as respostas são anónimas e confidenciais, sendo que os resultados obtidos serão apenas utilizados no âmbito desta investigação científica sem identificar, de qualquer forma, os respondentes.

2.4 Análise de dados

Neste subcapítulo será analisada a caracterização da amostra inquirida e serão analisados os dados obtidos através da aplicação do questionário anteriormente caracterizado.

2.4.1 Caracterização da Amostra

Nos seguintes subcapítulos serão expostos os resultados obtidos com a aplicação do questionário, que resultou de um total de 255 membros do ISACA, um total de 16 respostas e deste total 10 respostas completas e 6 respostas parciais.

Das 16 respostas obtidas apenas serão consideradas para análise as 10 respostas completas, ou seja, respostas cujos inquiridos responderam até à última pergunta do questionário. Ainda assim, em respostas abertas se esta for relevante será considerada com a devida indicação que advém de uma resposta parcial.

No entanto é importante compreender um pouco as respostas parciais e por isso é de referir que 1 inquirido entrou no questionário e não respondeu a nenhuma questão e os outros 5 inquiridos com respostas parciais responderam até à segunda página referente às perguntas relacionadas com a frequência de utilização.

Analisando agora a caracterização da amostra pode indicar-se que 4 inquiridos são do género feminino e 6 inquiridos do género masculino, representando respetivamente 40% de mulheres e 60% de homens (ver Gráfico 1).

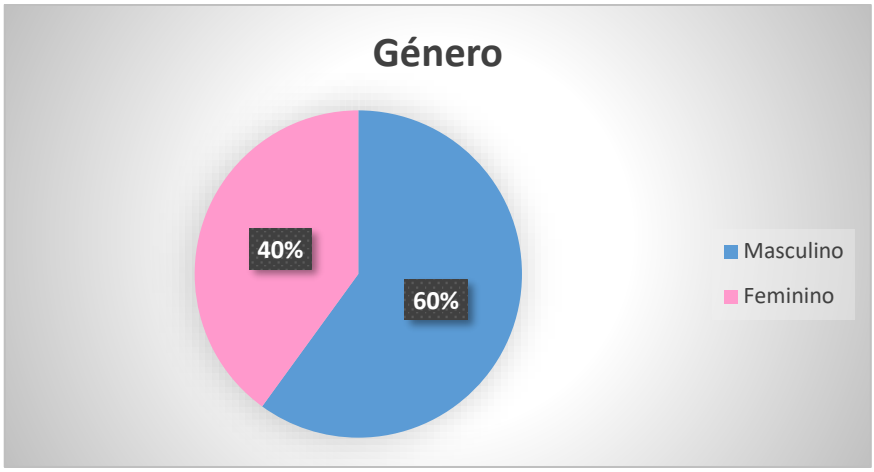


Gráfico 1 – Género, em percentagem, da amostra inquirida.

No que diz respeito à idade dos inquiridos verificou-se que nenhum inquirido possui idade inferior a 35 anos inclusive, 7 inquiridos possuem entre 36 e 45 anos de idade, 2 inquiridos possuem idade entre os 46 e os 55 anos e apenas 1 inquirido possui mais de 56 anos (ver Gráfico 2).

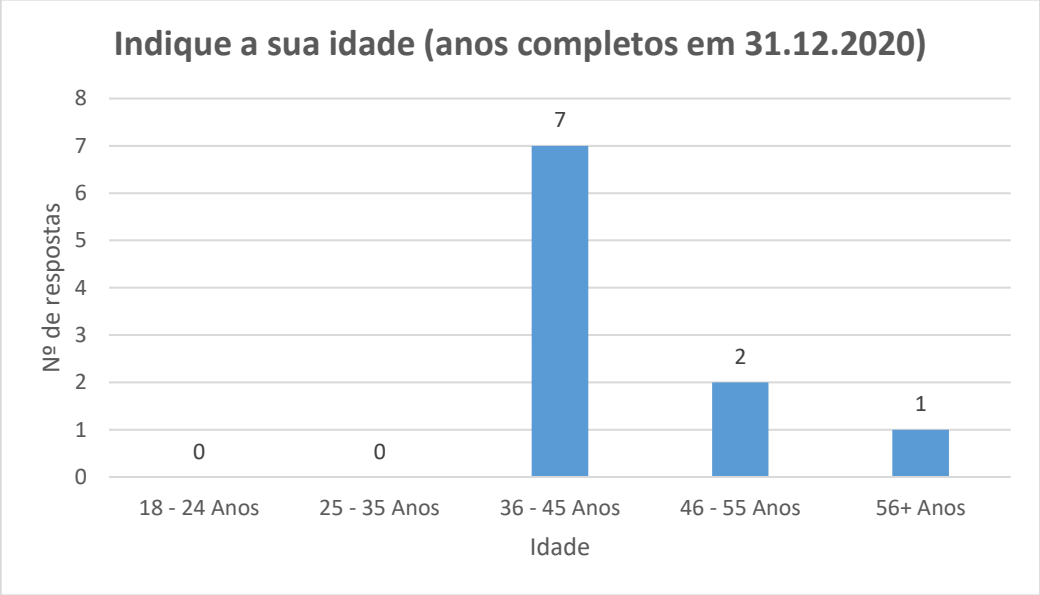


Gráfico 2 – Idade dos inquiridos, em anos.

Para a questão "quantos anos de experiência possui com auditor, à data de 31 de dezembro de 2020", (ver Gráfico 3) constata-se que 4 inquiridos possuem entre 5 e 9 anos de experiência, 3 inquiridos entre 10 e 14 anos de experiência e outos 3 inquiridos possuem mais de 15 anos de experiência em auditoria. Pode ainda referir-se que não foi indicada qualquer resposta para as opções entre 1 e 2 anos de experiência e entre 3 e 4 anos.

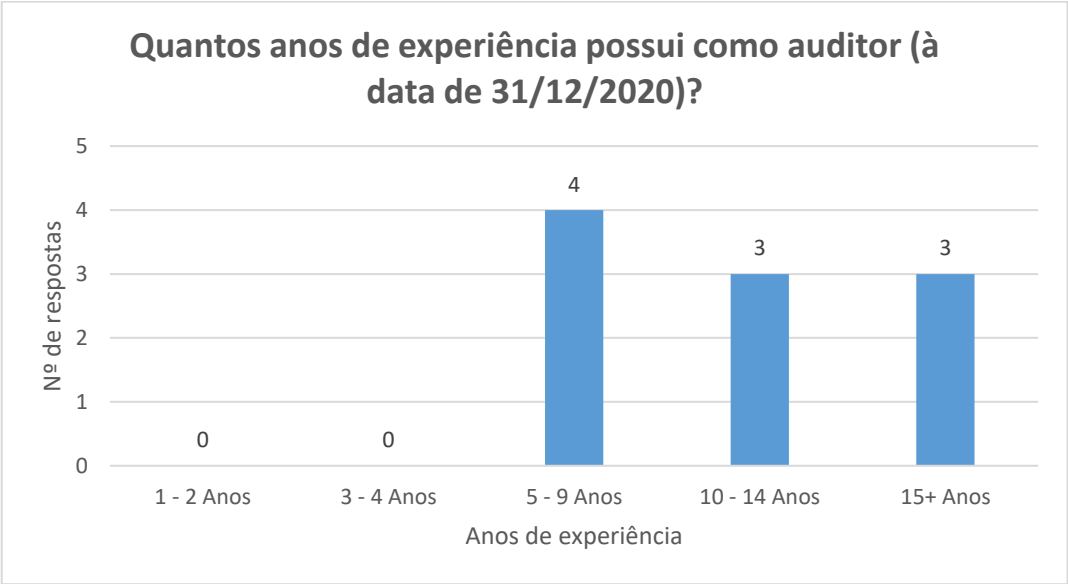


Gráfico 3 – Experiência, em anos, dos inquiridos em auditoria.

Relativamente a anos de experiência em auditoria de SI, que os inquiridos possuíam à data de 31 de dezembro de 2020, pode referir-se que 4 inquiridos possuem entre 5 e 9 anos, 2 inquiridos possuem entre 10 e 14 anos e outros 2 inquiridos indicam possuir mais de 15 anos de experiência em auditoria de SI. De notar que 2 inquiridos indicam possuir zero anos de experiência como auditor de SI e nenhum inquirido indicou possuir entre 1 e 2 anos e entre 3 e 4 anos de experiência em auditoria de SI (ver Gráfico 4).

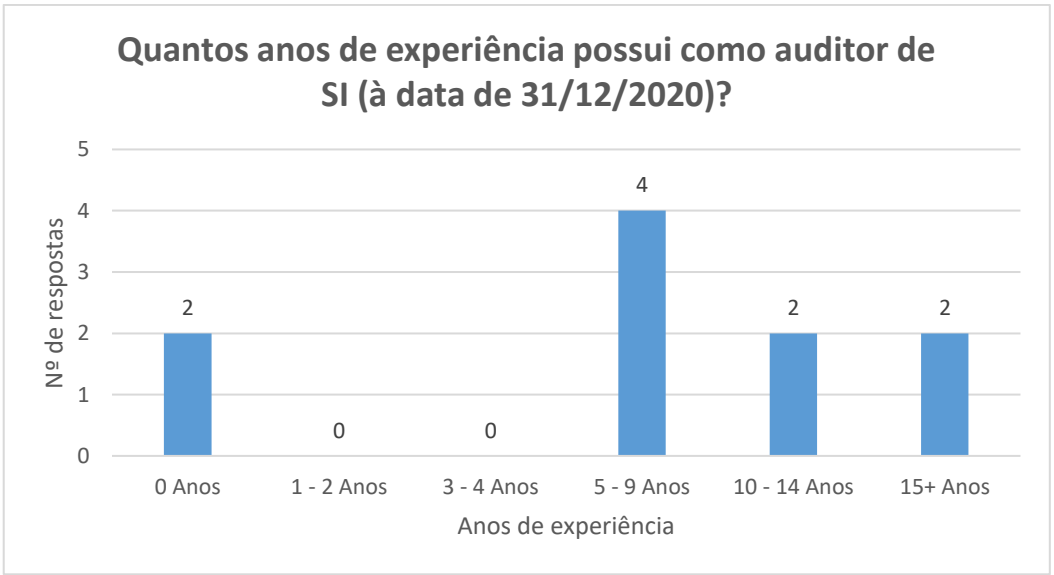


Gráfico 4 – Experiência, em anos, dos inquiridos em auditoria de SI.

Para a questão, "Indique o âmbito geográfico de atividade da sua empresa?", 1 inquirido respondeu Big Four, 5 inquiridos responderam âmbito nacional, 3 inquiridos responderam âmbito regional e 1 inquirido respondeu que a empresa para a qual trabalha é de âmbito local (ver Gráfico 5).

De notar que, entende-se por âmbito geográfico Big Four, empresas multinacionais, no entanto compreende-se agora que sendo o objetivo identificar os inquiridos a trabalhar em empresas que fazem parte das Big Four (Deloitte, Ernst & Young, KPMG e PwC), deveria ter sido considerado também o âmbito geográfico multinacional. O âmbito geográfico nacional, a meu entender, corresponde às NUTS I, ou seja, a empresa atua em diversas áreas do território continental. Como âmbito geográfico regional entende-se uma atuação, da empresa para a qual o inquirido trabalha, em apenas uma das 7 NUTS II. Por fim, para o âmbito geográfico local refere-se, na minha perspetiva, a uma atuação da empresa em apenas uma das 25 NUTS III. Para um melhor entendimento desta divisão, NUTS são um sistema hierárquico de divisão do território em regiões.

Gráfico 5 – Âmbito geográfico de atividade da empresa para a qual o inquirido trabalha, em percentagem.

Sobre a questão "Indique o setor/área de negócio a que pertence a sua empresa?" foram verificadas 7 (70%) respostas para a área financeira/banca, 1 (10%) resposta na área de serviços tecnológicos/consultoria, 1 (10%) resposta na área de seguros e 1 (10%) outra resposta na área de educação. Os restantes setores/áreas militar, contabilidade pública, fabrico/engenharia, cuidados de saúde/médico, comércio a retalho/grossista/distribuição,

construção/mineiro/petrolífero/agrícola, telecomunicações/comunicações, serviços públicos, transportes, farmacêutico, publicidade/marketing/comunicação social e aviação não foram indicados por nenhum inquirido (ver Gráfico 6).

Gráfico 6 – Setor/área de negócios a que pertence a empresa para a qual os inquiridos trabalham.

2.4.2 Frequência de Utilização

Relativamente à primeira questão da segunda parte do questionário, "Indique quais as ferramentas que conhece (independentemente se já trabalhou ou não com essa ferramenta)" constata-se que 9 inquiridos (90%) referem as ferramentas Microsoft Access e Microsoft Excel, 8 inquiridos indicam conhecer a ferramenta CaseWare IDEA Analytics, Galvanize e MySQL, 7 inquiridos, ou seja, 70% aponta conhecer a ferramenta TeamMate Audit Management, 6 inquiridos assinalaram a ferramenta Nessus, 5 inquiridos a ferramenta TeamMate Analytics, 4 inquiridos (40%) a ferramenta Nagios e ferramenta desenvolvida pela própria empresa. Ainda 3 inquiridos indicaram Pentana Audit e SAP Audit Management, 2 inquiridos referem conhecer as ferramentas

MetricStream, Access Rights Manager, Tripwire e outra ferramenta, nomeadamente a ferramenta Power BI.

De salientar que apenas 1 inquirido refere conhecer as ferramentas Active Data, ASD Auditor, Magique Galileo, SIPTA e outra ferramenta, sendo elas MicroStrateg, SAS, Azure Data Studio e Bwise Audit Management. Por fim, é ainda importante salientar que nenhum inquirido apontou conhecer a ferramenta, CaseWare Working Papers, DRAI, MyWorkpapers, SIAUDI, SE Audit e Si Audit (ver Gráfico 7).

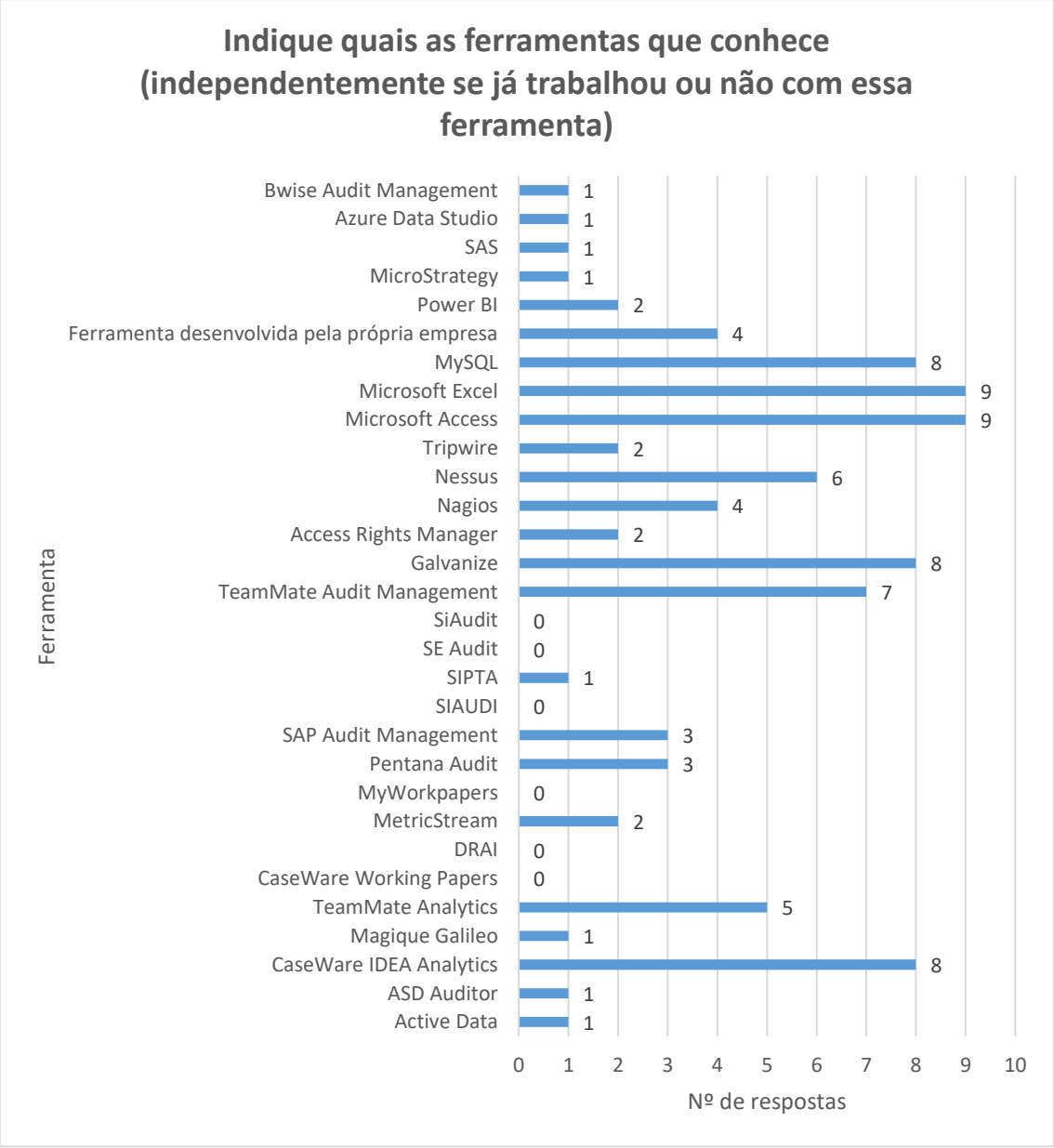


Gráfico 7 – Número de inquiridos que utiliza as ferramentas em análise.

Na realização e aplicação do questionário foi pensada a possibilidade de os inquiridos referirem outras ferramentas, através da questão "se indicou outra/as ferramenta/as na questão anterior, esclareça concretamente a opção selecionada a que ferramenta corresponde", assim foram indicadas as ferramentas Power BI mais que uma vez, MicroStrategy, SAS, Azure Data Studio e Bwise Audit Management. Por inquiridos com respostas parciais foram referidas as ferramentas Microsoft Word (ferramenta de utilidade geral), FoxPro que é uma base de dados, enquadrando-se por isso nas ferramentas de extração e análise de dados e foram ainda de forma genérica ferramentas próprias.

Especificando a que tipologia de ferramentas correspondem as indicadas pelos inquiridos, pode referir-se que as ferramentas Power BI, MicroStrategy, SAS, Azure Data Studio são ferramentas de extração e análise de dados e a ferramenta Bwise Audit Management é uma ferramenta de gestão de papéis de trabalho, mas a ferramenta Bwise também se pode estender à segurança de sistemas informáticos.

Seguidamente, no âmbito de frequência de utilização das ferramentas informáticas de apoio à auditoria, CAATs, por parte dos inquiridos no último ano (ver Gráfico 8), constata-se que as seguintes ferramentas: Magique Galileo, MetricStream, MyWorkpapers, SIAUDI, SIPTA, SE Audit, SiAudit, Access Rights Manager, Nagios, Nessus, Tripwire e outra Ferramenta, Azure Data Studio, não foram utilizadas por nenhum dos inquiridos.

As ferramentas utilizadas menos de uma vez por semana são as seguintes: Active Data, CaseWare IDEA Analytics, TeamMate Analytics, CaseWare Working Papers, DRAI, SAP Audit Management, Galvanize, Microsoft Access, Microsoft Excel e MySQL. Todas estas ferramentas foram indicadas por 1 inquirido como utilizadas menos de uma vez por semana, com exceção da ferramenta CaseWare IDEA Analytics referida, com esta frequência de utilização (manos de uma vez por semana), por 2 inquiridos.

Ferramentas como ASD Auditor, CaseWare IDEA Analytics e Galvanize foram utilizadas cerca de uma vez por semana, por apenas 1 inquirido.

A frequência de utilização "2 ou 3 vezes por semana" não foi referida para nenhuma ferramenta, por nenhum inquirido. Relativamente à frequência de utilização, várias vezes por semana, esta foi indicada por 1 inquirido para a opção de resposta "outra ferramenta 2", que corresponde à ferramenta SAS. Ainda nesta frequência de utilização, várias vezes por semana, esta foi assinalada por 2 inquiridos para as ferramentas CaseWare IDEA

Analytics, TeamMate Audit Management, MySQL e ferramenta desenvolvida pela própria empresa e a ferramenta Microsoft Excel mencionada por 3 inquiridos.

A ferramenta Microsoft Access foi indicada por apenas 1 inquirido como utilizada no seu trabalho cerca de uma vez por dia.

Por fim, relativamente à frequência de utilização, várias vezes por dia, as ferramentas CaseWare IDEA Analytics, Pentana Audit, Microsoft Access e outras ferramentas indicadas pelos inquiridos, nomeadamente Power BI, MicroStrategy e Bwise Audit Management foram indicadas por 1 inquirido, por 2 inquiridos foi indicada a ferramenta MySQL, por 3 inquiridos ferramenta desenvolvida pela própria empresa e por 5 inquiridos Microsoft Excel.

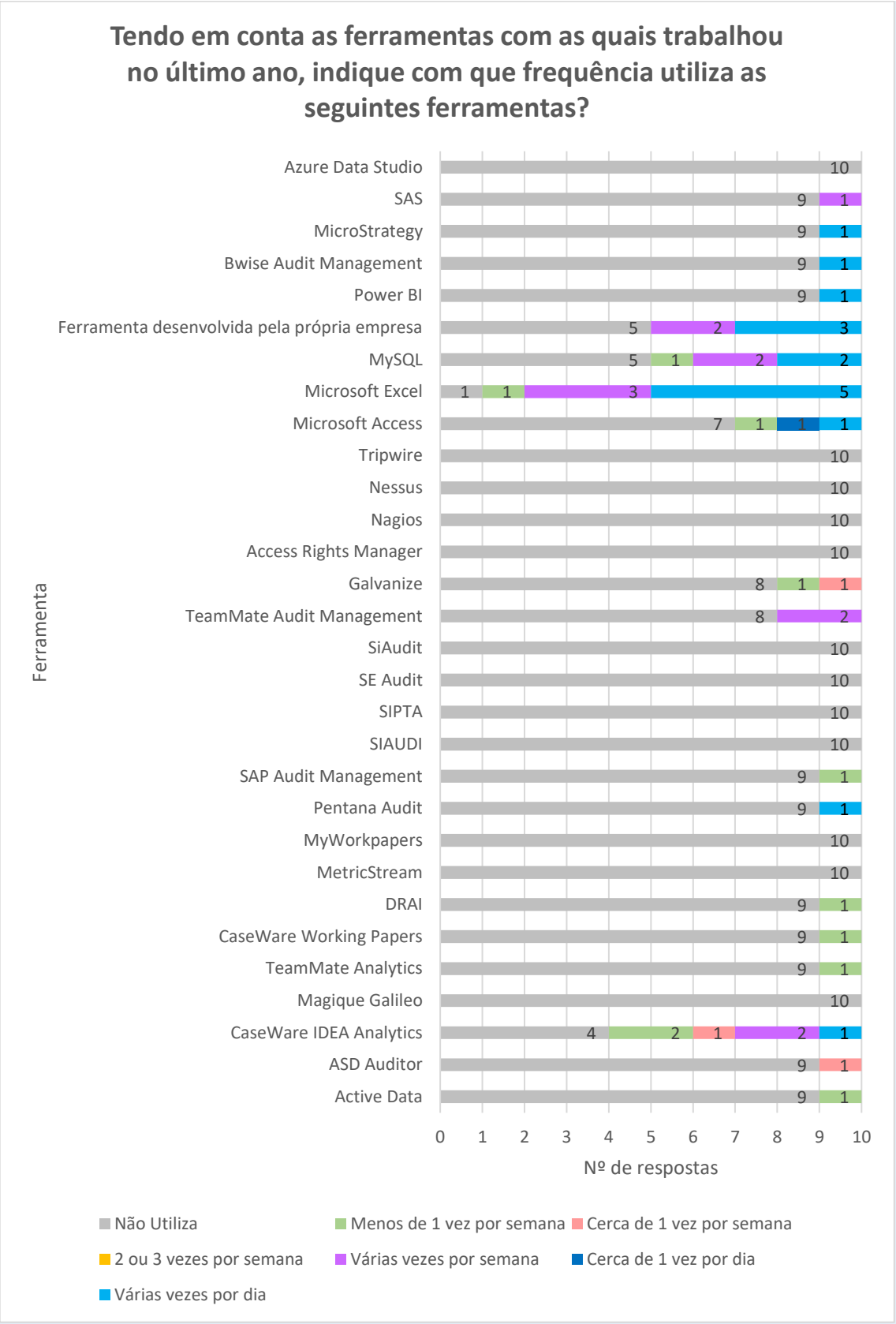


Gráfico 8 – Frequência de utilização das ferramentas informáticas de apoio à auditoria.

Questionados os inquiridos para hierarquizarem as ferramentas com as quais trabalham com mais frequência para as ferramentas com as quais trabalham com menos frequência foi possível verificar que as seguintes ferramentas ASD Auditor, Magique Galileo, CaseWare Working Papers, DRAI, MetricStream, MyWorkpapers, SIAUDI, SIPTA, Access Rights Manager, Nagios, Nessus, Tripwire e outra ferramenta 3, nomeadamente Azure Data Studio, não são mencionadas em qualquer nível de hierarquização. É ainda possível mencionar que foram apenas mencionados seis níveis de hierarquização (ver Gráfico 9).

Em primeiro na hierarquização foram identificados por 1 inquirido as ferramentas Active Data, CaseWare IDEA Analytics, Pentana Audit, SAP Audit Management, TeamMate Audit Management, outras ferramentas, nomeadamente Power B e Bwise Audit Management. Em primeiro lugar na hierarquização foi ainda identificado o Microsoft Excel por 3 inquiridos.

Na segunda posição da hierarquia foi mencionada, por 1 inquirido, a ferramenta CaseWare IDEA Analytics, SiAudit, TeamMate Audit Management, Microsoft Access, MySQL, ferramenta desenvolvida pela própria empresa e outra ferramenta, que corresponde à ferramenta MicroStrategy. Ainda em segundo lugar na hierarquização foi identificado o Microsoft Excel por 2 inquiridos.

Como terceiro na hierarquia foram indicadas as ferramentas SE Audit por 1 inquirido, a ferramenta Microsoft Access e ferramenta desenvolvida pela própria empresa referidas por 2 inquiridos e referida por 3 inquiridos o Microsoft Excel.

Na hierarquização, em quarto lugar foram identificadas por 1 inquirido as ferramentas CaseWare IDEA Analytics, TeamMate Analytics, Microsoft Excel e outra Ferramenta, o SAS e por 3 inquiridos o MySQL.

Na quinta posição da hierarquia foram identificadas apenas as ferramentas CaseWare IDEA Analytics e Microsoft Access, por 1 inquirido. Por fim, na sexta posição foram referidas a ferramenta Galvanize e Microsoft Excel, por 1 inquirido.

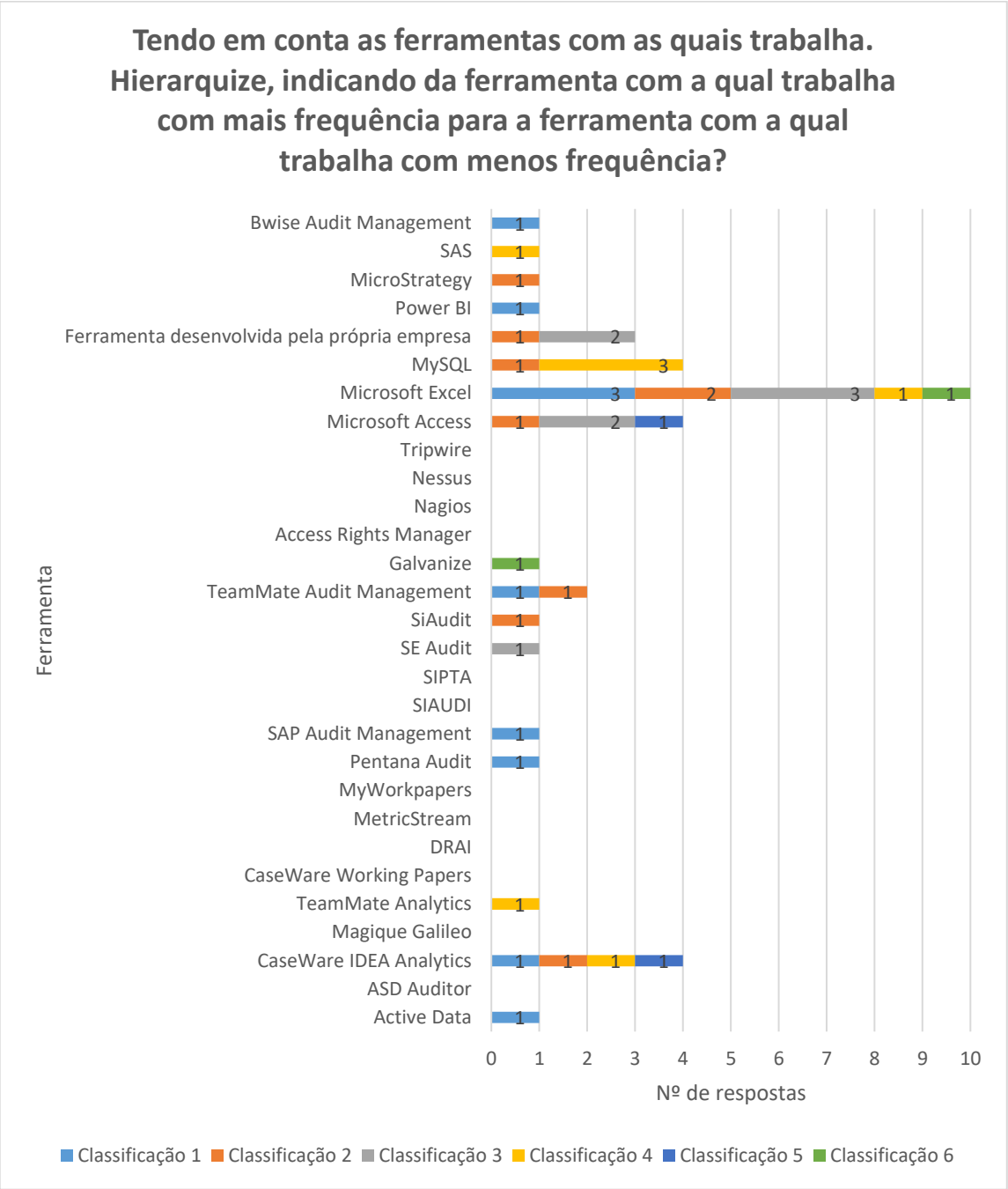


Gráfico 9 – Hierarquia de frequência de utilização das CAATs.

2.4.3 Vantagens, Análises e Impactos das CAATs

Analisando a perceção dos inquiridos sobre algumas vantagens da utilização de CAATs para a auditoria (ver Gráfico 10, onde se optou por apresentar, através de um identificador numérico e no eixo horizontal, cada uma das vantagens enumeradas na Tabela 7) é possível afirmar que relativamente à vantagem "economia de quantias substanciais de dinheiro para a empresa" (1) 2 inquiridos discordam parcialmente com esta vantagem, 1

inquirido não concorda nem discorda, 6 inquiridos concordam parcialmente e 1 inquirido concorda totalmente com esta primeira vantagem.

Para a segunda vantagem apresentada no Gráfico 10, "redução de níveis de risco" (2) 4 inquiridos dizem concordar parcialmente e 6 inquiridos afirmam concordar totalmente. Relativamente à "maior partilha de conhecimento" (3) 8 inquiridos concordam parcialmente e apenas 2 inquiridos concordam totalmente. Sobre a quarta vantagem apresentada, "diminuição das limitações impostas pelos arquivos em papel" (4) 3 inquiridos concordam parcialmente e 7 inquiridos concordam totalmente.

Para a vantagem "maximização de tempo" (5) 2 inquiridos concordam parcialmente e 8 inquiridos concordam totalmente. Seguidamente 4 inquiridos concordam parcialmente e 6 indicam concordar totalmente com uma "melhor qualidade de apresentação" (6) dos resultados da auditoria. Em relação à "disponibilização de profissionais mais experientes para áreas mais técnicas e de maior risco" (7) contata-se uma concordância parcial por parte de 3 inquiridos e uma concordância total de 7 inquiridos.

Questionados os inquiridos sobre o seu nível de concordância sobre a "agregação de valor ao trabalho de auditoria" (8) 2 inquiridos afirmam concordar parcialmente e 8 inquiridos revelam concordar totalmente com esta vantagem. Sobre uma "maior especialização dos profissionais" (9) de auditoria, os inquiridos identificam-se com esta vantagem da seguinte forma, 4 inquiridos concordam parcialmente e 6 inquiridos concordam totalmente com a afirmação nove, presente no Gráfico 10. Quanto a um "fluxo de informação mais rápido" (10), 2 inquiridos revelam não concordar nem discordar desta vantagem, outros 2 inquiridos concordam parcialmente e 6 inquiridos dizem concordar totalmente. Acerca de uma "maior satisfação profissional" (11) 2 inquiridos não concordam nem discordam, 3 inquiridos demostram concordar parcialmente e 5 inquiridos concordar totalmente.

No que diz respeito a um "aumento da produtividade" (12) 1 inquirido não concorda nem discorda desta vantagem, 2 inquiridos concordam parcialmente e 7 inquiridos concordam totalmente. Relativamente às vantagens "possibilidade de realização de um maior número de tarefas por parte de profissionais mais jovens /menos experientes" (13), "capacidade de realizar testes específicos para encontrar erros, na população" (14) e uma "diminuição significativa dos riscos de amostragem" (16) 4 inquiridos afirmam concordar parcialmente e 6 inquiridos concordam totalmente com as três vantagens referidas

anteriormente. Acerca da "possibilidade de realizar testes a toda a população" (15) 3 inquiridos afirmam concordar parcialmente e 7 inquiridos afirmam concordar totalmente com a vantagem.

Continuando a analisar as respostas dos inquiridos, 3 deles concordam parcialmente e 7 concordam totalmente com a "capacidade de executar análises adicionais, análises de maior volume e relatórios personalizados" (17). No que concerne a uma "maior garantia dos resultados da auditoria" (18), através da utilização de CAATs, 4 inquiridos concordam parcialmente e 6 inquiridos concordam totalmente. A respeito de um "aumento da confidencialidade, uma vez que o departamento de SI não sabe o que está a ser testado" (19) 1 inquirido diz não concordar nem discordar com a vantagem identificada, 3 inquiridos concordam parcialmente e 6 concordam totalmente.

Relativamente à vantagem de uma "deteção precoce de riscos e avaliação mais abrangente destes, melhorando assim o planeamento da auditoria" (20) e à "capacidade de limitar a amostra, tendo em conta a seleção de determinados dados como o departamento, conta, cliente ou fornecedor, etc" (22) 1 inquirido afirma não concordar nem discordar com as duas vantagens anteriormente referidas, 5 inquiridos revelam concordar parcialmente e 4 inquiridos apontam concordar plenamente.

Por fim, sobre uma "independência por parte da auditoria, uma vez que antes de usar o *software* era necessário solicitar formalmente os relatórios *ad-hoc* específicos do departamento de SI" (21) e sobre uma "maior rapidez na obtenção e análise de dados" (23) 5 inquiridos concordam parcialmente com estas afirmações tal como 5 inquiridos concordam totalmente.

Tabela 7 – Descrição das vantagens da utilização de CAATs para a auditoria.

Número	Vantagem
1	Economia de quantias substanciais de dinheiro para a empresa.
2	Redução de níveis de risco.
3	Maior partilha de conhecimento.
4	Diminuição das limitações impostas pelos arquivos em papel.
5	Maximização de tempo.
6	Melhor qualidade de apresentação.
7	Disponibilização de profissionais mais experientes para áreas mais técnicas e de maior risco.
8	Agregação de valor ao trabalho de auditoria.
9	Maior especialização dos profissionais.

Número	Vantagem
10	Fluxo de informação mais rápido.
11	Maior satisfação profissional.
12	Aumento da produtividade.
13	Possibilidade de realização de um maior número de tarefas por parte de profissionais mais jovens /menos experientes.
14	Capacidade de realizar testes específicos para encontrar erros, na população.
15	Possibilidade de realizar testes a toda a população.
16	Diminuição significativa dos riscos de amostragem.
17	Capacidade de executar análises adicionais, análises de maior volume e relatórios personalizados.
18	Maior garantia dos resultados da auditoria.
19	Aumento da confidencialidade, uma vez que o departamento de SI não sabe o que está a ser testado.
20	Deteção precoce de riscos e avaliação mais abrangente destes, melhorando assim o planeamento da auditoria.
21	Independência por parte da auditoria, uma vez que antes de usar o *software* era necessário solicitar formalmente os relatórios *ad-hoc* específicos do departamento de SI.
22	Capacidade de limitar a amostra, tendo em conta a seleção de determinados dados como o departamento, conta, cliente ou fornecedor, etc.
23	Maior rapidez na obtenção e análise de dados.

Para uma melhor compreensão do Gráfico 10 é de mencionar que a Tabela 7 esclarece a que número corresponde cada vantagem, presente no eixo horizontal do Gráfico 10.

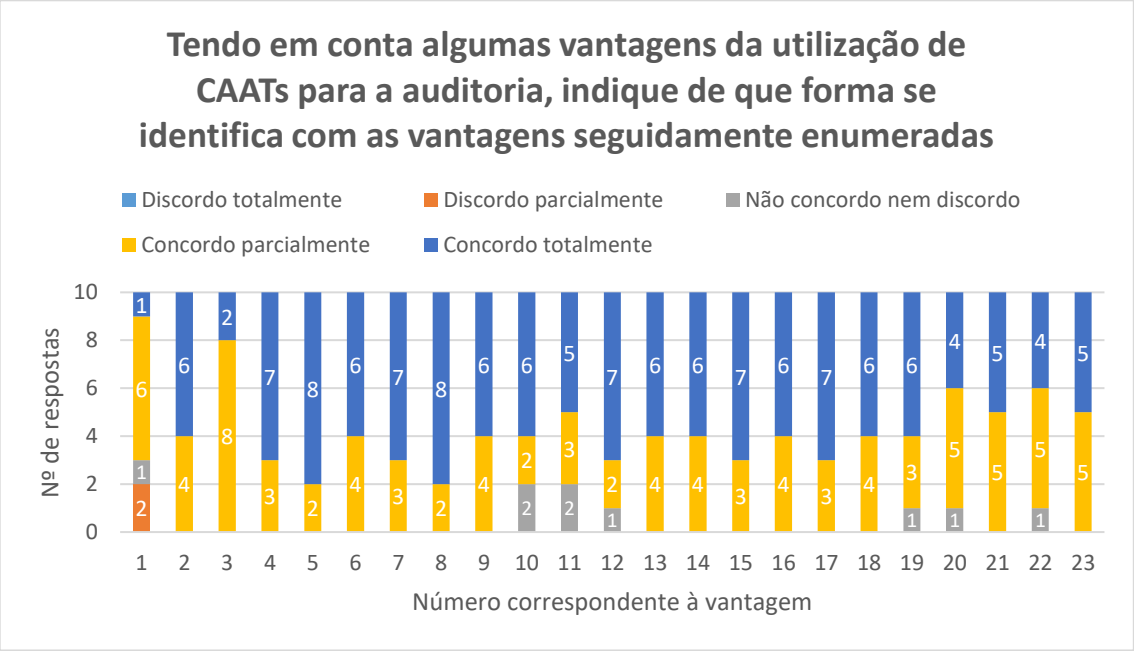


Gráfico 10 – Nível de concordância com algumas vantagens da utilização de CAATs para a auditoria.

Para a questão "em que medida considera que as ferramentas que utiliza como suporte às auditorias que realiza são uma boa base de trabalho e contribuem positivamente para o trabalho que executa" 1 inquirido indicou não concordar nem discordar da afirmação, 2 inquiridos responderem concordo parcialmente e 7 inquiridos responderam concordo totalmente. Relativamente às opções de resposta discordo totalmente e discordo parcialmente não foi registada qualquer resposta (ver Gráfico 11).

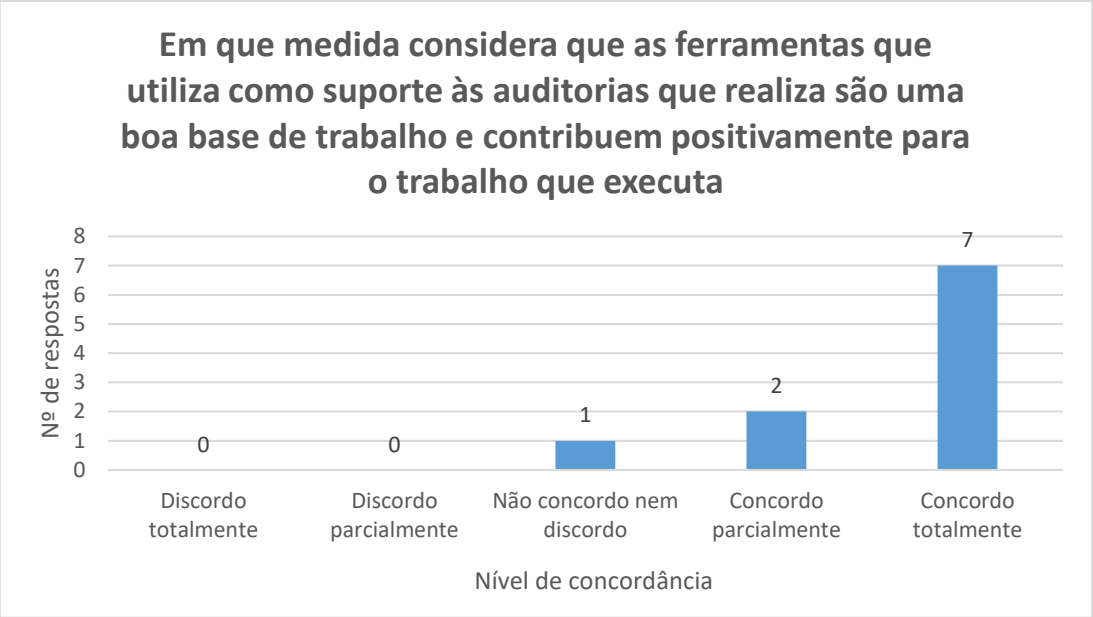


Gráfico 11 – Nível de concordância relativamente à contribuição positiva das CAATs para o trabalho que o inquirido executa.

Questionados os inquiridos "através das CAATs que utiliza com mais frequência indique as principais análises que estas lhe permitem realizar" foram referidas análises como a "identificação de exceções, anomalias e padrões", a "análise de *logs*, controlo de acessos, *data quality*", a verificação de "duplicações, extração de amostras, acessos indevidos". Outros inquiridos referiram a "análise de grandes quantidades de dados, a relação de dados de sistemas diferentes e a rapidez de processamento de grandes quantidades de dados", os "acessos indevidos, análise de *logs*" e "sequências duplicadas, dados fora do padrão e configuração de *thresholds*".

Seguidamente, no que diz respeito à concordância dos inquiridos com alguns impactos de uma auditoria de SI para a organização auditada, (ver Gráfico 12) pode referir-se que relativamente à gestão de vulnerabilidades 4 inquiridos concordam parcialmente e 6

inquiridos concordam totalmente com este impacto, seguidamente para o impacto no controlo interno constata-se uma concordância parcial de 5 inquiridos e uma concordância total de outros 5 inquiridos. Relativamente ao impacto nos mecanismos de gestão de risco constata-se que 3 inquiridos concordam parcialmente e 7 inquiridos concordam totalmente.

Para o impacto referente aos mecanismos de controlo dos SI verifica-se uma concordância parcial por parte de 4 inquiridos e uma concordância total de 6 inquiridos, no que se refere à imagem da organização perante os *stakeholders* observa-se que 8 inquiridos concordam parcialmente e apenas 2 inquiridos concordam totalmente com este impacto de uma auditoria de SI na organização auditada. Sobre o impacto na tomada de decisão, 1 inquirido não concorda nem discorda, 4 inquiridos concordam parcialmente com este impacto na organização auditada e 5 inquiridos concordam totalmente.

Por fim, em relação ao impacto de uma auditoria de SI no alcance de objetivos verifica-se que 1 inquirido não concorda nem discorda, 7 inquiridos concordam parcialmente e 2 inquiridos concordam totalmente e ainda relativamente ao impacto na eficiência da organização 6 inquiridos concordam parcialmente e 4 inquiridos concordam totalmente.

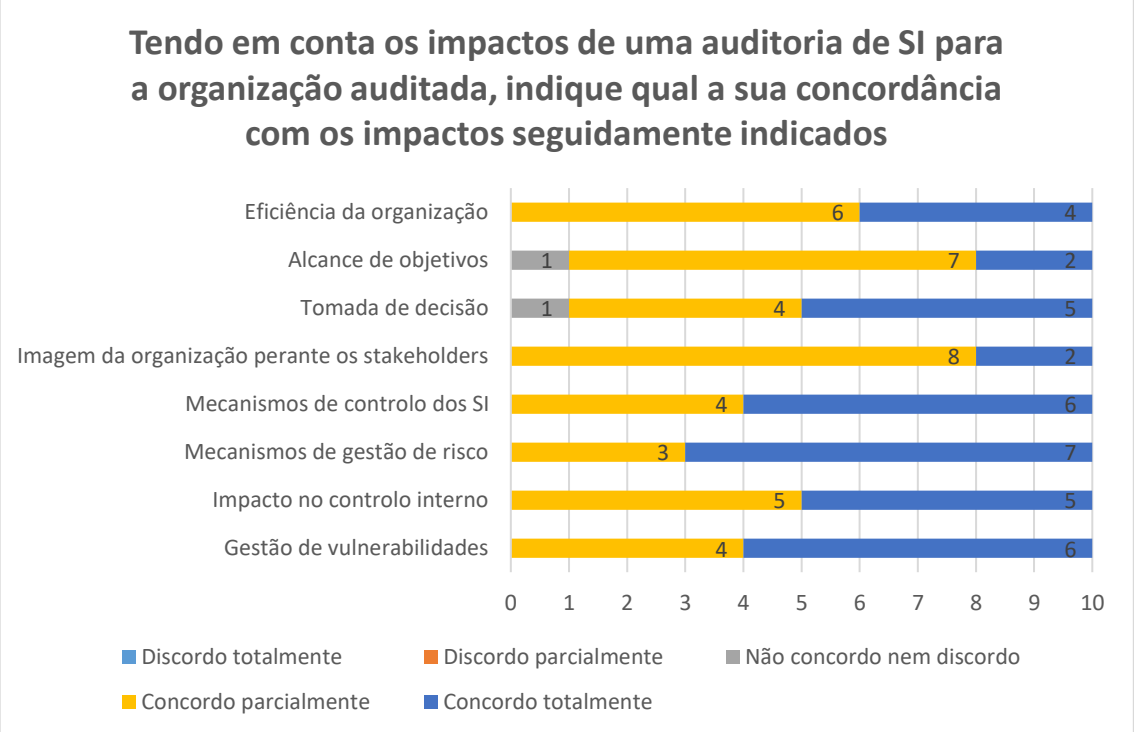


Gráfico 12 – Nível de concordância dos inquiridos relativamente aos impactos de uma auditoria de SI para a organização auditada.

Questionados os inquiridos, se consideram que existem outros impactos de uma auditoria de SI para a organização auditada, foi indicado por um inquirido "vários impactos para a melhoria do sistema de controlo interno".

2.4.4 Formação e Certificação

No que diz respeito à formação e certificação dos inquiridos, para a questão "em que medida considera que possui a formação adequada para o desempenho de funções com a utilização de CAATs" 2 inquiridos referem possuir uma formação insuficiente, 3 inquiridos indicam deter uma formação suficiente, 5 inquiridos, ou seja, 50% considera possuir uma formação adequada para o desempenho de funções que implicam a utilização de CAATs. Por fim, nenhum inquirido, neste âmbito, indicou possuir uma formação nula ou muito adequada, como é possível verificar no Gráfico 13.

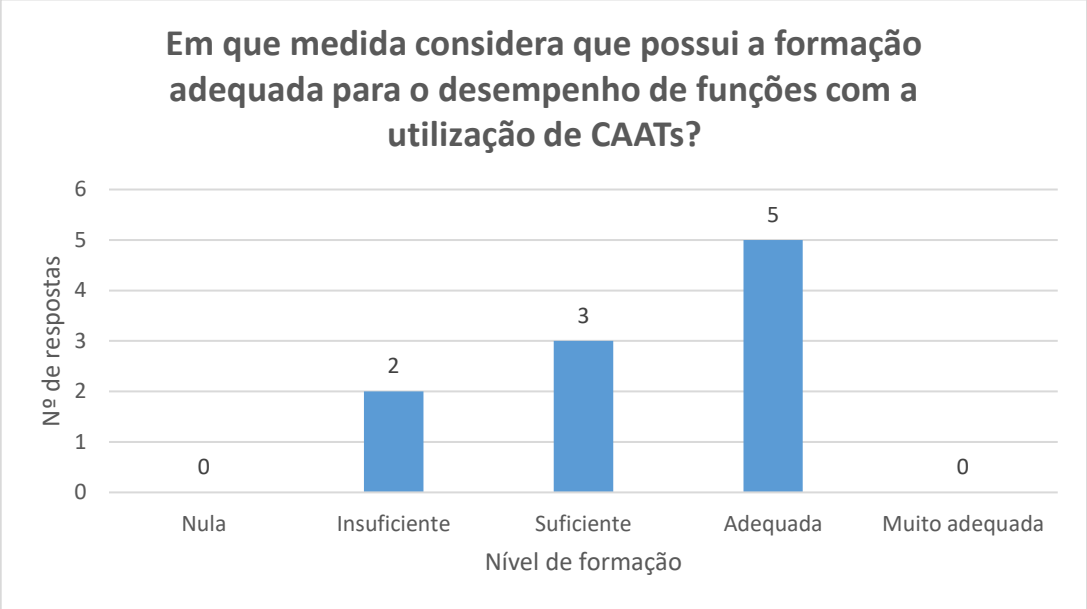


Gráfico 13 – Nível de formação para a utilização de CAATs.

Na área de estudo relativa às certificações foi questionado aos inquiridos se "atualmente possuem alguma certificação com relevância para a auditoria de SI", desta forma, constata-se que 90% dos inquiridos, ou seja, 9 inquiridos responderam "sim" e 1 inquirido

(10%) respondeu não possuir nenhuma certificação com relevância para a auditoria de SI (ver Gráfico 14).

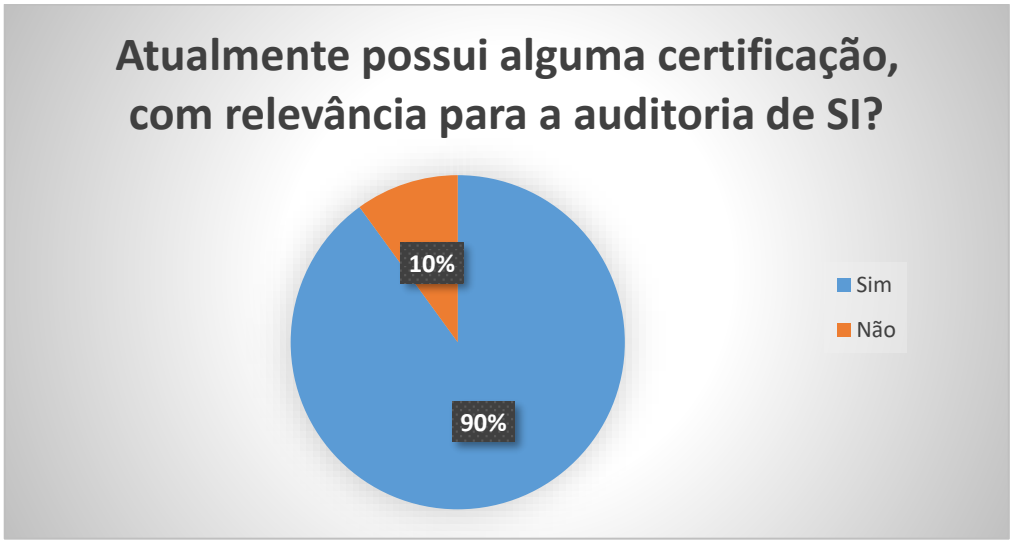


Gráfico 14 – Inquiridos com certificações de relevância para a auditoria de SI.

Dos inquiridos que indicaram possuir alguma certificação com relevância para a auditoria de SI, 7 inquiridos referem possuir a certificação CISA, 4 inquiridos possuem certificado CIA, 2 inquiridos são certificados em CRISC e CGEIT, 1 inquirido em CSX-P e nenhum inquirido refere a certificação CISM e a certificação CDPSE (ver Gráfico 15). Por fim, é importante referir que 4 inquiridos referem possuir outras certificações, nomeadamente CIDA, COBIT, ITIL, ISO 20000 e ISO 27001.

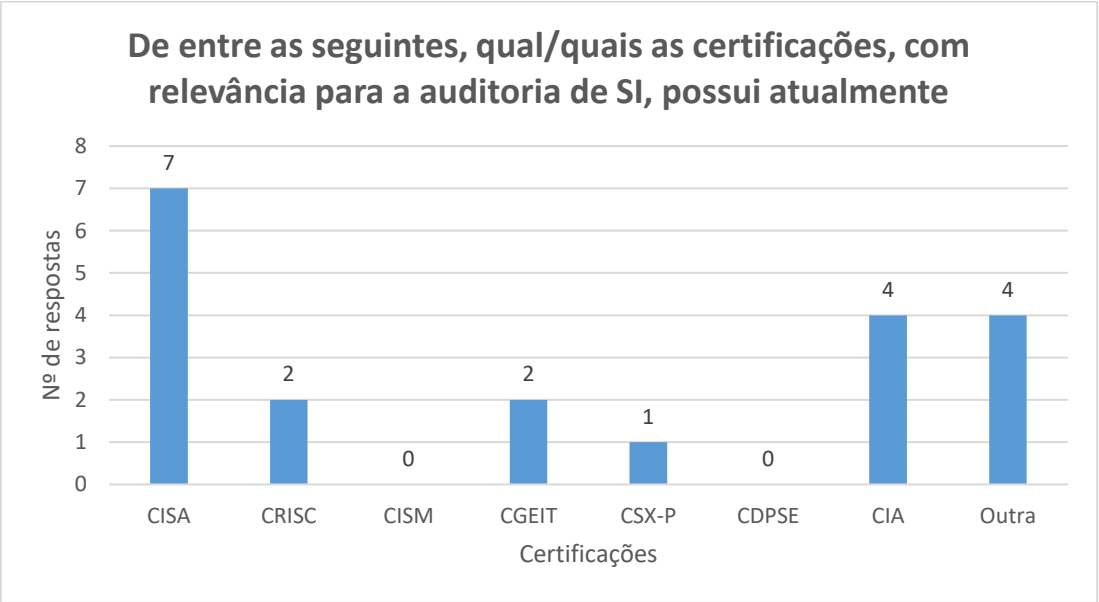


Gráfico 15 – Número de inquiridos que possui determinada certificação.

Realizado uma análise por género da questão "de entre as seguintes, qual/quais as certificações, com relevância para a auditoria de SI, possui atualmente", constata-se que apenas 1 inquirido do género masculino (10%) não possui qualquer certificação com relevância para a auditoria de SI. Seguidamente observa-se que 4 inquiridos (40%) do género masculino e 1 do género feminino (10%) possuem 1 certificação. Apenas 1 inquirido do género feminino (10%) possui 2 certificações e 1 inquirido do género masculino (10%) e 2 do género feminino (20%) possuem 3 certificações. De referir que nesta análise não estão a ser consideradas as respostas apresentas na opção "outra" certificação (ver Gráfico 16).

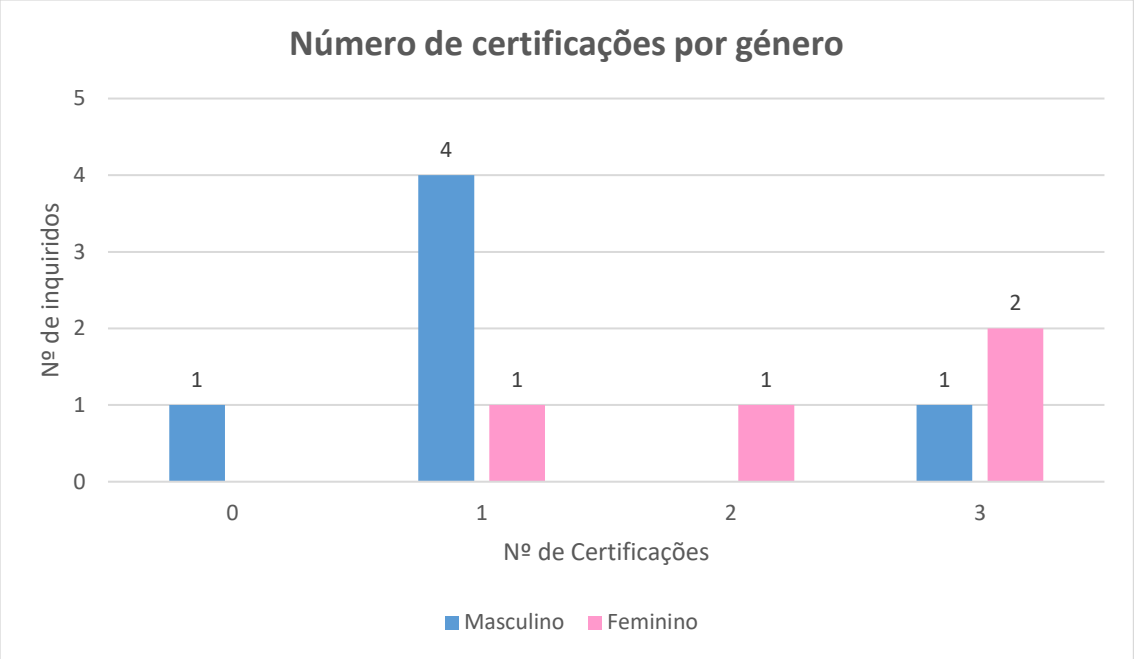


Gráfico 16 – Quantidade de certificações por género.

2.4.5 Comentários/Observações

Nesta secção do questionário foi dado espaço aos inquiridos para expressarem algum comentário ou observação pertinente no âmbito do estudo em causa. Desta forma, foi apresentado o seguinte comentário, "A utilização de CAATs na auditoria é muito vantajosa porque permite a automatização de procedimentos/testes rotineiros e, por outro lado, liberta o auditor para que este possa focar em análise mais técnicas".

2.5 Discussão de resultados

Neste subcapítulo será apresentada a discussão dos resultados verificados no subcapítulo anterior, 2.4 - Análise de dados, com origem no questionário aplicado aos membros do ISACA Lisbon Chapter.

Sobre a caracterização da amostra pode afirmar-se que foram obtidas mais respostas por parte de membros do género masculino (60%), o que era expectável, uma vez que na população constata-se que 86,7% dos membros são do género masculino, enquanto que 13,3% são do género feminino (ISACA, 2020g).

Relativamente à idade dos inquiridos, todos possuem acima dos 36 anos de idade e a maioria destes possui entre 36 e 45 anos de idade. Em anos de experiência tanto como auditor, como auditor de SI, a resposta mais dada pelos inquiridos foi entre 5 e 9 anos, nomeadamente por 4 inquiridos. De salientar que apenas em anos de experiência como auditor de SI, foram dadas respostas inferiores a 5 anos, nomeadamente 0 anos, o que dá a entender que estes inquiridos não possuem uma experiência como auditor de SI inferior a 1 ano ou então não são auditores de SI.

No que respeita ao âmbito geográfico de atividade da empresa para a qual os inquiridos trabalham, nota-se que a maioria é de âmbito nacional, nomeadamente 50% dos inquiridos. Com menor representatividade foi indicado o âmbito geográfico local e Big Four, ambas as opções de resposta com uma representatividade de 10%.

Relativamente ao setor/área de negócio no qual a população trabalha, através de dados fornecidos pelo ISACA Lisbon Chapter, é possível indicar que 38,82% indica o setor de atividade de consultoria, 18,04% o setor de serviços financeiros, 9,02% o setor do estado, 6,27% o setor *telco*, 5,10% o setor do ensino, e com as seguintes percentagens inferiores a 5%, o setor *utilities* (4,31%), desconhecido (3,53%), tecnológica (3,53%), retalho (3,14%), seguros (2,75%), indústria (2,35%), serviços (1,57%), saúde (1,18%) e hotelaria e turismo (0,39%) (ISACA, 2020g). Desta forma, é possível afirmar que um dos setores mais referidos na população é também o mais referido pelos inquiridos, o setor de serviços financeiros, com uma relevância de 70% no total de inquiridos.

Analisando agora o conhecimento de ferramentas CAATs, nota-se que as ferramentas mais mencionadas são nomeadamente Microsoft Access, Microsoft Excel, MySQL, CaseWare IDEA Analytics, TeamMate Audit Management, Galvanize e o Nessus, com mais expressão encontram-se ferramentas de utilidade geral. Como ferramentas menos mencionadas destacam-se Active Data, ASD Auditor, Magique Galileo, SIPTA, MetricStream, Access Rights Manager e o Tripwire, ou seja, principalmente ferramentas de extração e análise de dados. E não mencionadas por qualquer inquirido destacam-se CaseWare Working Papers, DRAI, MyWorkpapers SIAUDI, SE Audit e SiAudit, apenas ferramentas de gestão de papéis de trabalho.

De modo a retirar conclusões mais concretas e verdadeiras foi feita uma média relativa ao conhecimento, por parte dos inquiridos, da tipologia de ferramentas, para conseguir compreender sobre que tipologias de ferramentas CAATs os inquiridos mais têm

conhecimento. Assim, é possível concluir que os inquiridos conhecem mais ferramentas de utilidade geral, uma vez que 86,67% dos inquiridos diz conhecer as ferramentas de utilidade geral referidas no questionário. A tipologia de ferramentas menos conhecida pelos inquiridos são as ferramentas de gestão de papéis de trabalho, pois apenas 14,55% dos inquiridos afirma conhecer as ferramentas de gestão de papéis de trabalho referidas no questionário aplicado (ver Gráfico 17). Tal como se pode constatar na descrição detalhadas das ferramentas realizada no parágrafo anterior.

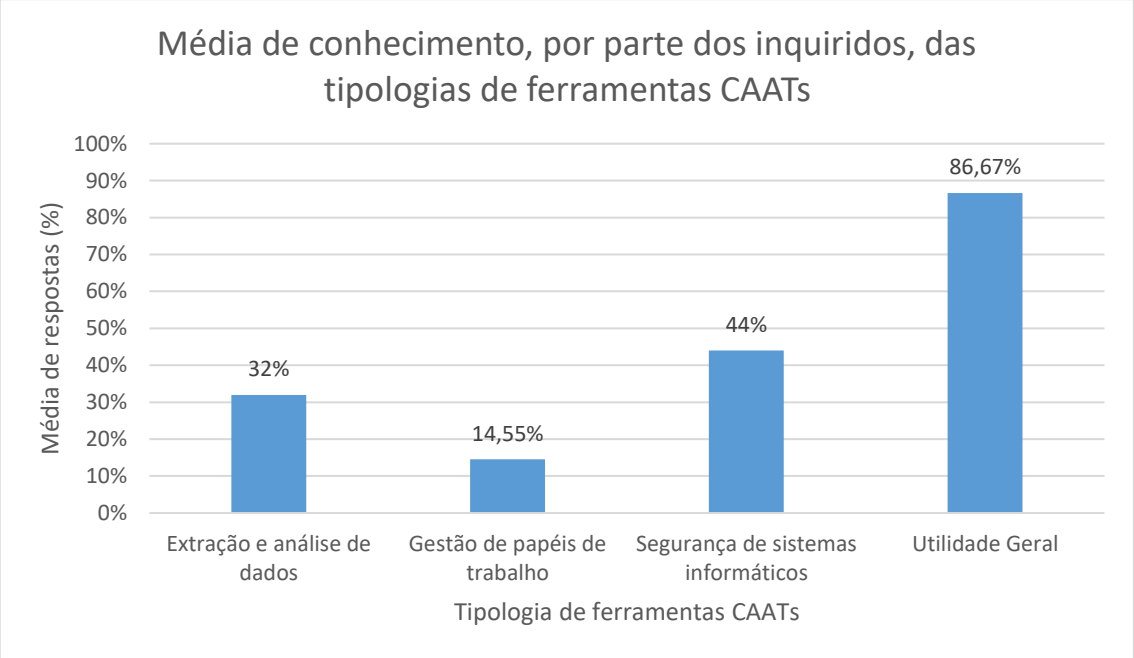


Gráfico 17 – Em média quantos inquiridos conhecem ferramentas CAATs de determinada tipologia.

Relativamente à frequência de utilização das ferramentas os inquiridos referem utilizar com mais frequência as ferramentas CaseWare IDEA Analytics, Pentana Audit, Microsoft Access, Microsoft Excel, MySQL e ferramenta desenvolvida pela própria empresa. Considera-se uma utilização de maior frequência as opções "cerca de uma vez por dia" e "várias vezes por dia". De notar que, e considerando a tipologia das ferramentas, a maioria das ferramentas utilizadas com maior frequência são de utilidade geral, o que vai ao encontro do verificado anteriormente no Gráfico 17.

Foram ainda referidas, com a frequência várias vezes por dia, outras ferramentas mencionadas pelos inquiridos, nomeadamente Power BI, Bwise Audit Management e Microstrategy.

Realizando uma análise entre as ferramentas que são conhecidas e as que não são utilizadas pelos inquiridos, podem referir-se as seguintes: Magique Galileo, MetricStream, SIPTA, Access Rights Manager, Nagios, Nessus, Tripwire e outra indicada pelos inquiridos Azure Data Studio.

Relativamente à hierarquização da utilização das ferramentas foi notada uma maior referência, independentemente do nível de hierarquização, às ferramentas de utilidade geral, nomeadamente ao Microsoft Access, Microsoft Excel MySQL, tal como verificado e mencionado nos parágrafos anteriores. Como ferramentas mencionadas em primeiro na hierarquização são indicadas Active Data, CaseWare IDEA Analytics, Pentana Audit, SAP Audit Management, TeamMate Audit Management, Microsoft Excel, Power BI e Bwise Audit Microstrategy.

As ferramentas CaseWare IDEA Analytics, Pentana Audit e Microsoft Excel foram mencionadas em primeiro na hierarquização da utilização e indicadas como as utilizadas com mais frequência. No entanto as ferramentas Active Data, SAP Audit Management e TeamMate Audit Management são referidas em primeiro na hierarquia das ferramentas que os inquiridos utilizam com mais frequência, mas são mencionadas na frequência de utilização como apenas utilizadas várias vezes por semana ou menos de 1 vez por semana, tal pode justificar-se se os inquiridos utilizarem as ferramentas, com as quais trabalham, com pouca frequência e assim sendo referi-las em primeiro na hierarquia.

No âmbito das vantagens da utilização de CAATs para auditoria os inquiridos estão em concordância parcial ou total para a maioria das vantagens apresentadas. As vantagens com as quais mais inquiridos concordam a um nível mais elevado são: "maximização de tempo", "agregação de valor ao trabalho de auditoria", "diminuição das limitações impostas pelos arquivos em papel", "disponibilização de profissionais mais experientes para áreas mais técnicas e de maior risco", "aumento da produtividade", "possibilidade de realizar testes a toda a população" e "capacidade de executar análises adicionais, análises de maior volume e relatórios personalizados".

Por outro lado, uma minoria entre 10 e 20% dos inquiridos revela não concordar nem discordar das existência de um "fluxo de informação mais rápido", de uma "maior satisfação profissional", de um "aumento da produtividade", um "aumento da confidencialidade, uma vez que o departamento de SI não sabe o que está a ser testado", de uma "deteção precoce de riscos e avaliação mais abrangente destes, melhorando assim o planeamento da auditoria" e da "capacidade de limitar a amostra, tendo em conta a seleção de determinados dados como o

departamento, conta, cliente ou fornecedor, etc.". Ainda, 2 inquiridos discordam parcialmente e 1 diz não concordar nem discordar da "economia de quantias substanciais de dinheiro para a empresa", possivelmente porque tiveram em consideração que a aposta na tecnologia implica gastos.

Assim, compreende-se o que foi verificado na revisão da literatura, sendo de extrema importância avaliar os ganhos e os benefícios da aposta e utilização de CAATs, sem esquecer os custos no investimento em *software* e na formação dos utilizadores.

Para além dos inquiridos estarem maioritariamente em concordância com as vantagens da utilização de CAATs apresentadas para a auditoria, nota-se que maioritariamente estes também consideram que as ferramentas que utilizam como suporte às auditorias que realizam são uma boa base de trabalho e contribuem positivamente para o trabalho que executam e apenas 10% dos inquiridos não concorda nem discorda desta opinião.

Questionados os inquiridos sobre as análises que as CAATs que utilizam lhes permitem realizar, estes referiram a identificação de exceções, anomalias e de padrões, a análise de *logs*, o controlo de acessos/acessos indevidos, a verificação de duplicações, extração de amostras, ou seja, na maioria das análises anteriores esta implícita a análise à qualidade dos dados. De notar que foram identificadas mais que uma vez a análise a acessos indevidos, a análise de *logs*, sequências duplicadas e análise de dados fora do padrão. É ainda importante referir que estas análises foram verificadas e mencionadas na revisão da literatura.

Relativamente aos impactos, da utilização de CAATs numa auditoria, verificou-se que a maioria dos inquiridos concordam total ou parcialmente com os impactos apresentados. Os impactos com os quais os inquiridos concordam mais, a um nível de concordância mais elevado, são os impactos nos mecanismos de gestão de risco, nos mecanismos de controlo dos SI e na gestão de vulnerabilidades.

No que concerne à medida em que os inquiridos consideram possuir uma formação adequada para o desempenho de funções com a utilização de CAATs, é de salientar que 50% dos inquiridos refere possuir uma formação adequada, nenhum inquirido refere possuir uma formação nula ou muito adequada e 2 inquiridos referem possuir uma formação insuficiente. Desta forma, o facto de 2 inquiridos terem referido possuir uma formação insuficiente vem salientar o que foi concluído na revisão da literatura, nomeadamente, que o facto de a auditoria estar em constante evolução e essa evolução

implicar alterações e evoluções no que diz respeito ao papel que o autor desempenha, isto irá implicar um acompanhamento das competências dos auditores.

Relativamente à certificação dos inquiridos quase a totalidade destes afirmou possuir alguma certificação com relevância para a auditoria de SI, concretamente 90% dos inquiridos. Destes inquiridos que dizem possuir alguma certificação com pertinência para a auditoria de SI, a certificação com mais respostas foi a CISA, a certificação CSX-P foi mencionada apenas por 1 inquirido e as certificações CISM e CDPSE não foram mencionadas por nenhum inquirido.

No que diz respeito à população verifica-se que de um total de 231 certificações, 85 membros do ISACA Lisbon Chapter possuem certificação CISA, 44 membros a certificação CRISC, 58 membros a certificação CISM, 23 membros a certificação CGEIT, 7 membros a certificação CSX-P, 14 membros a certificação CDPSE e não foi indicada informação sobre a certificação CIA ou outras certificações (ISACA, 2020g). Assim, pode concluir-se que tanto no questionário aplicado como na população, a certificação com mais relevância é a CISA e a certificação CDPSE é a que possui menos importância na população, e na aplicação do questionário a CDPSE é uma das certificações que nenhum inquirido possui. Assim, podemos dizer que os dados obtidos vão, em parte, de encontro ao que se constata nos dados referentes à população.

Através da revisão da literatura a certificação CISA é a segunda mais antiga, com data da primeira certificação no ano de 1978 e também a segunda com um maior número de pessoas certificadas, assim é plausível que, tanto na população como na amostra inquirida, esta seja a certificação com maior número de membros/inquiridos certificados.

Relativamente à certificação CDPSE, com data da primeira certificação em 2020, esta é a certificação mais recente, não existindo dados na revisão da literatura referentes ao número de pessoas certificadas, podendo concluir-se que esse número é pequeno, dai esta certificação não ter sido mencionada por nenhum inquirido.

Por sua vez, os resultados obtidos relativamente à certificação CISM são fora do padrão, uma vez que esta certificação já não é recente, 2003 é o ano da primeira certificação, e na revisão da literatura refere-se que existem mais de 46.000 pessoas certificadas, no entanto nenhum inquirido referiu possuir esta certificação.

Realizando agora uma análise entre as certificações que os inquiridos possuem e o setor de atividade/área de negócio para a qual trabalham, pode referir-se que a certificação

CISA é indicada nos 4 setores mencionados pelos inquiridos (financeiro/banca, serviços tecnológicos/consultoria, seguros e educação). A certificação CIA é indicada pelos inquiridos nos setores financeiro/banca, serviços tecnológicos/consultoria e educação, por sua vez a certificação CGEIT é indicada pelos inquiridos nos setores serviços tecnológicos/consultoria e educação. Por fim, as certificações CRISC e CSX-P são mencionadas pelos inquiridos apenas no setor financeiro/banca.

De entre as outras certificações referidas pelos inquiridos pode mencionar-se que as mencionas mais que uma vez foram ITIL e ISO 27001.

Realizado uma análise por género da questão "de entre as seguintes, qual/quais as certificações, com relevância para a auditoria de SI, possui atualmente", na população (ver Gráfico 18) verifica-se que 103 (40,39%) membros do género masculino e 23 (9,02%) do género feminino não possui nenhuma certificação (entre CISA, CRISC, CGEIT, CISM, CDPSE e CSX-P), 60 (23,53%) membros do género masculino e 8 (3,14%) membros do género feminino possui apenas 1 certificação, 29 (11,37%) membros do género masculino e 2 (0,78%) membros do género feminino possuem 2 certificações, 20 (7,84%) membros do género masculino e 1 (0,39%) membro do género feminino possuem 3 certificações. Por fim, apenas membros do género masculino possuem 4 e 5 certificações, 7 (2,75%) membros e 2 (0,78%) membros respetivamente (ISACA, 2020g).

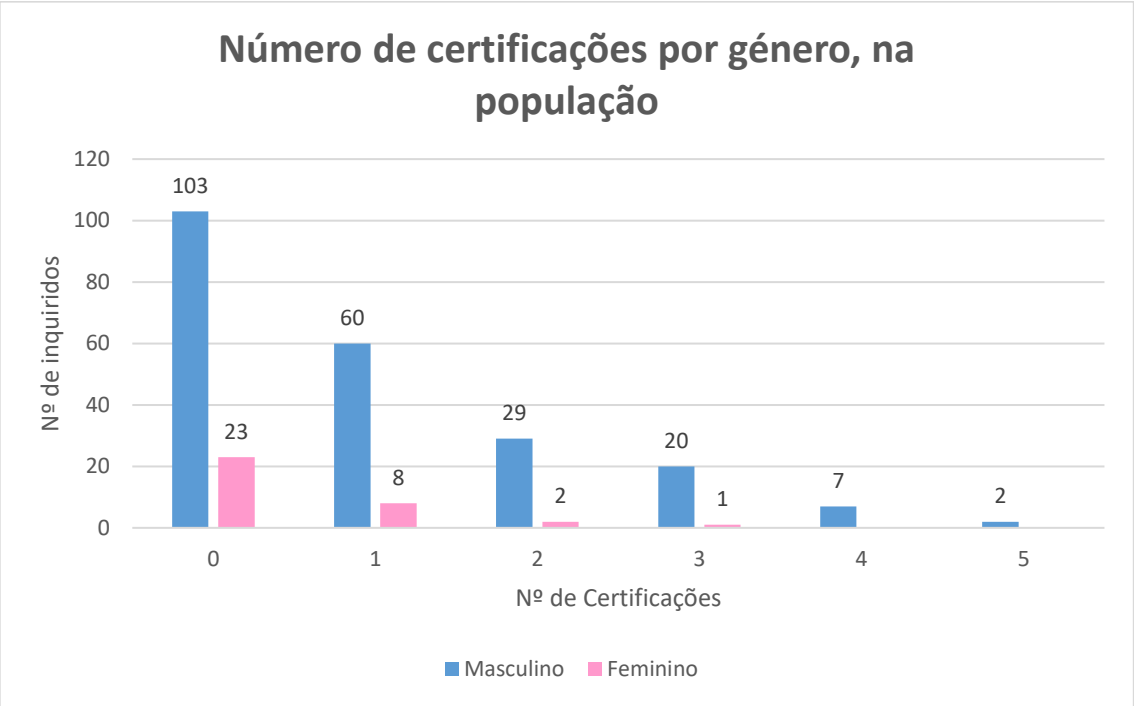


Gráfico 18 – Quantidade de certificações por género, na população.

Nos dados obtidos através da aplicação do questionário constata-se que os inquiridos do género feminino são quem possui um maior número de certificações (considerando apenas as certificações CISA, CRISC, CISM, CGEIT, CSX-P, CDPSE, CIA) sendo que metade dos inquiridos do género feminino diz possui 3 destas certificações. Pelo contrário os inquiridos do género masculino são quem possui menos certificações, uma vez que 4 inquiridos deste género referem possuir apenas 1 destas 7 certificações.

Realizando agora a mesma análise, mas nos dados referentes à população, constata-se que à medida que o número de certificações aumenta o número de membros certificados diminui (ver Gráfico 18), o que não se constata na amostra inquirida. Assim, na população a resposta mais dada tanto por membros do género masculino como por membros do género feminino são 0 certificações. Desta forma, não é possível realizar uma extrapolação dos dados obtidos na amostra.

2.6 Conclusões do estudo

Realizando uma conclusão do estudo apresentado anteriormente, relativamente à caracterização da amostra inquirida pode afirmar-se que o inquirido padrão é do género

masculino, possui entre 36 e 45 anos de idade, entre 5 e 9 anos em termos de experiência como auditor e como auditor de SI, o âmbito geográfico de atividade da empresa para a qual trabalha é nacional e o setor/área de negócio para o qual trabalha são os serviços financeiros.

As ferramentas que os inquiridos mais conhecem são, nomeadamente, Microsoft Access, Microsoft Excel, MySQL, CaseWare IDEA Analytics, TeamMate Audit Management, Galvanize e o Nessus, podendo afirmar-se que com mais expressão encontram-se ferramentas de utilidade geral. Outras ferramentas mencionadas pelos inquiridos são: Power BI, MicroStrategy, SAS, Azure Data Studio e Bwise Audit Management.

Como ferramentas não conhecidas por qualquer inquirido destacam-se o CaseWare Working Papers, DRAI, MyWorkpapers, SIAUDI, SE Audit e SiAudit, todas na área de ferramentas de gestão de papéis de trabalho.

Por outra perspetiva, os inquiridos referem utilizar com mais frequência as ferramentas CaseWare IDEA Analytics, Pentana Audit, Microsoft Access, Microsoft Excel, MySQL e ferramenta desenvolvida pela própria empresa, sendo de maior representatividade ferramentas de utilidade geral. Desta forma, numa hierarquização de utilização das ferramentas as mais utilizadas também são de utilidade geral.

No âmbito das vantagens da utilização de CAATs para auditoria, os inquiridos estão em concordância parcial ou total relativamente à maioria das vantagens apresentadas, sendo a "maximização de tempo" e a "agregação de valor ao trabalho de auditoria" as vantagens com as quais mais inquiridos concordam a um nível mais elevado. No entanto, 2 inquiridos discordam parcialmente da "economia de quantias substanciais de dinheiro para a empresa", o que revela que é de extrema importância avaliar os ganhos e os benefícios da aposta e utilização de CAATs, sem esquecer os custos de investimento em *software* e na formação dos utilizadores.

De notar, ainda, que, maioritariamente, os inquiridos consideram que as ferramentas que utilizam como suporte às auditorias que realizam são uma boa base de trabalho e contribuem positivamente para o trabalho que executam.

As análises que os inquiridos mencionaram que as CAATs lhes permitem realizar são nomeadamente a identificação de exceções, anomalias e de padrões, a análise de *logs*, o controlo de acessos/acessos indevidos, a verificação de duplicações, extração de amostras, ou seja, na maioria das análises anteriores esta implícita a análise à qualidade

dos dados. Assim, é ainda possível concluir que as análises mencionadas pelos inquiridos foram ao encontro das mencionadas na revisão da literatura.

Em relação aos impactos verificou-se que a maioria dos inquiridos concordam total ou parcialmente com os impactos apresentados, sendo os impactos com os quais os inquiridos concordam mais, ou seja, a um nível de concordância mais elevado, os impactos nos mecanismos de gestão de risco, nos mecanismos de controlo dos SI e na gestão de vulnerabilidades.

Relativamente à secção do questionário sobre formação e certificação, pode concluir-se que a maioria dos inquiridos considera que possui uma formação adequada para o desempenho das suas funções com a utilização de CAATs. No entanto, alguns inquiridos referem possuir uma formação insuficiente, o que ressalta que o facto de a auditoria estar em constante evolução e essa evolução implicar alterações e evoluções no que diz respeito ao papel que o autor desempenha e às ferramentas que usa, o que irá implicar uma necessidade constante de formação e atualização das competências dos auditores.

No que diz respeito às certificações, a certificação com mais relevância, tanto na população como na amostra inquirida, é a certificação CISA.

Por fim, é importante salientar que o número de respostas ao questionário foi reduzido, desta forma estas conclusões não se devem generalizar, ou seja, não é possível realizar uma extrapolação dos dados obtidos para a população.

Conclusão

A presente investigação teve como principais objetivos de estudo identificar quais as CAATs que os auditores de SI podem aplicar nas etapas de trabalho de campo, que análises podem os auditores de SI realizar através do uso destas ferramentas de auditoria auxiliadas por computador, quais os impactos de uma auditoria de SI para a organização auditada, quais as vantagens da utilização das CAATs para o trabalho dos auditores de SI e, ainda, quais as áreas de enfoque de uma auditoria de SI.

Relativamente às CAATs que os auditores de SI podem utilizar numa auditoria, ao nível de tipologia, na revisão da literatura, foram identificadas ferramentas de extração e análise de dados, ferramentas de gestão de papéis de trabalho, ferramentas para a segurança de sistemas informáticos e ferramentas de utilidade geral. Através do questionário realizado *on-line* verificou-se que as ferramentas que os inquiridos mais conhecem e mais utilizam são ferramentas de utilidade geral, nomeadamente as ferramentas Microsoft Access, Microsoft Excel e MySQL.

Em termos de análises que os auditores de SI podem realizar através das CAATs, na referência individual feita a cada ferramenta, na revisão da literatura, foram indicadas várias análises que determinada ferramenta permite realizar. Com a aplicação do questionário constatou-se que as análises referidas pelos inquiridos vão ao encontro das análises mencionadas na revisão da literatura.

No que diz respeito aos impactos de uma auditoria de SI para a organização auditada, pode concluir-se que, ao nível da estrutura organizacional, a realização de auditoria de SI transmite confiança aos *stakeholders* e acarreta impactos positivos ao nível da tomada de decisão, controlo interno, gestão de riscos e gestão de vulnerabilidades. Desta forma, a auditoria de SI possibilita inúmeros benefícios que tornam mais fácil o alcance dos objetivos organizacionais, bem como operar de um modo mais eficiente, o que, consequentemente, favorece e promove a viabilidade da organização.

No estudo empírico verificou-se que a opinião dos inquiridos está, na sua maioria, em concordância com os impactos mencionados na revisão da literatura.

Foram ainda identificadas, na revisão da literatura, diversas vantagens por diferentes autores, sobre as quais se verificou, maioritariamente, uma concordância, através da aplicação do questionário aos membros do ISACA Lisbon Chapter. No entanto, foi ainda possível concluir que é de extrema importância avaliar os ganhos e os benefícios na aposta

e utilização de CAATs, sem esquecer os custos no investimento em *software* e na formação dos utilizadores.

Por fim, no que respeita às áreas de enfoque de uma auditoria de SI, verificou-se, através da revisão da literatura, que o foco de uma auditoria de SI incide sobre o *hardware*, *software*, base de dados e redes de comunicações.

Contributos

Ao nível de contributos pode destacar-se o levantamento efetuado de diversas ferramentas que os auditores de SI utilizam ou podem utilizar, de modo a dar conhecimento de e sobre ferramentas de apoio à auditoria e de que modo estas contribuem para os trabalhos de uma auditoria.

Assim, pretende-se que, com o conhecimento da existência de várias ferramentas disponíveis no mercado e das suas potencialidades, seja possível a escolha da mais adequada, tendo em conta os objetivos e as necessidades da auditoria que se pretende realizar.

Destaca-se ainda como contributo a realização de questionários, a fim de averiguar e compreender a utilização e perceção de CAATs por auditores de SI e o contributo de alguma forma para o desenvolvimento de trabalhos futuros, relacionados com este tema.

Desta forma, pretende-se que o presente trabalho contribua para um aumento de conhecimento, nomeadamente ao nível da auditoria de SI, da existência e uso de CAATs, do papel do auditor e do contributo dos SI para o auditor e, consequentemente, para um trabalho de auditoria mais eficiente e eficaz.

Limitações

Em termos de limitações constata-se que a recolha de dados através da realização de inquéritos, em tempos de pandemia, exigiu várias tentativas (ver apêndice 3 - Aplicação do Questionários – Fluxo Temporal), sendo difícil a obtenção de respostas ao questionário por parte da população em estudo, os profissionais de auditoria de SI, membros do ISACA Lisbon Chapter.

Desta forma, o número de respostas obtido foi reduzido, não sendo possível analisar a amostra inicialmente pretendida. Assim, é importante referir que as conclusões obtidas não devem ser generalizadas à população em estudo.

Trabalho Futuro

Fruto de uma reflexão efetuada durante a realização e conclusão deste trabalho de investigação identificam-se alguns aspetos a ter em consideração para a realização de trabalhos futuros.

Devido à constante evolução tecnológica, novas ferramentas de apoio à auditoria, CAATs, dignas de análise irão com certeza surgir. Desta forma será possível futuramente atualizar a pesquisa realizada, neste trabalho de investigação, relativamente a novas ferramentas ou a atualizações de CAATs já investigadas com o presente trabalho.

Outras linhas de investigação futuras poderão ser a análise da evolução da utilização de CAATs por auditores membros do ISACA Lisbon Chapter ou o desenvolvimento de um estudo comparativo entre conclusões obtidas em Portugal e conclusões obtidas noutros países, analisando as principais diferenças e os principais pontos em comum.

Relativamente ao tema desta investigação sugere-se ainda em trabalho futuro uma análise relativa à evolução futura das CAATs e de como estas apoiam e contribuem para uma evolução do trabalho de auditoria.

Ao nível de trabalho futuro que implique a recolha de dados sugere-se a realização de entrevistas ou contacto em formação, uma vez que através da recolha de dados por questionários foi levantada como uma limitação, devido ao reduzido número de respostas, após diversas tentativas.

Considera-se, finalmente, que esta área de investigação é relevante e, em especial em Portugal, tem ainda poucas publicações e investigação disponíveis pelo que importa promover a colaboração entre a Academia e o ISACA, ou com outros organismos profissionais, no sentido de incentivar novos estudos.

REFERÊNCIAS BIBLIOGRÁFICAS

Andrade, F. C. C. (2013). Fórum Nacional de Governança, Tecnologia e Inovação. *Certificações ISACA CISA, CISM, CGEIT, CRISC*. https://docplayer.com.br/3420259-Certificacoes-isaca-cisa-cism-cgeit-crisc-forum-nacional-de-governanca-tecnologia-e-inovacao-lavras-mg-marco-2013.html

Auditing Software Distributor. (2020a). *O software mais completo para auditorias financeiras. Descubra as nossas soluções para o auditor*. https://www.asdaudit.pt/

Auditing Software Distributor. (2020b). *Software de auditoría y análisis financiero*. https://www.asdaudit.pt/productos/auditor/

BDO. (2020a). *DRAI 3 – SNC*. https://www.bdo.pt/getmedia/367bae2b-667f-4a2d-8fe9-dd262e673744/drai3-brochura-snc.pdf.aspx

BDO. (2020b). *DRAI SAFT*. https://www.bdo.pt/getmedia/b811fa71-84cf-4629-bc81-998b85fa2f5b/drai-saf-t-brochura.pdf.aspx

BDO. (2020c). *Ferramentas Informáticas de Apoio à Auditoria*. https://www.bdo.pt/pt-pt/servicos/audit-assurance/ferramentas-informaticas-de-apoio-a-auditoria

Bourgeois, D. T. (2021). *Information Systems for Business and Beyond*. https://bus206.pressbooks.com/chapter/chapter-1/#footnote-5-2

Brito, T. F. C. de. (2015). *Tecnologias de informação de suporte à auditoria*. http://repositorio.ual.pt/handle/11144/2398

Business Wire. (2015). *Nexus Cybersecurity da ISACA lança a Certificação Profissional CSX*. https://www.businesswire.com/news/home/20150805005472/pt/

CaseWare International. (2020a). *CaseWare Working Papers 2020*. https://www.caseware.com/products/working-papers

CaseWare International. (2020b). *The Trusted Tool for Data Analysis*. https://idea.caseware.com/products/idea

Coelho, D. M. S. (2010). *IDEA - lnteractive Data Extraction & Analysis: Principais benefícios e vantragens na sua utilização no trabalho de auditoria e na detecção de erros e fraudes* [Universidade de Évora]. https://dspace.uevora.pt/rdpc/handle/10174/21050

Correia, T. S. O. (2017). *Software Open Source em Auditoria* [Instituto Superior de Contabilidade e Administração de Coimbra]. https://doi.org/10.23919/cisti.2018.8399428

Duque, F. J. V., & Arias, J. A. T. (2012). Evidencia digital y técnicas y herramientas de auditoría asistidas por computador. *Ventana Informatica*, *26*, 93–110. https://doi.org/10.30554/ventanainform.26.142.2012

Duque, F. J. V., & Arias, J. A. T. (2017). Modelos de Auditoría Continua: Una Propuesta Taxonómica. *Journal of Information Systems and Technology Management - – Jistem USP*, *14*(3), 463–481. https://doi.org/10.4301/s1807-17752017000300010

Fargason, S. (2001). Using Audit Software for Risk Management , Continuous Monitoring , And Data Analysis. *The IIA Research Foundation*, 1–13. https://na.theiia.org/about-us/Public Documents/Sawyer_Award_2001.pdf

Francisco, L. M. F. (2013). *A Análise Digital em Portugal – Um estudo empírico* [Escola Superior de Tecnologia e Gestão]. https://iconline.ipleiria.pt/handle/10400.8/2111

Galvanize. (2020a). *AuditBond*. https://www.wegalvanize.com/audit-management/

Galvanize. (2020b). *GRC software that strengthens organizations*. https://www.wegalvanize.com/

Gelbstein, E. (2017). Risk-based Audit Planning basics for Beginners. *Isaca Journal*, *2*, 1–4. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/is-audit-basics-risk-based-audit-planning-for-beginners

Guimarães, F. J. R. S. (2018). *Ontologias com Suporte em Metadados para Interoperabilidade entre Arquitetura Empresarial e Business Intelligence* [Universidade de Évora]. http://hdl.handle.net/10174/23561%0A

IAASB. (2009). *Glossary of terms*. https://www.ifac.org/system/files/downloads/a005-2010-iaasb-handbook-handbook-glossary.pdf

Ideagen. (2020). *Audit management software*. https://www.ideagen.com/products/pentana-audit

IIA. (2017a). *Exame CIA : Por Que e Como Está Mudando*. https://global.theiia.org/translations/PublicDocuments/CIA-Exam-Syllabi-Changes-Handbook-Portuguese.pdf

IIA. (2017b). *International Standards for the Professional Practice of Internal Auditing (Standards)*. https://na.theiia.org/standards-guidance/Public Documents/IPPF-Standards-2017.pdf

IIA. (2020). *Prove Credibility & Proficiency*. https://global.theiia.org/certification/CIA-Certification/Pages/CIA-Certification.aspx

InformationActive. (2020). *ActiveData - Analytics For Excel*. https://www.informationactive.com/ia.cgi?f=home-en

IPAI. (2019a). *Certificações - Manual do Candidato*. 1–31. https://www.ipai.pt/fotos/gca/certificacoes_iia_manual_em_portugues_2019_1563976631.pdf

IPAI. (2019b). *CIA*. https://www.ipai.pt/gca/index.php?id=48

ISACA. (2014). *CISA Review Manual*.

ISACA. (2015). *ISACA Glossary of Terms*. https://www.isaca.org/resources/glossary

ISACA. (2019a). *Cerfiticação em Risco e Controle em Sistemas de Informação (CRISC)*. https://engage.isaca.org/brasiliachapter/certificacao/certificacoesisaca/crisc

ISACA. (2019b). *Certificação em Gestão de Segurança da Informação (CISM)*. https://engage.isaca.org/brasiliachapter/certificacao/certificacoesisaca/cism

ISACA. (2019c). *Certificação em Governança Corporativa de TI (CGEIT)*. https://engage.isaca.org/brasiliachapter/certificacao/certificacoesisaca/cgeit

ISACA. (2019d). *CISA Review Manual. 27th Editi*.

ISACA. (2020a). *CDPSE*. https://www.isaca.org/credentialing/certified-data-privacy-solutions-engineer

ISACA. (2020b). *CGEIT*. https://www.isaca.org/credentialing/cgeit

ISACA. (2020c). *CISA*. https://www.isaca.org/credentialing/cisa

ISACA. (2020d). *CISM*. https://www.isaca.org/credentialing/cism

ISACA. (2020e). *CRISC*. https://www.isaca.org/credentialing/crisc

ISACA. (2020f). *CSX-P*. https://www.isaca.org/credentialing/csx-p

ISACA. (2020g). *Estatísticas Associados*.

Lima, M. N., & Souza, Z. (2001). Tecnologia da Informação ao Alcance da Auditoria. *Revista de Contabilidade Do Mestrado Em Ciências Contábeis Da UERJ*. http://www.atena.org.br/revista/ojs-2.2.3-08/index.php/UERJ/article/view/1663/1484

Magique Galileo. (2019). *Audit Management*. https://magiquegalileo.com/audit-management/

MetricStream. (2020a). *Internal Audit Management*. https://www.metricstream.com/products/internal-audit-management.htm

MetricStream. (2020b). *Operational Audit Management*. https://www.metricstream.com/products/operational-audit-management.htm

Microsoft. (2020a). *Microsoft Excel*. https://www.microsoft.com/pt-pt/microsoft-365/excel

Microsoft. (2020b). *Tire o máximo partido dos seus dados*. https://www.microsoft.com/pt-pt/microsoft-365/access

Morais, G., & Martins, I. (2013). *Auditoria Interna* (4ª Edição). Áreas Editora.

MyWorkpapers. (2020). *Audit Content Pack*. https://www.myworkpapers.com/content-packs/myworkpapers-content-pack/audit-content-pack/

Nagios. (2020). *What Is Nagios?* https://www.nagios.org/about/

Oracle. (2020a). *MySQL Database Service*. https://www.oracle.com/mysql/

Oracle. (2020b). *MySQL Enterprise Audit*. https://www.mysql.com/products/enterprise/audit.html

Pedrosa, I. M. M. (2015). *Computer-assisted Audit Tools and Techniques use: Determinants for Individual Acceptance* [Instituto Uniersitário de Lisboa]. https://doi.org/10.1377/hlthaff.2013.0625

Porto, J. (2011). *CAATs – Técnicas de Auditoria Auxiliada por Computadores*. https://audiit.wordpress.com/2011/11/07/caats-tecnicas-de-auditoria-auxiliada-por-computadores/

Ribeiro, R. (2017). A importância da utilização de software no processo de documentação de uma auditoria. *Revisores e Auditores*, *76*, 67–69. https://www.oroc.pt/publicacoes/revista/revista/anos-anteriores/2017/

SAP. (2020). *SAP Audit Management*. https://www.sap.com/products/audit-management.html?btp=7b2c7ba1-a2ff-4b3f-88a8-c895e934cbd2

Sayana, S. A. (2002). The IS Audit Process. *Information Systems Control Journal*, *1*. http://carl.sandiego.edu/ctu/IS_audit_process.pdf

Sayana, S. A. (2003). Using CAATs to support IS audit. *Information Systems Control Journal*, *1*, 21–23. https://csbweb01.uncw.edu/people/ivancevichd/classes/msa516/extra readings on topics/caats/using caatts to support it audit.pdf

SIAUDIT. (2020). *El Software Para Revisoria Fiscal y Auditoria Financiera que Necesitas*. https://www.siaudit.co/

Silva, P. M. G. (2007). *A Função Auditoria de Sistemas de Informação : Modelo Funcional e de Competências* [Universidade do Minho]. http://repositorium.sdum.uminho.pt/handle/1822/8058

SoftExpert Software. (2020). *SoftExpert Audit*. https://www.softexpert.com/produto/audit-planning-control/

Software Público Brasileiro. (2020). *Siaudi - Sistema de Auditoria*. https://softwarepublico.gov.br/social/siaudi

SolarWinds. (2020a). *Access Rights Manager*. https://www.solarwinds.com/pt/access-rights-manager

SolarWinds. (2020b). *SolarWinds Access Rights Manager*. https://www.solarwinds.com/-/media/solarwinds/swdcv2/licensed-products/access-rights-manager/resources/datasheets/arm-datasheet-pt.ashx?rev=0a71a764a84643f0917bee1e4dcc3532

Tenable. (2020). *A Família Nessus*. https://pt-br.tenable.com/products/nessus

Teruel, E. C. (2010). Principais ferramentas utilizadas na auditoria de sistemas e suas características. *Universidade Nove de Julho (UNINOVE), São Paulo*, 1–10. https://dhg1h5j42swfq.cloudfront.net/2018/06/28174439/teruel-evandro-carlos.pdf

Tribunal de Contas. (1999). *Manual de Auditoria de Procedimentos*. *1*, 1–139. https://www.tcontas.pt/pt-pt/NormasOrientacoes/ManuaisTC/Documents/Manual_vol1.pdf

Tripwire. (2020a). *About Tripwire*. https://www.tripwire.com/company

Tripwire. (2020b). *Cybersecurity Services by Tripwire*. https://www.tripwire.com/solutions/tripwire-cybersecurity-services

Tripwire. (2020c). *Tripwire's IP360™ Vulnerability Management Solution Awarded 5-Star Review from SC Media*. https://www.tripwire.com/company/press-releases/2020/07/ip360-vulnerability-management-solution-awarded-5star-review-from-sc-media

WIS 4. (2018). *Sistema Informático de Papéis de Trabalho de Auditoria*. https://www.sipta.pt/site/

Wolters Kluwer. (2020a). *TeamMate Analytics Features*. https://www.wolterskluwer.com/en/solutions/teammate/teammate-analytics/features

Wolters Kluwer. (2020b). *TeamMate Analytics for Audit*. https://www.wolterskluwer.com/en/solutions/teammate/teammate-analytics

Wolters Kluwer. (2020c). *TeamMate Audit Solutions*. https://www.wolterskluwer.com/en/solutions/teammate

APÊNDICES

APÊNDICE 1. Endereços dos websites das CAATs analisadas

Nome da ferramenta	**Site Web**
Active Data	https://www.informationactive.com/ia.cgi?f=home-en
ASD Auditor	https://www.asdaudit.pt/ https://www.asdaudit.pt/productos/auditor/
CaseWare IDEA Analytics	https://idea.caseware.com/products/idea
Magique Galileo	https://magiquegalileo.com/audit-management/
TeamMate Analytics	https://www.wolterskluwer.com/en/solutions/teammate/teammate-analytics/features https://www.wolterskluwer.com/en/solutions/teammate/teammate-analytics
CaseWare Working Papers	https://www.caseware.com/products/working-papers
DRAI	https://www.bdo.pt/pt-pt/servicos/audit-assurance/ferramentas-informaticas-de-apoio-a-auditoria https://www.bdo.pt/getmedia/b811fa71-84cf-4629-bc81-998b85fa2f5b/drai-saf-t-brochura.pdf.aspx https://www.bdo.pt/getmedia/367bae2b-667f-4a2d-8fe9-dd262e673744/drai3-brochura-snc.pdf.aspx
MetricStream	https://www.metricstream.com/products/internal-audit-management.htm https://www.metricstream.com/products/operational-audit-management.htm
MyWorkpapers	https://www.myworkpapers.com/content-packs/myworkpapers-content-pack/audit-content-pack/
Pentana Audit	https://www.ideagen.com/products/pentana-audit

Nome da ferramenta	**Site Web**
SAP Audit Management	https://www.sap.com/products/audit-management.html?btp=9726bfb4-d7e8-4006-b898-ec56d31b84b6
SIAUDI	https://softwarepublico.gov.br/social/siaudi
SIPTA	https://www.sipta.pt/
SE Audit	https://www.softexpert.com/produto/audit-planning-control/
SiAudit	https://www.siaudit.co/
TeamMate Audit Management	https://www.wolterskluwer.com/en/solutions/teammate
Galvanize (anterior ACL Data Analysis)	https://www.wegalvanize.com/ https://www.wegalvanize.com/audit-management/
Access Rights Manager	https://www.solarwinds.com/pt/access-rights-manager https://www.solarwinds.com/-/media/solarwinds/swdcv2/licensed-products/access-rights-manager/resources/datasheets/arm-datasheet-pt.ashx?rev=0a71a764a84643f0917bee1e4dcc3532
Nagios	https://www.nagios.org/about/
Nessus	https://pt-br.tenable.com/products/nessus
Tripwire	https://www.tripwire.com/company https://www.tripwire.com/solutions/tripwire-cybersecurity-services https://www.tripwire.com/company/press-releases/2020/07/ip360-vulnerability-management-solution-awarded-5star-review-from-sc-media
Microsoft Access	https://www.microsoft.com/pt-pt/microsoft-365/access

Nome da ferramenta	**Site Web**
Microsoft Excel	https://www.microsoft.com/pt-pt/microsoft-365/excel
MySQL	https://www.oracle.com/mysql/ https://www.mysql.com/products/enterprise/audit.html

APÊNDICE 2. Questionário

Auditoria de Sistemas de Informação e a Utilização de CAATs

O presente questionário enquadra-se no âmbito da fase final do Mestrado de Auditoria Empresarial e Pública, segundo ciclo, no Instituto Superior de Contabilidade e Administração de Coimbra.
Este formulário tem como objetivo averiguar a utilização e percepção de Computer-assisted Audit Techniques (CAATs) por auditores de Sistemas de Informação (SI).
As respostas ao questionário são anónimas e confidências, sendo que os resultados obtidos serão apenas utilizados no âmbito da investigação científica e apenas de forma agregada, sem identificar, de qualquer forma, os respondentes.
Agradeço desde já a sua colaboração.
Mónica Silva, Mestrado em Auditoria Empresarial e Pública, iscac17593@alumni.iscac.pt
Instituto Superior de Contabilidade e Administração de Coimbra, ISCAC
Instituto Politécnico de Coimbra.

0% 100%

* **Género**

◯ Feminino ◯ Masculino

*
Indique a sua idade (anos completos em 31.12.2020).

Neste campo só se aceitam números

*
Quantos anos de experiência possui como auditor (à data de 31/12/2020)?

Neste campo só se aceitam números

*
Quantos anos de experiência possui como auditor de SI (à data de 31/12/2020)?

Neste campo só se aceitam números

*
Indique o âmbito de atividade da sua empresa?

Escolha uma das seguintes respostas

◯ Big Four
◯ Nacional
◯ Regional
◯ Local

*

Indique o setor/área de négocio a que percetence a sua empresa?

Seleccione todas as que se apliquem

- ☐ Financeiro/Banca
- ☐ Militar
- ☐ Serviços Tecnológicos/Consultoria
- ☐ Seguros
- ☐ Contabilidade Pública
- ☐ Fabrico/Engenharia
- ☐ Cuidados de Saúde/Médico
- ☐ Comércio a Retalho/Grossista/Distribuição
- ☐ Construção/Mineiro/Petrolífero/Agrícola
- ☐ Telecomunicações/Comunicações
- ☐ Serviços Públicos
- ☐ Transportes
- ☐ Farmacêutico
- ☐ Publicidade/Marketing/Comunicação Social
- ☐ Aviação
- ☐ Outro:

* **Indique quais as ferramentas que conhece (independentemente se já trabalhou ou não com essa ferramenta).**

Seleccione todas as que se apliquem

- ☐ Active Data
- ☐ ASD Auditor
- ☐ CaseWare IDEA Analytics
- ☐ Galvanize (anterior ACL Data Analysis)
- ☐ Magique Galileo
- ☐ SE Audit
- ☐ SiAudit
- ☐ TeamMate Analytics
- ☐ CaseWare Working Papers
- ☐ DRAI
- ☐ MetricStream
- ☐ MyWorkpapers
- ☐ Pentana Audit
- ☐ SAP Audit Management
- ☐ SIAUDI
- ☐ SIPTA
- ☐ TeamMate Audit Management
- ☐ Access Rights Manager
- ☐ Nagios
- ☐ Nessus
- ☐ Tripwire
- ☐ Microsoft Access
- ☐ Microsoft Excel
- ☐ MySQL
- ☐ Ferramenta desenvolvida pela própria empresa
- ☐ Outra Ferramenta 1
- ☐ Outra Ferramenta 2
- ☐ Outra Ferramenta 3

Se indicou outra/as ferramenta/as na questão anterior, esclareça concretamente a opção selecionada a que ferramenta corresponde, por exemplo "outra ferramenta 1 = Microsoft Word"

*

Tendo em conta as ferramentas com as quais trabalhou no último ano, indique com que frequência utiliza as seguintes ferramentas?

	Não utiliza	Menos de 1 vez por semana	Cerca de 1 vez por semana	2 ou 3 vezes por semana	Várias vezes por semana	Cerca de 1 vez por dia	Várias vezes por dia
Active Data	○	○	○	○	○	○	○
ASD Auditor	○	○	○	○	○	○	○
CaseWare IDEA Analytics	○	○	○	○	○	○	○
Galvanize (anterior ACL Data Analysis)	○	○	○	○	○	○	○
Magique Galileo	○	○	○	○	○	○	○
SE Audit	○	○	○	○	○	○	○
SiAudit	○	○	○	○	○	○	○
TeamMate Analytics	○	○	○	○	○	○	○
CaseWare Working Papers	○	○	○	○	○	○	○
DRAI	○	○	○	○	○	○	○
MetricStream	○	○	○	○	○	○	○
MyWorkpapers	○	○	○	○	○	○	○
Pentana Audit	○	○	○	○	○	○	○
SAP Audit Management	○	○	○	○	○	○	○
SIAUDI	○	○	○	○	○	○	○
SIPTA	○	○	○	○	○	○	○
TeamMate Audit Management	○	○	○	○	○	○	○
Access Rights Manager	○	○	○	○	○	○	○
Nagios	○	○	○	○	○	○	○
Nessus	○	○	○	○	○	○	○
Tripwire	○	○	○	○	○	○	○
Microsoft Access	○	○	○	○	○	○	○
Microsoft Excel	○	○	○	○	○	○	○
MySQL	○	○	○	○	○	○	○
Ferramenta desenvolvida pela própria empresa	○	○	○	○	○	○	○
Outra Ferramenta 1	○	○	○	○	○	○	○
Outra Ferramenta 2	○	○	○	○	○	○	○
Outra Ferramenta 3	○	○	○	○	○	○	○

Tendo em conta as ferramentas com as quais trabalha.
Hierarquize, indicando da ferramenta com a qual trabalha com mais frequência para a ferramenta com a qual trabalha com menos frequência?

Clique num item na lista à esquerda, começando com o item de maior classificação, e percorrendo os itens até ao menor.

As suas escolhas:	A sua classificação:
Active Data	1:
ASD Auditor	2:
CaseWare IDEA Analytics	3:
Galvanize (anterior ACL Data Analysis)	4:
Magique Galileo	5:
SE Audit	6:
SiAudit	7:
TeamMate Analytics	8:
CaseWare Working Papers	9:
DRAI	10:
MetricStream	11:
MyWorkpapers	12:
Pentana Audit	13:
SAP Audit Management	14:
SIAUDI	15:
SIPTA	16:
TeamMate Audit Management	17:
Access Rights Manager	18:
Nagios	19:
Nessus	20:
Tripwire	21:
Microsoft Access	22:
Microsoft Excel	23:
MySQL	24:
Ferramenta desenvolvida pela própria empresa	25:
Outra ferramenta 1	26:
Outra ferramenta 2	27:
Outra ferramenta 3	28:

Carregue na tesoura próxima de cada item à direita para remover o último item da sua lista de classificação

*

Tendo em conta algumas vantagens da utilização de CAAT's para a auditoria, indique de que forma se identifica com as vantagens seguidamente enumeradas.

	Discordo totalmente	Discordo parcialmente	Não concordo nem discordo	Concordo parcialmente	Concordo totalmente
Economia de quantias substanciais de dinheiro para a empresa.	○	○	○	○	○
Redução de níveis de risco.	○	○	○	○	○
Maior partilha de conhecimento.	○	○	○	○	○
Diminuição das limitações impostas pelos arquivos em papel.	○	○	○	○	○
Maximização de tempo.	○	○	○	○	○
Melhor qualidade de apresentação.	○	○	○	○	○
Disponibilização de profissionais mais experientes para áreas mais técnicas e de maior risco.	○	○	○	○	○

	Discordo totalmente	Discordo parcialmente	Não concordo nem discordo	Concordo parcialmente	Concordo totalmente
Agregação de valor ao trabalho de auditoria.	○	○	○	○	○
Maior especialização dos profissionais.	○	○	○	○	○
Fluxo de informação mais rápido.	○	○	○	○	○
Maior satisfação profissional.	○	○	○	○	○
Aumento da produtividade.	○	○	○	○	○
Possibilidade de realização de um maior número de tarefas por parte de profissionais mais jovens /menos experientes.	○	○	○	○	○
Capacidade de realizar testes específicos para encontrar erros, na população.	○	○	○	○	○
Possibilidade de realizar testes a toda a população.	○	○	○	○	○
Diminuição significativa dos riscos de amostragem.	○	○	○	○	○
Capacidade de executar análises adicionais, análises de maior volume e relatórios personalizados.	○	○	○	○	○
Maior garantia dos resultados da auditoria.	○	○	○	○	○
Aumento da confidencialidade, uma vez que o departamento de SI não sabe o que está a ser testado.	○	○	○	○	○
Deteção precoce de riscos e avaliação mais abrangente destes, melhorando assim o planeamento da auditoria.	○	○	○	○	○

	Discordo totalmente	Discordo parcialmente	Não concordo nem discordo	Concordo parcialmente	Concordo totalmente
Independência por parte da auditoria, uma vez que antes de usar o software era necessário solicitar formalmente os relatórios ad-hoc específicos do departamento de SI.	○	○	○	○	○
Capacidade de limitar a amostra, tendo em conta a selecção de determinados dados como o departamento, conta, cliente ou fornecedor, etc.	○	○	○	○	○
Maior rapidez na obtenção e análise de dados.	○	○	○	○	○

*
Em que medida considera que as ferramentas que utiliza como suporte às auditorias que realiza são uma boa base de trabalho e contribuem positivamente para o trabalho que executa.

Escolha uma das seguintes respostas

- ○ Discordo totalmente
- ○ Discordo parcialmente
- ○ Não concordo nem discordo
- ○ Concordo parcialmente
- ○ Concordo totalmente

Através das CAATs que utiliza com mais frequência indique as principais análises que estas lhe permitem realizar?

(ex. análise de campos vazios, caracteres inválidos, duplicações, rácios, tendências, acessos indevidos, integridade de sistemas, estratificação de dados, extração de amostras, recálculos, etc.)

*
Tendo em conta os impactos de uma auditoria de SI para a organização auditada, indique qual a sua concordância com os impactos seguidamente indicados.

	Discordo totalmente	Discordo parcialmente	Não concordo nem discordo	Concordo parcialmente	Concordo totalmente
Gestão de vulnerabilidades.	○	○	○	○	○
Impacto no controlo interno.	○	○	○	○	○
Mecanismos de gestão de risco.	○	○	○	○	○
Mecanismos de controlo dos SI.	○	○	○	○	○
Imagem da organização perante os stakeholders.	○	○	○	○	○
Tomada de decisão.	○	○	○	○	○
Alcance de objetivos.	○	○	○	○	○
Eficiência da organização.	○	○	○	○	○

Se considera que existem outros impactos de uma auditoria de SI para a organização auditada indique-os.

*** Em que medida considera que possui a formação adequada para o desempenho de funções com a utilização de CAATs?**
Escolha uma das seguintes respostas

- ○ Nula
- ○ Insuficiente
- ○ Suficiente
- ○ Adequada
- ○ Muito adequada

*****
Atualmente possui alguma certificação, com relevância para a auditoria de SI?
(ex. CIA, CISA, CRISC, CISM, CGEIT, CSX-P, CDPSE, CIA, etc.)

○ Sim ○ Não

* **Em que medida considera que possui a formação adequada para o desempenho de funções com a utilização de CAATs?**
Escolha uma das seguintes respostas

- (•) Nula
- ( ) Insuficiente
- ( ) Suficiente
- ( ) Adequada
- ( ) Muito adequada

*
Atualmente possui alguma certificação, com relevância para a auditoria de SI?
(ex. CIA, CISA, CRISC, CISM, CGEIT, CSX-P, CDPSE, CIA, etc.)

(•) Sim ( ) Não

De entre as seguintes, qual/quais as certificações, com relevância para a auditoria de SI, possui actualmente.

Seleccione todas as que se apliquem

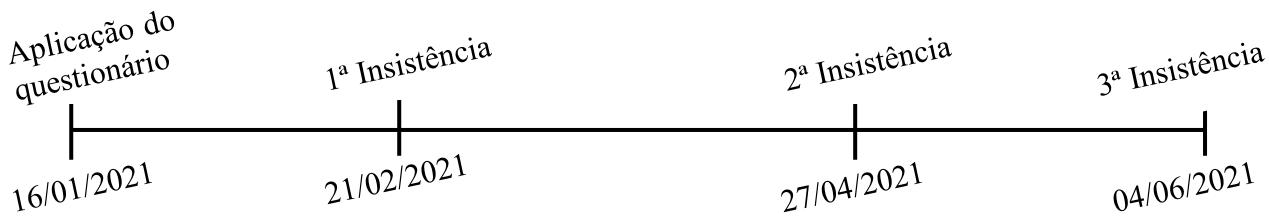
- [ ] CISA
- [ ] CRISC
- [ ] CISM
- [ ] CGEIT
- [ ] CSX-P
- [ ] CDPSE
- [ ] CIA
- [ ] Outro:

Comentários/Observações
Utilize o seguinte espaço de texto para algum comentário ou observação que entenda ser pertinente no âmbito do presente estudo.

Indique o seu endereço de e-mail se pretende ter acesso aos resultados deste questionário.

APÊNDICE 3. Aplicação do Questionário - Fluxo Temporal

No seguinte fluxo é apresentada a data de aplicação do questionário aos membros do ISACA Lisbon Chapter e são ainda apresentadas as datas das várias insistências realizadas a fim de obter respostas ao questionário aplicado no âmbito desta dissertação.



O seguinte e-mail apresenta a mensagem enviada inicialmente, a dia 16 de janeiro de 2021 aos membros do ISACA Lisbon Chapter.

Caro associado,
O ISACA Lisbon Chapter apoia o ISCAC (Coimbra Business School) em várias iniciativas tais como as seguintes:

- ISACA Student Group
- Conferência anual "Leadership of Tomorrow"
- Pós-Graduação em Auditoria, Risco e Controlo de Sistemas de Informação. Este curso é o 1.º Programa em língua portuguesa e 2.º na Europa com o reconhecimento "ISACA Model Curriculum for IS Audit and Control"
- Mentorship a Mestrandos em áreas relacionadas com a ISACA

Como parte do apoio de Mentorship, gostaríamos de contar convosco para o preenchimento do questionário da Mónica Silva, Aluna do 2.º ano do Mestrado em Auditoria Empresarial e Pública (MAEP), relacionado com "utilização de Computer-assisted Audit Techniques (CAATs)". Agradecíamos igualmente que pudessem reenviar o questionário para alguns contactos vossos na área de Auditoria.

Em adicional, no plano operacional de 2021-2022 tencionamos aumentar o alcance deste modelo para podermos apoiar outras universidades a nível nacional. Para estarem ao corrente e caso tenham interesse em saber mais informação sobre esta linha de atividades do ILC, incluindo eventual disponibilidade que tenham para apoiar alunos no desenvolvimento dos seus estudos pós-graduados, podem consultar o nosso site em WebSite ou enviem-nos um email para info@isaca-lisbon.org.

Atenciosamente,
Direcção do ISACA Lisbon Chapter